

How Distributed Ledger Technology is Transforming the Financial Marketplace

by

Michelle Bougas

A Capstone Project Submitted to the Faculty of

Utica College

December 2016

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in  
Economic Crime Management

ProQuest Number: 10245691

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10245691

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code  
Microform Edition © ProQuest LLC.

ProQuest LLC.  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106 - 1346

© Copyright 2016 by Michelle Bougas

All Rights Reserved

## **Abstract**

This project focused on exploring distributed ledger technology, specifically as it relates to its use in the financial marketplace, including addressing cybersecurity and consumer protection concerns. Distributed ledger technology is an innovative technology that offers the potential to revolutionize numerous financial sector functions, including trade settlement, clearing and execution, and anti-money laundering and know-your-customer protocols. The technology may increase procedural efficiencies, while also reducing costs and certain operational redundancies. Available research covers various aspects of the technology; however, the research also indicates there is much to learn. Various industries and governments are expending resources to further develop and enhance the technology in their efforts to implement the technology in future business practices. These research endeavors expect to highlight strengths and weaknesses, allowing for a fulsome understanding of the technology and, thus, its best use(s) within different market sectors. While distributed ledger technology may be appropriate for a variety of markets and sectors, its current standing within the financial marketplace is less certain.

Future research needs to examine specific aspects of the technology, such as cybersecurity and privacy, before its implementation into the highly regulated financial marketplace. Research efforts are ongoing, with continuous disclosure and publication of new findings. There is strong momentum and support to encourage and incorporate this technology, evidenced through the constant examination, analyses, and discourse. Public and private sectors must work together to establish global standards and policies, including cybersecurity, consumer and privacy protections, and regulation. Collaboration among technology users will be essential for its widespread success.

**Keywords:** Economic Crime Management, Paul Pantani, DLT, blockchain, fintech

## **Acknowledgments**

An incredible thank you goes out to my friends, family, and colleagues. I am truly grateful for your continued patience, encouragement, and guidance over the course of this program. Your love and support motivated me each and every day. I would not be here were it not for you and your stellar cheerleading and emotional assistance. I appreciate you all more than you will ever know.

A big thank you to Paul Pantani, my committee chair, and my second reader. Your observations and expertise help guide me in the right direction and kept me on track. To my fellow classmates in Cohort 36, I am so happy to cross the finish line with you. It has been a pleasure working with and learning from you. You made this program worthwhile. I will cherish the friendships and memories from our late night study sessions, hangouts, and residency projects. You all are amazing and I look forward to our continued friendships.

Disclaimer: The research for this Paper was conducted and the Paper was written by Michelle Bougas in her personal capacity and not in her official capacity as an employee of the Commodity Futures Trading Commission (CFTC). The analyses and conclusions expressed in this Paper are those of Ms. Bougas and do not reflect the views of other employees of the CFTC Division of Enforcement, other CFTC staff, the Commission itself, or the United States Government.

## Table of Contents

List of Illustrative Materials.....	vi
How Distributed Ledger Technology is Transforming the Financial Marketplace .....	1
Definition and Characteristics .....	2
Innovations and Trends.....	4
Potential Benefits and Complications.....	6
Cybersecurity and Vulnerability .....	7
Mitigating Fraud and Abuse .....	8
Moving Forward .....	9
Literature Review.....	10
Distributed Ledgers.....	11
Underlying Technology .....	12
Examining DLT Attributes .....	18
Current Trends .....	26
Security Issues .....	33
Consumer Protection.....	38
Looking Ahead .....	39
Discussion of the Findings.....	41
Promising Features .....	41
Inconsistencies .....	43
Limitations of the Research .....	45
Recommendations.....	48
Moving Forward .....	49
Communication.....	52
Implementation .....	56
Future Research .....	56
Conclusion .....	57
References.....	60
Appendix A – List of DLT applications in various business sectors.....	66

## **List of Illustrative Materials**

Figure 1 – Permutations of DLT systems .....	4
Figure 2 – Degrees of centralization .....	13
Figure 3 – Models of various systems: centralized, public, and private ledgers .....	16
Figure 4 – Key requirements to obtain industry-wide acceptance and usage .....	27

## **How Distributed Ledger Technology is Transforming the Financial Marketplace**

Today's financial marketplace is an intricate and complex system. It involves numerous parties, varying levels of trust, and continuous flows of information. Crafted over time, the current system is reliable, efficient, and provides transparency and certainty. The financial marketplace is currently facing a modernization that aims enhance its efficiency, transparency, and reliability. It is finding that change in its consideration of distributed ledger technology (DLT) (Depository Trust and Clearing Corporation [DTCC], 2016).

Businesses have maintained transaction ledgers for hundreds of years, beginning with stone tablets. Over time, the method of recordation evolved from stone to paper, from paper to a digital format (e.g. computers), and is now changing once again to a distributed ledger system. Each transition brought both improvements and impairments to the overall process. The move towards integrating DLT into today's financial marketplace would extend traditional systems' capabilities and offer more accuracy and security (Government Office for Science, 2016).

The purpose of this research project was to discuss and explore DLT and its impact on the financial marketplace in order to establish a more secure financial marketplace structure. Specifically, the research focused on three areas of DLT. The first area was to explore how the financial industries offering DLT-based products could best utilize the technology. In order to do so, financial market participants and regulators need to understand the technology, including current use cases as well as how it will influence current and future business models. The second area of research addressed understanding and addressing the security surrounding the technology. Specifically, the industry must consider and evaluate whether DLT can sufficiently mitigate the risk of cybersecurity vulnerabilities and whether DLT-based products are worth the



potential cybersecurity threats and vulnerabilities. The third and final area of research sought to explore how DLT users could mitigate potential fraud or misuse of DLT-based products.

The research herein focused on government research and industry white papers as well as industry publications and news articles. Several global entities, including governments, messaging services, and financial market participants extended resources in an effort to better understand the technology and start a conversation on how to best integrate it into our current financial marketplace and system. The target audience of this research project is those individuals attempting to better understand this technology and how it can and will affect the financial marketplace.

### **Definition and Characteristics**

While maintaining ledgers is not a new practice, the DLT adds a new dimension to an old procedure. In its simplest definition, a distributed ledger is a shared database that records the properties and history of an asset. A DLT can operate on a public (permissionless) or a private (permissioned) platform, each offering varying levels of distribution, consensus and verification methods, and trust. Participants on the network receive real-time updates and data dissemination. Each participant maintains a separate copy of the ledger based on the allowed permissions within a particular network. The technology presents benefits as well as the potential for increased challenges and disruptions. These changes are happening on a global scale, further magnifying its affects (Government Office for Science, 2016).

Different sources provide various definitions for DLT, and many sources use the term “blockchain” interchangeably. For the purposes of the research paper, the following definition defined the research: distributed ledger technology is a decentralized digital asset transaction database accessible across various users, sites, geographies, or institutions whose users

algorithmically verify all transactions (Government Office for Science, 2016; McLean & Deane-Johns, 2016). The technology stems from the blockchain innovation set forth in Satoshi Nakamoto's 2008 Bitcoin whitepaper, though the concept is decades older (DeRose, 2015). Blockchain is a verified record of ownership, whereby participants on a network create a transaction history through sequentially adding verified transactions into a block of data. The blocks of data subsequently join to form chains of data, creating a history spread among participants (Stafford, 2015). DLT extends well beyond the blockchain structure to offer alternative methods of verified transaction accounts (ROBECO, 2016b).

One of DLT's offered improvements is through its distributed nature, meaning multiple parties can access information contained within the ledger, provided the ledger's and the accompanying participant's permission statuses allow for such access and sharing. Another benefit is of the distribution of information in that maintaining data in a decentralized environment minimized potential risks associated with data losses. The sharing of information across nodes may reduce certain maintenance costs; however, not all agree that DLT will lower operating costs. While the technology maintains the potential to reduce back office personnel costs, DLT does require increased technical, computing, and electrical costs. The distributed and decentralized attributes of DLT contribute towards DLT's dynamic influence on the financial marketplace (ROBECO, 2016b).

It is important to note the distinction between public and private systems as each is applicable to different scenarios. There are various permutations of the public, private, permissioned, and permissionless systems, as illustrated in Figure 1. As will be addressed in depth, each system creates distinct environments in terms of trust, methodology, distribution, and

consensus. The financial marketplace will likely gravitate towards private and permissioned systems, as those systems are more in line with regulatory requirements (Digital Asset, 2016).

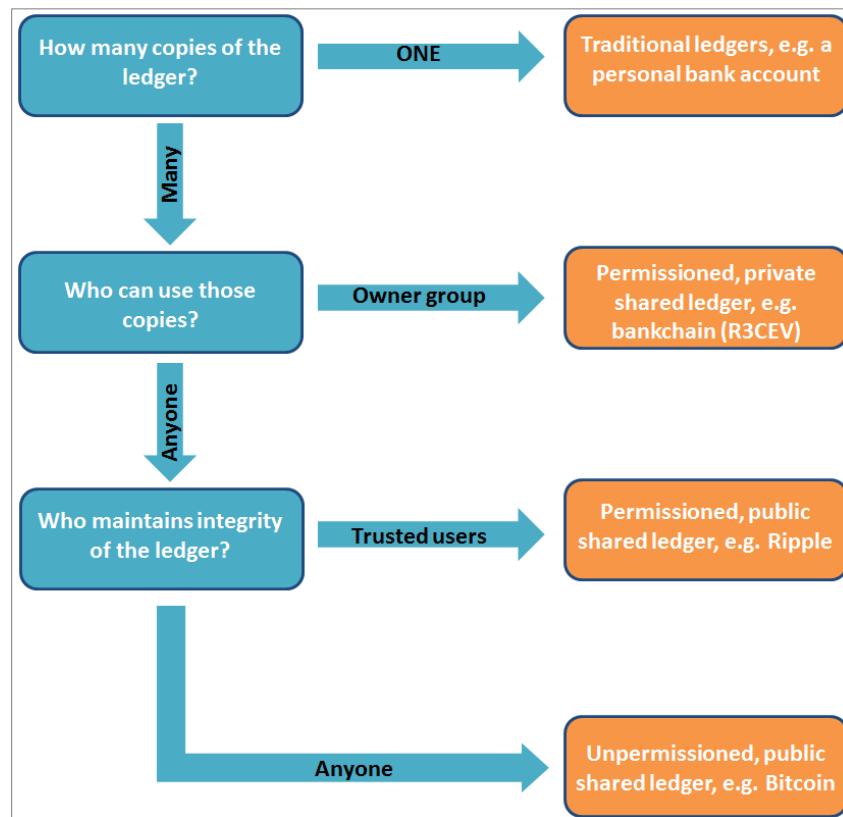


Figure 1: Permutations of DLT systems (ROBECO, 2016b)

## Innovations and Trends

Lael Brainard, member of the Board of Governors of the Federal Reserve System, stated, that the financial marketplace has much experience facing and incorporating drastic and far-reaching innovations and changes. The marketplace is clearly capable of handling major changes so long as the ultimate affects are to the benefit of the consumer and market. Advances in “the digitization of finance” are important and worthy of extensive and fulsome consideration and evaluation (Brainard, 2016, p. 1, para. 3). Regulators and developers need to establish and sustain open communication to discuss related opportunities, risks, and impacts of the technology (Brainard, 2016).

The blockchain of Bitcoin is merely one example of a DLT. It is difficult for many to distinguish blockchain from Bitcoin, which is a limitation for blockchain and DLT generally. Despite this difficulty, industries are moving forward with DLT to enhance products, services, and procedures to reduce inefficiencies and enrich consumer benefits (ROBECO, 2016b). Blockchain Technologies (2016) described various uses of DLT, including finance and trade-related services, property recordation, self-executing contracts, and identity protection.

Financial markets are exploring this technology to as a means to utilize more cost efficient processes as well as offer new products (World Federation of Exchanges, 2016). The technology is currently finding opportunities in multiple market sectors, including payment and remittance processes, insurance, personalized government services, tax receipts, smarthome networks, and crowd analysis. The important features of the technology to sustain these applications include decentralized networks, permanent records, large-scale coordination, and real-time accessibility (ROBECO, 2016b). Appendix A provides additional examples of potential DLT-based products, services, and applications as well as the necessary underlying DLT attributes. It is important to note that the technology will manifest itself and affect different industries differently (Brainard, 2016). Each context will offer a different DLT structure; however, all share the outcome of a decentralized, verified, and distributed transaction database (McLean & Deane-Johns, 2016).

One of the most prominent developments offered is the smart contract. Defined as a self-executing agreement, smart contracts function on a pre-determined set of criteria and conditions. One of the distinguishing features of the smart contract is that it relies upon programmers and codes rather than lawyers and legal terminology. Upon meeting the pre-set conditions, the contract will automatically execute (Government Office for Science, 2016). These obligations

can include transferring funds, title, property, or other assets. As with other distributed ledgers, smart contracts provide for permanent recordation of independent, verified transactions (Lambert, 2016).

### **Potential Benefits and Complications**

DLT is in its infancy, continuously expanding and evolving (ROBECO, 2016b). It offers an innovative change to the marketplace. The potential benefits could drastically modernize and enhance current processes and procedures on a global scale (D'Antona, 2016). Each product and service, though operating on a separate DLT, is associated with similar benefits and risks. Yet the technology and its implications are cause for both excitement and concern (Blockchain Technologies, 2016).

Although DLT is in its early stages of development, there is potential to transform several industries. Both technological advances and regulatory approval are required for this technology to reach its full potential within the financial marketplace, with each area needing substantial time for exploration and development. DLT has the potential to create long lasting change if the industries are prudent, cautious, and meticulous in its implementation. While there are obstacles, properly addressing those obstacles over time will allow for further development and adaptation (ROBECO, 2016b). The technology will be evolutionary, not revolutionary (Wilkins, 2016).

In July 2016, the World Federation of Exchanges (WFE) surveyed 25 worldwide market participants in an effort to gain insight as to how market participants view DLT. Respondents identified positive and negative aspects to the technology. There are aspects requiring deeper consideration and further development, including standardization, security, regulatory obligations, and scalability (WFE, 2016). Uniformity is essential for data consistency, verifiability, and reconciliation in any system. It is especially necessary for DLT. Cross-platform

consistency already poses a problem in today's disconnected and siloed business environments. Correcting this environment is a monumental task. DLT users should make efforts to address a variety of standardization issues prior to implementation, thereby avoiding aggravating an already disjointed system (DTCC, 2016).

Companies appear to be quick to incorporate DLT, specifically blockchain, into business practices (Kuchler, 2016). The Financial Stability Oversight Council within the United States (U.S.) cautioned that all new technology, including DLT, present known and unknown risks and insecurities, all of which require monitoring. Even those creating the technology acknowledge that programs and codes are not impenetrable and the industry is not capable of understanding or addressing all security needs; time, use, and experience may address these concerns (Miller, 2016).

### **Cybersecurity and Vulnerability**

Security issues and vulnerabilities are of concern to any market. Those embracing new and evolving technologies must understand these concerns and take appropriate and necessary steps to enrich security features and reduce vulnerabilities (Johnson, 2016). Vulnerabilities can occur through both internal and external compromises, including unwanted intrusions and hardware or software failure. Businesses must address their specific circumstances to determine an appropriate system for technology and the security thereof (Government Office for Science, 2016).

In 2016, different forms of DLT experienced hacks and system compromises resulting in hundreds of millions of dollars in customer losses. In April 2016, the DAO Hub, a decentralized autonomous organization, raised funds through DLT-based crowdfunding, with thousands of people purchasing into the DAO Hub via coins. Those coins entitled purchasers the power to

make suggestions on how the DAO Hub would operate and function through various smart contracts. By May 2016, over 11,000 subscribers contributed over \$150 million USD in support of the DAO Hub. In early June 2016, one of the DAO Hub creators acknowledged a bug in the system but stated that the DAO Hub's funds were not compromised or at risk. Within days of the announcement, a hacker entered the system and stole nearly \$50 million USD of the DAO Hub's value, diverting the funds into another similarly constructed organization (Siegel, 2016). The DAO Hub creators and programmers claimed to fix the programming issues and purported it would reclaim any stolen funds (Sier, 2016).

This is one example of a DLT hack or system compromise. Some of the details of the hack and proposed remedy remain unclear. This hack calls into question the permanency and irreversibility of DLT. A distributed ledger is set up to permanently record transactions without any recourse for errors. Here the DAO Hub programmers desired to unwind the ledger to the period just prior to the attack, a move that required permission and approval from a majority of participants within the network (Johnson, 2016). This action goes against one of the permanency characteristic of DLT (Siegel, 2016).

### **Mitigating Fraud and Abuse**

The financial marketplace is currently set up to handle and account for errors and mistakes, which admittedly adds time delays. The timing delays are not necessarily due to current technological limitations but rather regulatory mandates, restrictions, and protections. Implementation of DLT would impede the ability to correct errors and mistakes. The irreversibility of the DLT directly contradicts the current regulatory structure. Fraudulent or abusive transactions errors will become harder to correct in a DLT environment (DTCC, 2016).

McLean and Deane-Johns, attorneys representing global financial market-based clients, summarized that the decentralized nature of the technology inhibits accountability. Similarly, there are outstanding questions and concerns regarding security, privacy, and contract-enforceability, affecting consumer protections. With a known lack of accountability, consumers will have no redress if or when needed (McLean & Deane-Johns, 2016).

Similar to accountability, financial institutions are responsible for establishing and following strict know your client (KYC) and anti-money laundering (AML) procedures. These procedures require the in-depth collection and retention of customer information. Since DLT limits the ability to see the underlying account holder information, it hinders a financial institution's ability to monitor KYC and AML activities and conduct required due diligence (DTCC, 2016). "Effective governance and regulation are key to the successful implementation of distributed ledgers" (Government Office for Science, 2016, p. 11, para. 4). Proper and effective governance and regulatory framework will go towards protecting the consumer from fraud and abuse.

## **Moving Forward**

Despite regulatory uncertainty within the financial sector, countries are utilizing DLT for government-related services and processes. Estonia offers a strong case study of a country and government embracing DLT as a means to facilitate its operations. It is currently using DLT to maintain citizen's information for business registration, banking, and tax purposes, among others. Its population of 1.3 million presents a robust test environment for this technology as it strives forward to establish the effectiveness and efficiency of DLT as well as address security and developmental needs. Estonia is one of the global leaders in its efforts to advance this technology. Other strong proponents keen to utilize and encourage the use of DLT include the



United Kingdom, Israel, New Zealand, South Korea, Poland, China, Singapore, Latin America and the U.S. (Government Office for Science, 2016). A comprehensive understanding of the benefits and difficulties is necessary as more industries and countries turn to this technology.

### **Literature Review**

The current financial marketplace evolved over many years to meet a variety of concerns and demands. The system is set up to address settlement, clearing, and risk within the proscribed regulatory confines. The process took time, coordination, and cooperation among participants, though initial efforts appeared drastic. Each change provided improvements to the overall processes while accounting for changing regulations, technology, and market concerns. The result was a well-designed, secure, and trusted market (Brainard, 2016).

In April 2016, the U.S. Office of the Comptroller of the Currency (OCC) released a white paper providing its view on financial technology (fintech) and its place and role within the global economy. The project outlined significant criteria and structures necessary to address fintech and its future role. Specifically, it acknowledged the need to have a complete understanding of current markets, including structures, benefits, pitfalls, and regulations. The market cannot implement enhancements and improvements if it does not understand the current status. Equally, it must understand the proposed enhancements and their effects to maximize full potential. Only after obtaining this knowledge can the industry constructively move forward (OCC, 2016).

The OCC (2016) stated that it is engaging in this learning process regarding DLT, and recognized roadblocks impeding the process. It claimed that DLT has the “potential to transform how transactions are processed and settled” and the technology is a responsible innovation, especially if implemented correctly (p. 3, para. 4). The current regulatory environment is cloudy

and communication between participants and regulators is not always clear or consistent. Achieving this clearer environment requires changes from all involved parties (OCC, 2016).

ROBECO is a global asset manager based in the Netherlands. One of its mission statements centers on understanding the global marketplace and its inner and outer workings. To further this mission, it conducts market research on innovations that will bring meaningful impact and success to its clients. ROBECO (2016a) identified DLT as one of the emerging technologies with potential to drastically alter how the global market conducts business. It released a white paper in May 2016, in which it discussed the strengths and weaknesses of DLT and offered suggestions on how to improve and implement the technology (ROBECO, 2016b).

Distributed ledgers are customizable to address a variety of efficiency concerns, such as privacy, dependency, and threat models (Digital Asset, 2016). Distributed ledgers offer increased technological benefits; however, the market must acknowledge that current limits and restrictions are due to regulations and laws rather than the actual technology (DTCC, 2016). Regardless, businesses and governments continue to explore the DLT's transformative relationship and implications on financial marketplace (McLean & Deane-Johns, 2016).

## **Distributed Ledgers**

It is important to understand the technology behind distributed ledgers, including the distinction between the distributed ledger and blockchain technologies. Traditional ledgers maintain centralized authority. This centralized authority is responsible for verifying, adding, and distributing information. It also dictates the storage location and methods. In this environment, security of the information rests within limiting access to the data. Conversely, distributed ledgers maintain a peer-to-peer structure, with all nodes responsible for maintaining the data within the ledger. In a distributed ledger, the participating nodes share the verification, addition,

and maintenance responsibilities. This environment requires consensus for information verification, rather than reliance on a centralized authority. All copies of the ledger are similar and those with the appropriate permissions can view the data (Deloitte, 2016).

**Blockchain.** The blockchain is a commonly known type of distributed ledger, often associated with the cryptocurrency Bitcoin. The underlying technology relies on a peer-to-peer network wherein verified transactions join sequential into blocks of data, with those blocks merging into a chain of data. Each block is cryptographically verified and maintained, creating a visible and verifiable transaction history. The transaction history, or ledger, is distributed among the network for all to see and verify (Government Office for Science, 2016). As the data is widely distributed, making changes or alterations would require changing every copy of the ledger, which is difficult (Stafford, 2016).

Blockchain was one of the underlying technologies that inspired distributed ledgers. The two are related but distinct. Blockchain is commonly associated with cryptocurrencies, such as Bitcoin, though its application extends well beyond cryptocurrencies (Del Castillo, 2016). A blockchain is one type of distributed ledger. Not all DLT use or rely upon the blockchain structure. The market has yet to determine if blockchain itself is the best or most enduring version of DLT (ROBECO, 2016b).

### **Underlying Technology**

Distributed ledgers allow for a variety of structures and permutations. It can differ between permissioned and permissionless, public and private, and have varying degrees of distribution. A business's needs will dictate the system's level of decentralization and privacy. Each permutation will find its specific market area. Figure 2 provides a visual as to the differing degrees of permission, privacy, and centralization (Government Office for Science, 2016).

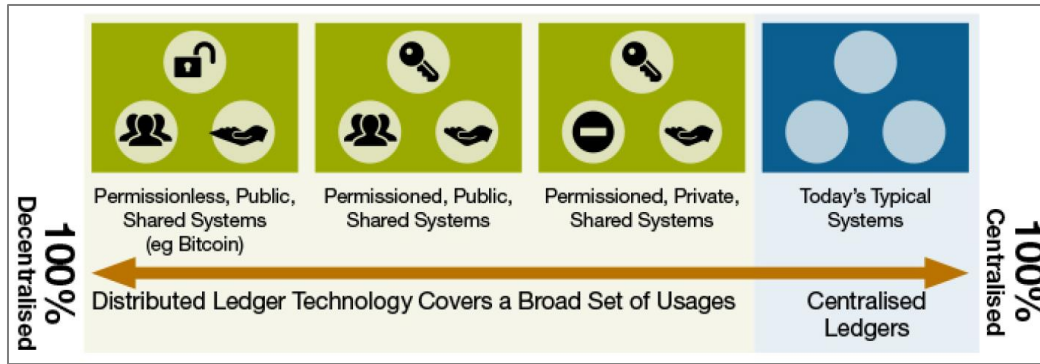


Figure 2: Degrees of centralization (Government Office for Science, 2016).

**Consensus.** One of the defining features of the DLT is the consensus algorithm.

Consensus algorithms permit transaction verification thereby allowing the tracking and recordation of a particular asset's attributes. (Digital Asset, 2016; ROBECO, 2016b). The resulting transaction history is permanent, verified, and public (ROBECO, 2016b). There are different types of distributed ledgers and each can maintain their own consensus or verification methods. Though operating under different names, all achieve the same output: Consensus commits transactions to the ledger (Digital Asset, 2016).

There are different methods to reach consensus and validation. The ledger's underlying structure and purpose will determine the appropriate method. Two such methods include proof of work and proof of stake. The proof of work method relies on the verification of mathematical problem solving. Each particular mathematical problem requires intense computing power to solve a mathematical equation. Only systems with allowable access can contribute towards the final output. Upon solving the problem, the node distributes the answer among the network for validation and acceptance. Other nodes on the network will verify the work product to ensure that only an allowed node completed the work and that it is accurate. Upon satisfaction, the transaction is accepted and added to the transaction history (European Central Bank [ECB], 2016).

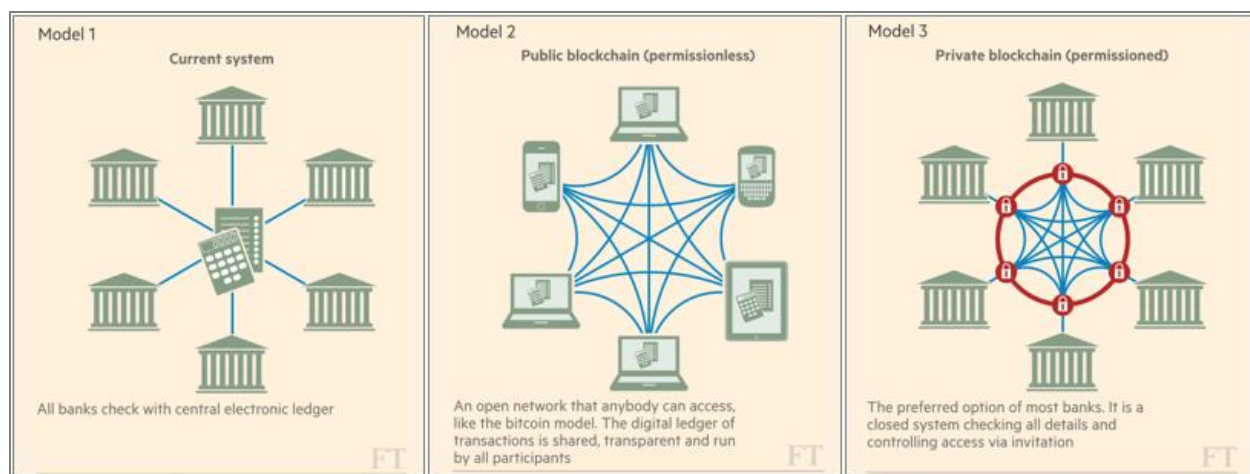
Proof of stake is another validation method. This method provides validation capabilities to specific users on the network based on their stake in the network. The owners of the network determine the criteria to establish a stake, such as identity or potentially off-ledger assets. In a proof of stake system, legitimate stakeholders work together to keep the ledger up-to-date and honest. Permissioned or restricted systems are more likely to use this consensus method (ECB, 2016). Proof of work methods depend on intense computing and energy resources, whereas proof of stake shifts its focus to those with higher interests and ownership of the system. A proof of stake structure is less costly and less likely to face malicious actions as those with more interest are unlikely to attack themselves (Deloitte, 2016; ECB, 2016).

**Decentralization.** Distributed ledgers operate in a decentralized environment. Decentralized and distributed ledgers connect to and among each other, rather than to a centralized point (Government Office for Science, 2016). Each distributed ledger operates among various nodes or locations, working together to establish, validate, and share information contained across and within the ledger. It is because of the decentralized network that there is reduction in the potential for fraud, false, or otherwise inappropriate information. It will contribute towards maintaining the ledger's integrity (DTCC, 2016).

Current systems operate within centralized or replicated ledgers. In either instance, the centralized authority maintains control of the ledger. Here, when a party is interested in submitting or retrieving information, it must communicate with the central authority to obtain that information. Additionally, replicated ledgers need to ensure it is working with the most current version of the ledger, which requires continuous requests to the central authority for updated information. In a distributed system, the entire network shares the same data, updating protocols, and maintenance responsibilities (Deloitte, 2016).

**Public versus private systems.** Public systems are open sourced and available to anyone with appropriate computing capabilities. The public distribution of the transaction information and the code is open to all nodes within the system (ROBECO, 2016b). Unrestricted ledgers are open to whomever can access the system. Anyone with access and computing capabilities can contribute towards the systems validation process (ECB, 2016). Permissionless ledgers do not have any single or identifiable owner. These ledgers allow for the possibility that anyone with computing power can validate transactions into the ledger (Government Office for Science, 2016).

Private systems are more restrictive in terms of access, consensus and verification, and distribution. In private ledgers, a central authority has the ability to restrict access and validation capabilities to a select, trusted group (ROBECO, 2016b). The central authority in these permissioned or restricted ledgers is comprised of one or multiple owners. The owner(s) authorize a select group the ability to verify and confirm transactions (Government Office for Science, 2016). Only those authorized members have permission to contribute towards the validation process (ECB, 2016). Figure 3 presents a graphical illustration of centralized, public, and private systems.



*Figure 3: Models of various systems: centralized, public, and private ledgers (Wild, Arnold, & Stafford, 2016).*

**Transparency and trust.** The current financial marketplace centers and relies on high levels of trust and confidence in the system. Any change or alteration to the system must maintain the same level of trust. Although it could manifest itself in different methods, trust is a prerequisite for any lasting change to the financial market. Lack of trust and confidence in the market, including its structures, procedures, and participants, will have monumental and disastrous effects (Brainard, 2016).

Embedded within the permissioned or permissionless issue is the concept of trust. Rather than maintaining a designated or central party to control the trust, the entire network becomes responsible and fulfills that role (ROBEKO, 2016b). Distributed ledgers establish trust through cryptography and consensus. A low trust environment requires higher degrees of consensus, which becomes increasingly difficult as more participants are within the network (Deloitte, 2016).

Permissionless systems maintain a trustless mentality. The open and unauthenticated access will remain true and honest so long as a majority (over 51%) of the network running the ledger or blockchain remains honest. Conversely, a permissioned system exerts varying levels of

trust when it limits those able to see and/or verify transactions (DTCC, 2016). The concept of trust is important as it contributes towards levels of transparency as well as the reduced need for third parties (Hinkes, 2014). Information distributed among numerous nodes lends towards credibility of information during subsequent comparison and verification of the established ledger (DTCC, 2016).

Distributed ledgers provide transparency through their permanent and public record, elimination of third parties, and improved transaction and ownership histories (Brainard, 2016). The distributed and verifiable features extend to the transparency of information. High degrees of transparency are welcome though it calls into question privacy of individuals, information, and transactions (Government Office for Science, 2016).

ROBECO stated that the transparency and trust afforded through DLTs have the potential to reduce fraud, misuse of identities, and other potential fraud-related risks. The theory is that the DLT will only accept verified transactions. Given the widespread and distributed nature of the ledger, the system will reject fraudulent transactions or attempts to change information. The result is a complete and honest history that all can trust (ROBECO, 2016b).

**Immutable transaction history.** All transactions must achieve a consensus for inclusion onto the ledger. The consensus algorithms subsequently transfer information across all nodes of the ledger, creating an immutable transaction history. Real-time updates transfer information across the network upon each new verification. The process creates accountability among the participants. Further, all additions to the ledger are permanent (ROBECO, 2016b).

While the process creates accountability and a permanent transaction history, the ledger's underlying structure can permit adjustments. Restricted and permissioned ledgers can create a



system wherein the ledger can reverse specific transactions if necessary. This reversibility is unlikely in a permissionless or unrestricted system (ECB, 2016).

### **Examining DLT Attributes**

DLT presents itself with benefits, limitations, and unknowns. It is a huge investment of an immature and currently non-regulatory compliant technology. There is a push to integrate DLT on an already functioning system (Brainard, 2016). Certain DLT benefits already exist in today's current systems (DeRose, 2016). There are many benefits seen as motivating factors to further investigate and develop the technology. Other benefits could exist in today's system, but do not because of regulatory constraints (WFE, 2016). It is too soon to tell if the technology can adequately address the market's current problems and inefficiencies, and whether it is worth the time and resources to invest towards developing DLT (ECB, 2016; WFE, 2016).

**Distribution and replication of data.** The decentralized nature of the technology offers potential to increase efficiency and reliability across the network. All nodes within a particular ledger are subject to the same programming and codes, thereby following the same rules and validation protocols to verify and store data. The ledger distributes the same information across all working nodes, keeping the information distribution up-to-date. Localized outages will not affect the consensus validation process across the network (DTCC, 2016). A decentralized structure can also prohibit fraudulent transactions or the distribution thereof. The consensus verification protocols will reject inappropriate information. It is unlikely that a single user will be able to hack into, or otherwise compromise a majority of nodes on the network; thereby reducing the ability to alter previously entered data or introduce and disseminate inaccurate information to the entire ledger (ROBECO, 2016b).

The distributed nature of the technology may allow businesses to recover quicker from large or centralized system failures. All nodes across the network are involved in the system's maintenance. Recovery efforts will involve fewer data losses as there are numerous nodes within the network, acting as widespread backup (SWIFT, 2016). While the distribution creates redundancy of information and records, this redundancy provides resiliency should the ledger face outages, system compromises, or other functional disruptions (ECB, 2016).

Shared information reduces the impact of potential information outages while also increasing its availability to numerous parties. This directly contrasts today's structure. Centralized data is problematic in that it may not be fully accessible and a localized outage could inhibit or prevent access and use. The current structure also tends to have latency issues as it relates to the recordation and dissemination of information. The result is that different groups might be working of different data sets (SWIFT, 2016).

Distributed ledgers will experience problems when there are network communication issues, such as latency in information distribution. The technology allows for real-time updating and dissemination of information; however, instances occur when there are data inconsistencies among the various nodes, leading to bifurcated or forked data. In these instances, the network holds ledgers with differing transaction histories. At present, the network needs to consider how to addresses this bifurcation, how does it determine the accurate and appropriate information, and what steps are available to rectify the discrepancy. The industry is currently testing methods to address and correct this issue but it remains a limitation (SWIFT, 2016).

**Costs and maintenance.** Reduction of costs, time delays, and settlement risks are appealing to the financial marketplace (Brainard, 2016). The WFE stated that DLT's benefits have the potential to simplify, standardize, and increase efficiency in today's market. The

technology can increase cost savings while reducing operational risks. Enhanced efficiency encompasses a variety of factors, all of which contribute towards a company's bottom line. Such factors include reduction in errors from manual data entry and reconciliations, reduced transaction times, improved authentication methods, and stronger data integrity and system resilience (WFE, 2016).

DLT functions without requiring paperwork or other typical back office functions. The absence of paperwork reduces the potential for data entry errors thereby ensuring increasingly accurate data histories. Distributed ledgers can lower personnel and administrative costs, as the program will subsume these responsibilities. The program will perform these functions with reduced mistakes or errors. Companies will require less administrative staff to fulfill these obligations (ROBECO, 2016b). Companies will be in a position to use these savings on new projects, developments, or other improvements efforts (Wilkins, 2016).

Nonetheless, any potential cost reductions in personnel may be offset with the increases in information technology (IT) costs. This technology has large implementation and maintenance costs, as the technology requires incredible computing power and energy, storage space, and speed (ROBECO, 2016b). In addition to the costs associated with the ledger's continual administration, computing requirements and costs will increase over time due to the permanent recordation of transactions: the database will continue to grow. Companies using the technology will likely need to increase both their storage and bandwidth capabilities, thereby potentially increasing overall costs (SWIFT, 2016). DLT offers the ability to reduce personnel and administrative costs, yet it will require changes to current systems. These changes, including starting and maintenance costs are both drastic and cost intensive and may prove to be prohibitive in the long term (Shubber, 2016).

**Integration.** Integrating technology with legacy systems presents a challenge. Extensive standards can ease implantation both across platforms and within legacy systems. The distributed ledger must incorporate older transactions, while the new system maintains new data. Otherwise, there remain two sets of records, which inefficient, time consuming, and leads to similar issues currently facing the industry. Segregating only specific business units to use distributed ledgers can be problematic, inefficient, and duplicative. However, this issue may become less significant as DLT's become thoroughly integrated into the business' practice (ROBECO, 2016b).

**Immutability and permanency.** DLT must evolve to include protocols to deal with errors and mistakes (WFE, 2016). The current system requires transaction delays to allow a company time to reverse or correct errors or mistakes (DeRose, 2016). Laws require that companies maintain the ability to undo or cancel fraudulent or erroneous transactions. The DLT permanently records every transaction, with limited ability to eliminate or tamper with validated transactions. Having the ability to adjust the ledger to account for mistakes and errors calls into question the immutability and permanency of the technology (Johnson, 2016).

**Trust.** The current financial marketplace functions on trust, relying on third party intermediaries to confirm asset ownership and provide authorization for subsequent transfers. This trust is an essential and required feature. In a distributed ledger system, the technology itself acts as the third party intermediary. The automatic and distributed information updates creates an agreed upon transaction history, providing the requisite confirmation of ownership and authority. The technology will only permit transactions from allowable parties. In doing so, it subsumes the function of the third party intermediary of confirmation and authorization of transactions (Brainard, 2016).

**Efficiency.** SWIFT highlighted several benefits DLT brings to the financial marketplace. Such benefits include exact replication of data across all nodes of the ledger, efficient distribution, traceability of transactions, real-time updates and changes, simplified reconciliation, and authenticated and validated data. These benefits create a trusted system that is highly resilient and durable (SWIFT, 2016).

Today's financial market faces limitations due to its structure and imposed regulations. The system operates in distinct and separate environments with limited communication and duplicative information. These features create a complex environment with the potential for inconsistent and stale information. Further, the structures are not capable of handling or combating today's security issues and cyber threats, potentially leaving data subject to compromise. DLT addresses those concerns, as it is a rule-based program with built-in features to address current security and data integrity concerns (DTCC, 2016).

Current systems and structures operate in silo environments. These silos often have different processes and recordation practices, which can prevent or hinder interoperability between data and business units. Conversely, each transaction and addition to the distributed ledger requires a sequential consensus validation, shared across the entire network. The resulting transaction history provides proof of ownership without conflicting versions of events (ECB, 2016). This technology gives a wider group of market participants the ability conduct transactions directly with each other. The transaction pattern, described above, enhances the immutable transaction history while also providing transparency into the market. Cumulatively, this process eliminates the need for a trusted third party (Brainard, 2016).

Digital Asset, a company focused on building processing tools and enhancing settlement efficiency and security, described the current financial marketplace and system as inefficient on

several levels. Legacy structures require expensive maintenance and rely on duplication of voluminous data. This replication increases the chance for errors and “incongruences within and across those systems create inconsistent transaction data” (Digital Asset, 2016, p. 4, para. 2). Legacy systems are vulnerable to cyber-attacks and are susceptible to increased operational and counterparty risks. A legacy system is redundant and subject to delays in recordation as well as uncorrected and unidentified errors. In contrast, DLT provides a more efficient infrastructure, one wherein cryptographic keys will secure data and distributed ledgers will increase reliability (Digital Asset, 2016).

**Accountability and accessibility.** Current regulations require accountability, trust, and transparency, though consumers may not fully appreciate or understand these demands and requirements. Regulated systems require protections and security of data, as demonstrated through limiting permission to access specific datasets and systems. It is difficult to determine whether the open source nature of DLT will provide the required protection and limited access. Permissioned ledgers take steps to address these concerns; however, it is too early to tell whether it goes far enough. Until the technology can adequately address those concerns, the marketplace needs trusted third parties to guarantee identity, ensure accountability, and facilitate claims processes and limit data dissemination (SWIFT, 2016).

Restricted ledgers limit the number of participants allowed to access and verify data. In doing so, it limits the ability for unknown intrusions or attacks. Attacks from within a restricted system are identifiable, enabling the system to maintain accountability. It is more difficult to maintain accountability in an unrestricted system as there is no incentive to follow the rules. An offender’s identity remains hidden, making it harder to enforce rules, compliance, and accountability (ECB, 2016).

Data contained within the ledger will be public and available for those with permission to view the system. Yet, this public data can create privacy concerns by disclosing potentially confidential, private, or proprietary information (Brainard, 2016; Digital Asset, 2016). The DLT creators and users must establish guidelines to denote differences between sharing public information and withholding private information (Brainard, 2016). There needs to be a method of information transfer while retaining privacy. The financial industry must find a balance between privacy and transparency. The industry also needs to investigate compliance issues to understand how DLT can appropriately address those issues (SWIFT, 2016).

**Standardization.** Causes of concern include the technology's undeveloped status, integration with legacy systems, standardization, developing protocols and regulations, and large capital requirements (Brainard, 2016). The technology also presents limitations with data retrieval and analytical functionality as well as the inability to handle or reverse errors and mistakes. In today's heavily regulated financial marketplace, companies, governments, and other market participants must address these features and functions and reach a consensus in order to move forward (DTCC, 2016).

There is concern that the lack of standardization, and therefore adaptability, will inhibit further innovation and development. ROBECO (2016b) suggests the creation of consortia to address these issues. Global standardization faces its own challenges. Before creating rules, the industry must determine the group(s) responsible for setting the standards as well as the group(s) responsible for enforcement. Once determined, the next issue becomes how to reach a consensus on the standards and whether it should be from cooperative efforts or competition (WFE, 2016). Given the global nature of the technology, developers and users must also consider and account

for potential cross-jurisdictional barriers such as competing or conflicting privacy or transaction laws (DTCC, 2016).

Industry working groups are collaborating in an effort to achieve DLT's potential, which includes discussions regarding its DLT's challenges. Standardization is one of the larger issues facing DLT. For it to reach its potential on a global level, users must agree and follow core standards and procedures (WFE, 2016). Inclusive of those standards are technical protocols, data formats, contract terms, and execution agreements and arrangements. Companies may unwittingly create systems in isolation to current business standards, resulting in incompatible systems. For DLT's to achieve full potential, it should become operational among all platforms (SWIFT, 2016).

**Regulations.** Regulatory hurdles are the technology's biggest obstacle (ROBECO, 2016b). Any advancement of the technology requires reviews and analyses of legal risks, data privacy, individual privacy, and security (WFE, 2016). There are discussions of the technology's current status. However, there needs to be a discussion of its future, including the information contained therein (Brainard, 2016; Digital Asset, 2016). While DLT is expanding services, it also needs to account for AML and KYC mandates (WFE, 2016). DLT purports to present a pseudo-anonymous environment, wherein identities are not readily apparent. Current regulations prohibit this type of structure in regulated businesses, as it goes against transparency and traceability (SWIFT, 2016).

Distributed ledgers require businesses to adjust current or establish new business plans, including shifting efforts to obtain and maintain appropriate IT structures, systems, and support. It also requires regulatory approval on a global scale (ROBECO, 2016b). The current legal status of the technology is questionable as is its enforceability. The financial market place needs to



address these issues and others prior to widespread implementation (ECB, 2016). Although regulated companies are limited in current use models, unregulated market areas may be able to move forward with developing and applying DLT (Digital Asset, 2016).

**Unknowns.** The technology is in its early developmental stages and lacks significant testing and real-time verification and application (ROBECO, 2016b). The current system offers stability, traceability, and reversibility as needed and required. DLT has yet to prove its capabilities in these regards. It remains unproven in widespread applications, and faces infrastructure and scaling limitations. Further, it will be difficult to integrate into today's current system (D'Antona, 2016). Developers and users must address issues related to governance, data controls, standardization, security, cyber defense, reliability, and regulatory requirements before DLT can become fully integrated (SWIFT, 2016).

There are problems with adopting this technology too quickly or too early. It is in the developmental stages and it is too early to determine its full potential. It will take years before the technology does reach its full potential, whatever that might be (Brainard, 2016). The technology needs clarification on its legal terms and conditions prior to widespread adoption. As it stands today, it cannot completely replace all features of the current financial marketplace (ECB, 2016).

### **Current Trends**

DLT is in the early stages of development and is an intricate and complex technology. There are many factors for consideration, discussion, inclusion, and exclusion as the technology develops (ROBECO, 2016b). Features and capabilities that focus on both current and future needs will be the most effective and efficient use of technology and current efforts (DTCC, 2016; Government Office for Science, 2016; ROBECO, 2016b).

The financial industry's needs and demands vary from its consumers. Companies face different burdens and regulations than their customers. Customers might not be aware of comprehend those differences. To move forward together, there needs to be a balance between each side's expectations. SWIFT discusses eight criteria to examine and explore before industry-wide implementation of the technology, as highlighted in Figure 4.



*Figure 4.* Key requirements to obtain industry-wide acceptance and usage. (SWIFT, 2016).

The OCC believes that fintech innovation, including DLT, can encourage more products, provide wider and nondiscriminatory access to a currently under- and unserved communities, and fulfill other market place needs. While it is important to know and understand the risks associated with any innovation, risks alone should not impede or otherwise inhibit technology's

progress. Thomas Curry, the Comptroller of the Currency stated that “effective risk management is essential to responsible innovation” (OCC, 2016, p. 1, para. 6).

Financial market participants are investigating how to best utilize DLT in their business practices. These participants are devoting time, money, and other resources to explore and develop the technology. Companies appear to be practicing the technology on in-house systems rather than live market situations as there are too many concerns and issues surrounding the live markets (WFE, 2016). Currently, companies require and utilize various parties to establish and maintain its books and records. The use of multiple parties can be time consuming and provides possibilities for increased mistakes, errors, or other inconsistencies as well as duplicative books and records. There is also a delay in the dissemination of information or, in certain circumstances, an inability to share information (ROBECO, 2016b).

The potential applications for DLT are promising, especially those outside of cryptocurrencies (Wilkins, 2016). For instance, DLT can create a method for direct asset transfer without the need for third party intervention. In order to do this, there must be a secure exchange, free from multiple transfers of the same asset, and up-to-date and verified ownership record. DLT’s structure and functionality provides such an environment (Brainard, 2016).

**Smart contracts.** One of the emerging DLT developments is the smart contract. A smart contract is a computer program that acts as an autonomous, self-functioning, and self-executing agreement between parties (Johnson, 2016; ROBECO, 2016b). Smart contracts are independently controlled and executed based on predetermined inputs. The automation aspect reduces the need for third party intermediaries. Outside parties are unable to alter or otherwise interfere with the transaction (Digital Asset, 2016). The result is the transferring of value between the parties (Johnson, 2016). The terms of a smart contract can vary greatly. As with

DLT generally, smart contracts are developing over time. As the technology advances, these contracts will become more complex, while retaining their autonomous virtue (ROBECO, 2016b).

Smart contracts can lead to increased savings in administration, personnel, and transaction fees. It reduces the need for record keeping obligations as the contract contains the history of the terms, conditions, validation, and execution within the contract itself. The data is stored within the program. There is a reduced need for an individual to follow up and execute the terms of the contract because the contract functions on its own. However, this requires a system specifically set up to allow for such automation (ROBECO, 2016b).

Smart contracts can also handle trade financing. The traditional system is a paper-based system vulnerable to errors, mistakes, fraud, and other risks. However, the smart contract's underlying technology creates an immutable transaction history. This leads to a reduced potential for input errors and fraud while also easing the time restrictions and delays within the reconciliation process. Industry experts estimate that DLT can reduce operational and compliance costs by 10% to 15% while increasing a bank's revenue by approximately 15% (Lambert, 2016).

**Asset and trade settlement.** DTCC defines financial asset sales as contracts between parties within specified rules and agreements. A distributed ledger is an optimal recordation method for a variety of asset sales and trades because the transactions follow defined rules. Rather than sending data to different systems for validation and verification, the DLT performs the verification itself, within the system. This simplified process saves time and resources in an otherwise complex system (DTCC, 2016). This method of verification creates tracking

capabilities and assists with audit functions. Holding reference data for securities and other transactions also improves auditing and accountability functions (Morgan Stanley, 2016).

However, there are obstacles to this process. There is a current lack of industry-wide standardization regarding these settlement rules. It also faces competing regulatory and legal battles between different jurisdictions. Distributed ledgers currently are set to provide information to all nodes within the system, regardless of region or location. This could present problems in a highly regulated environment if the ledgers and information contained within cross jurisdictional boundaries (DTCC, 2016). Others view DLT as incompatible with trading platforms, stating there will always be a need for centralized price formation and execution functions. Exchanges perform numerous transactions, all of which require data movement. Increased data movement, as would be required in a distributed ledger environment, will increase overhead costs and potentially hinder transaction speeds (Deloitte, 2016).

Some firms desire to create same-day settlement processes and procedures, believing that it creates a more efficient settlement model versus today's model, in which settlement occurs over a several-day period. As previously referenced, the current settlement period exists per regulatory conditions and legal constraints. The current settlement structure also provides more market liquidity as well as the ability to make adjustments or corrections when necessary. The proposed same-day settlement time might not work in today's market; however, DLT can provide the ability to establish particular settlement procedures for different contracts or sets of circumstances. Firms are looking to explore and expand on this concept of adaptability for settlements (Morgan Stanley, 2016).

**Banking industry.** DLT can provide benefits to the banking sector. Payment methods and transfers require a high degree of trust. A distributed ledger can act as a form of escrow,

removing the need for a third party intermediary and facilitating the transfer process (ROBECO, 2016b). In addition to the decreased reliance on third party intermediaries, the comprehensive transaction history and immediate distribution thereof further enhances transparency, privacy, and security (Brainard, 2016). Payments made through a distributed ledger could decrease transaction delays and costs, facilitating both intra- and international payments (Morgan Stanley, 2016).

Banks are keen to utilize DLT in an effort to reduce costs. The automated features would facilitate cost reduction efforts. However, the industry is facing problems in this regard. While DLT appears immune to systemic system failures and other compromises, other promising features are problematic. The transparency DLT provides to the market poses problems to both customers and competitors. Customers may no longer be anonymous. Banks may reveal secretive or proprietary information, which others could act on to the detriment of the institution (Shubber, 2016).

In 2014, R3 formed a working group with nine global banks. The purpose of their work was to explore DLT in terms of its structure and use cases while also exploring regulatory limitations. R3's goal was to use DLT to allow banks the ability to honor a variety of agreements between and among each other. It originally invested in architecture, use cases, and regulatory and compliance issues. It maintained technical labs that worked towards finding solutions and facilitating cooperation, research, and development. Currently, R3CEV, a 40-plus member global consortium, is furthering that mission by working on various DLT-related products, services, and other innovations (Del Castillo, 2016).

**Other uses.** Outside of the banking and trading environments, governments are looking towards DLT as a means to improve efficiency. The United Kingdom Government Office for

Science explained that DLT, when properly applied to address privacy and security concerns, offers a variety of benefits and enhancements to government operational procedures. Such improvements include a reduction on fraudulent payments, increased protection of information, increased government transparency, support for economic growth, inclusion of currently unreachable citizens, and better management of government contracts. The technology can directly address certain government practices while others areas require enhancements and additional development outside the technology (Government Office for Science, 2016).

DLT can also enable better tracking of business, registration, property, and identity information. Estonia currently uses DLT to allow its citizens to vote, file taxes, and apply for government benefits. Its businesses can file required reports and annual filings and apply for licenses. The Estonian government sends secure communications and interacts with its citizens in the above-mentioned scenarios using DLT. The technology provides a secure and verifiable record of information, which cannot be compromised, at least not without notice. The open and reliable information structures and systems create accountability to its citizens, which is something governments should strive for (Government Office for Science, 2016).

The Defense Advanced Research Projects Agency (DARPA), a branch of the U.S. Department of Defense, is exploring the use of blockchain to secure data. It is also considering the blockchain for tracking nuclear weapons and other military operations. DARPA hopes to rely on the permanent and immutable transaction history in an effort to identify any potential system compromises or hacks. Military information is highly sensitive and it is imperative to maintain data integrity. DARPA is investing resources to determine whether blockchain will provide the required and desired level of security (Wong, 2016).

Uses beyond government and military applications include tracking asset ownership, such as diamonds, real estate, or stocks. DLT could also benefit entitlement registers, such as copyright ownership, personal licenses, and business registers. The technology can act as evidence to agreements, warranties, insurance arrangements, or contracts, similar to the smart contract though extending beyond a singular agreement (Deloitte, 2016).

## **Security Issues**

Technological innovations create both solutions and risks. Before implementation, the industry must be aware of and be able to properly manage those risks (Wilkins, 2016). Firms looking to develop this technology should identify potential risks and propose mitigation methods while still satisfying regulatory requirements. Distributed ledger technology needs to ensure it maintains vigorous security protocols to protect all information, including personal and proprietary information. Financial institutions have high integrity and security standards and must remain resilient under a variety of circumstances. To that end, institutions need to ensure there are safeguards and recourses available should there be a hostile situation (Brainard, 2016).

Research suggests that cybersecurity is a big risk for the financial industry, particularly as it moves towards new technologies. The entire community needs to create and follow grounded strategic decisions and standards to meet consumer needs and regulatory demands. These decisions and standards must fall in line with long-term business objectives and risk profiles. Businesses must maintain a realistic outlook and appropriately address these risks (OCC, 2016). Market participants are aware of these concerns as they identified security as a big concern. At present, there is not enough information relating to real-life scenarios to understand how DLT actually handles theft or fraud (WFE, 2016). The industry needs to work together to develop best



practices, safeguards, and controls, all in an effort to increase security and other protections (Johnson, 2016).

The distributed feature of the technology makes the entire system harder to attack. However, there techniques available that can bypass security (Government Office for Science, 2016). The technology relies on the concept in information integrity, which centers on data owners knowing when anyone has viewed or modified the system or data within a system (Wong, 2016). Data and information security is very important. At its core, the goal is to protect data, including its users, from unwanted attacks and/or intrusions and reduce the potential for unauthorized information use (Gelbstein, 2011). A distributed ledger will track any attempt to access or modify information within a system. This tracking will provide system owners the transparency to detect those intrusions and trace an intruder's steps (Wong, 2016).

As an open and unrestricted system, DLT will not easily integrate into the current financial system. The original blockchain design was strong against cyber threats due to the open and availability of source code as well as the available cryptography. Due to the potential for malicious actors, the technology incorporates encryption features to create a fraud-resistant system. However, this does not easily transfer into the larger financial community. In order to protect customer and other private information, the system requires numerous forms of encryption. Though protecting information, these multiple levels of encryption and decryption create a logistical impasse and may inhibit authentication and verification protocols. It also demands intense and expensive computer power and capabilities (SWIFT, 2016).

By definition, DLT distributes information across multiple nodes within a network. This distribution provides resiliency and data integrity should there be a localized compromise, hack, or failure (Digital Asset, 2016). Should an attack occur, the system could recover with minimal

data losses as the various participating nodes provide a comprehensive backup. However, this requires uniform obligations for system maintenance. All participants must adhere to the same accountability rules and security protocols. Therefore, each node relies upon network-wide cooperation and uniformity. Programmers should develop these new systems as though they will be hacked or somehow compromised. The technology must know when there are flaws, compromises, or intrusions into its normal functions. This requires constant monitoring, testing, updates, and system improvements. Having multiple nodes and points of entry may exacerbate potential issues and complications as each entry point must follow the same monitoring and updating procedures. Currently, there is no single body or group to enforce security compliance across the network (SWIFT, 2016).

Blockchain, including cryptocurrencies rely on complex mathematical problems to ensure security. While there are different encryption schemes available, much of the research focuses on only limited techniques. Further, those techniques appear to be contradictory: the methodology of one encryption method has the potential to undermine another methodology. There is a false assumption that these mathematical problems are subject to intense examination. The complexity of these problems may actually undermine the touted security. While flaws in the system are by no means a precursor to a hack or compromise; however, it does mean that there are no guarantees Industries need to conduct additional experimentation and investigation into enhancing technology before its widespread release (Koblitz and Menezes, 2010).

The security issues go deeper when considering quantum-computing capabilities. There is a discussion that exposing public keys, as when spending Bitcoin, leaves users vulnerable to security breaches. Regular, at-home computers are not able to violate the public and private key functionality because they are incapable of expending computational power to reverse-engineer

this data. Quantum computers, on the other hand, rely on different algorithms, which can conduct reverse problem solving to determine a user's account, so long as the user expended funds from the account (Buterin, 2013).

Exchange of data is important and typically involves the transfer of personal, sensitive, or confidential data. Disclosure of this information can exploit confidential or competitive data such as trade strategies. Permissioned systems provide controlled and secure access and authorization to a limited group, thereby encouraging confidentiality and limiting disclosures of trade secrets. Permissioned systems are more in line with regulatory demands (SWIFT, 2016).

It is essential that participants, users, and programmer understand the construction of a smart contract and have appropriate means to undo a contract should there be errors or fraud (FE Online, 2016). Smart contracts are self-executing computer programs and have the potential to eliminate friction, decrease costs, and streamline processes. There is also the potential for malfunctions and improper payment distributions. In the case of the DAO Hub hack, a poor code design created a vulnerability, and allowed hacker(s) to enter the ledger and divert funds (Johnson, 2016).

**DLT hacks and compromises.** Security remains an issue with DLT. Recent hacks and unauthorized access resulted in millions of dollars in losses to the public (Johnson, 2016). DLTs have already experienced frauds, hacks, and other system failures that required emergency action. The technology is susceptible to partitions or divisions of information, leading to inconsistent ledgers and data. Further complicating such a situation is the difficulty in isolating impacted nodes without affecting the integrity of the entire network (SWIFT, 2016).

At least 48 Bitcoin-related thefts occurred between 2010 and 2014, with losses exceeding hundreds of millions of dollars (Dree12, 2014). In 2016, at least three blockchain hacks

compromised customer funds, including the DAO Hub. The companies experienced vulnerability in web browser functionality and programming flaws. In each instance, the resolution required that the transaction history roll back prior to the compromise to make customers whole. The blockchain underlying cryptocurrencies purports to be fraud resistant, in part due to the decentralization of data. However, as demonstrated through the 2016 hacks, there are still unknowns about security (KPTX, 2016).

In addition to the DAO Hub hack, Bitfinex also experienced a hack in 2016. Bitfinex is a digital currency exchange, located in Hong Kong. The exchange joined with a bitcoin wallet provider to create a multi-signature system to keep customer funds segregated and protected. The customer, exchange, and wallet provider each held the keys necessary to conduct transactions. In August 2016, Bitfinex disclosed it experienced a theft of approximately \$66 million USD. The details of the hack, including as how it happened, who is to blame, or the extent of impact on other exchanges, remain unknown (Higgins, 2016). It is possible that the company took shortcuts in security protocols and safeguarding information as opposed to experiencing a technological failure (Johnson 2016).

In the days after the Bitfinex attack, the amount of the theft rose to \$72 million USD. The exchange planned to distribute losses among all its customers. In addition to the distribution of losses, the company proposed offering electronic tokens to customers, potentially redeemable as shares in the parent company. Either option is problematic: the first violates the exchange contract's terms and conditions; the second potentially violates U.S. securities laws. Account holders had to absorb the losses with little ability for recourse, as the odds of customers taking the firm to court to obtain a judgment are low (Reuters, 2016).

## **Consumer Protection**

DLT requires additional developments before any industry can rely on it to hold personal and confidential information. At this time, the system's capabilities remain unknown and, therefore, lack trust to protect such sensitive information. The distributed nature of the technology does not preclude it from threats or attacks. The centralization or decentralization of information plays no part in the potential leak or hack of information. The underlying information makes it vulnerable to a compromise (DTCC, 2016). Only a permissioned and restricted ledger can begin to offer the security and protections that AML and KYC laws require (Morgan Stanley, 2016).

**AML and KYC.** In the development of global standards and procedures, users need to account for localized laws such as AML and KYC policies. Typically, AML and KYC protocols are time intensive and expensive, requiring weeks to obtain information from various sources. Different institutions conduct similar background checks on overlapping customers. Each investigation takes time, could yield different information, and requires updating. Proponents of the technology stated that an AML and KYC DLT could replace redundant paperwork and research. A DLT could ease background investigation procedures by maintaining a decentralized database of all customer information across institutions. This would eliminate the need for multiple and redundant background checks. An institution could merely go to the ledger to obtain specific information. Given the decentralized data of the DLT and its reduced likelihood of compromise or attack, consumers' information would be safer and less prone to theft or other fraud. This in effect could actually reduce the burden on regulators while also increasing business efficiency (ROBEKO, 2016b).

The current distributed ledger does not require a central point of authority or regulation to operate. However, "... it does need the regulator to allow for the legal usage of the technology" (ROBECO, 2016b, p. 19, para. 3). A DLT of AML and KYC data can potentially create a system outside regulatory boundaries, though its users must still account for AML, KYC, and other cross-border laws and consumer protections. There should remain a point of contact for consumers with questions or concerns in addition to accountability for AML, KYC, and other consumer-related laws (ROBECO, 2016b).

**Accountability.** The financial marketplace needs the ability to account for mistakes, errors, or fraudulent transactions (DeRose, 2015). In the case of the DAO Hub hack, a user found a flaw in the software code, using it to their advantage. The smart contract's code ran precisely as programmed yet it yielded an unintended outcome of customers losing millions of dollars. There remain unknowns about this system compromise, including whether or not these actions actually constitute a hack or compromise as the DAO Hub lacked a predefined purpose. The argument is that the diversion of funds technically did not violate the system's rules, as there were no rules to violate. At the same time, the DAO Hub's underling platform considered altering its rules in an effort to return lost funds to customers, though it would require the platform's consensus. In this instance, customers had no central authority in which to complain or seek assistance (Sayer, 2016).

## **Looking Ahead**

It is unlikely that DLT will entirely replace the current system and structure. There remains a need for trust, intermediaries, and monitoring (Wilkins, 2016). While DLT may alter the system in some way, the overall structure will likely remain intact. There are several factors for consideration before complete optimization, as well. The financial community needs to

consider whether the technology is applicable across all asset classes and industries. Prior to that, it must first examine and practice the technology on small use cases. There is much to learn in controlled environments (Brainard, 2016).

Properly implementing any new technology, including DLT, will take significant time. Successful implementation requires in-depth discussion regarding governance, transparency, reliability, and security (Government Office for Science, 2016). The global aspect of the technology does present problems in terms of regulations. Jurisdictions hold different rules, regulations, and laws as to allowable transactions and information sharing. DLT operators need to be careful so as not to conflict with various jurisdictions (DTCC, 2016). Collaborative efforts similar to the International Organization of Securities Commissions (IOSCO) could assist by establishing global standards that consider regulatory obligations and ensuring the mandates are not contradictory (WFE, 2016).

Currently, changes and developments are happening in under- and un-regulated fintech companies and markets. It would behoove all participants to work together towards maximizing DLT's potential. Smaller companies may have more talent and novel approaches whereas larger institutions have more financial capital for research and development. Working together can increase capabilities and enrich developments, particularly when coupled with increased communication between participants and regulators (OCC, 2016).

DLT has potentially unlimited uses and applications (Hardy, 2016). To-date, efforts to move forward remain uncoordinated. Moving forward in public and private partnerships can improve efforts. Without that coordination, businesses are at risk of repeating past mistakes and creating new silo environments (D'Antona, 2016). It is inefficient to use such technology in older and outdated systems. To do so will only reinforce a broken system (DTCC, 2016).

Adaptation will require changing business models and operations to fall in line with new standards and protocols (ROBECO, 2016b).

### **Discussion of the Findings**

This project's objective was to discover information regarding DLT with a specific focus on determining best uses, security vulnerabilities, and methods to mitigate fraud within the financial marketplace. Industry whitepapers revealed that there is much excitement related to DLT exploration within a variety of market sectors, including the financial marketplace. Governments and private sector firms have taken incredible steps towards exploring, understanding, and developing the technology. Establishing consortia and working groups to enhance developments reveals a clear indication of the support for the technology within the financial sector and beyond. While there are limited considerations related to security and fraud and it is too soon to know DLT's full impact, the technology appears promising (WFE, 2016).

Current DLT research is unprecedented and uncoordinated. There is much to learn about the technology and its potential (DTCC, 2016). The technology continues to evolve as its exploration expands. This process will provide answers and raise more questions as it reveals new strengths, as well as unknown capabilities and vulnerabilities (Miller, 2016). There remain many questions regarding DLT's capabilities and constraints, with both considerations essential for discourse (WFE, 2016). As mentioned, the potential unknowns should not inhibit innovation but rather drive efforts forward to maximize the technology's potential (OCC, 2016).

### **Promising Features**

There are progressive features to DLT, such as the immutable and traceable transaction history. It will provide a log of which, when, and how users accessed the system, including any unauthorized access. Using this history system administrator(s) will be able to hone in on the



accessed sections as well as identify the types of information. This specificity is valuable as it can direct ledger owners to system vulnerabilities in addition to highlighting sensitive or at-risk information. Such knowledge can alert those areas that may require additional safeguards (Wong, 2016). With numerous and stringent regulations regarding financial transactions, it is probable that initial enhancements and developments will occur outside the financial sector (WFE, 2016). One example is DARPA's investment into investigating blockchain technology to secure specific military information. In this environment, data integrity, such as detection of tampering or unauthorized access is critical (Wong, 2016).

The military's consideration and research into the technology will be very good for the technology, should the results prove positive (Wong, 2016). Use cases such as this will allow for freer exploration of the technological strengths and drawbacks. Additional use cases and studies outside the financial sector will further illuminate the technology's functionality, with discoveries further enhancing and expanding the overall knowledge base. This knowledge will be applicable and transferrable to other market sectors, to determine the best uses and applications of DLT (Digital Asset, 2016; OCC, 2016).

The technology presents itself as capable of facilitating a variety of financial transactions as well as contracts. Financial firms and customers preset varying demands and needs (SWIFT, 2016). Exploration and development of the technology will facilitate the creation of new products and services for both financial firms and customers (WFE, 2016). Smart contracts are a promising use of the technology. These contracts will function autonomously and execute contractual obligations without third party interference (Digital Asset, 2016; ROBECO, 2016b). Apart from smart contracts, the technology can also help with asset recordation and trade settlement. The financial industry is looking for methods in increase adaptability and efficiency.

Employing a computer program that will automatically perform back-office functions while potentially reducing errors is one means of increasing efficiency (DTCC, 2016; Lambert, 2016; Morgan Stanley, 2016).

### **Inconsistencies**

Despite these efforts, there remains much to learn about DLT. Available research presents both positive and negative information. The research also presents inconsistent information. Varying sources will address single points of view on any given topic without analysis or reference to alternative perspectives. For instance, competing sources suggest that either DLT will decrease or increase operating costs. Each reporting source focuses on different aspects of business operations to support their claim: administration and personnel costs versus IT costs. Costs associated with the former category may decrease while IT infrastructure and operating costs will increase (ROBECO, 2016b; WFE, 2016). Those utilizing the technology will need to conduct cost benefit analyses to determine the appropriate path for their business needs (Brainard, 2016; Shubber, 2016).

Another inconsistency within the research is a general inability to segregate dialog regarding protocols, security, and capabilities per system structure. Restricted and unrestricted systems operate under different criteria and expectations (ECB, 2016). Each system offers different strengths and may be better suited in different scenarios (Government Office for Science, 2016). The research indicated that restricted systems provide more features that are in line with financial regulatory requirements, due to the level of control and limited access (Digital Asset, 2016; SWIFT, 2016). Additionally, the defined authority associated with a restricted system provides and facilitates the capability to reverse transactions or address other errors or

misconduct. These are important distinctions and requirements when considering DLT's feasibility within the financial sector (ECB, 2016; SWIFT, 2016).

**Terminology.** What appears to be a widespread recurrence within the research is the inconsistency of terminology, most noticeably with the terms blockchain and DLT. Authors tend to use the two terms interchangeably, despite having different meanings (ROBECO, 2016b). It is increasingly challenging to define specific terms related to the technology, particularly blockchain (Stafford, 2015). As discussed, blockchain is a type of DLT. It is the most recognized form but it is not the only one. However, news articles and research alike often fail to make a proper distinction with the introduction of DLT and subsequent conversation of blockchain (Del Castillo, 2016; ROBECO, 2016b).

Another misconception lies within the technology's open nature. There is an important distinction between a system having an open source code and information being openly accessible. Maintaining open source code refers to the availability of the underlying program and code, whereas open accessibility references an unrestricted nature of the technology. Open accessibility of information, as seen in unrestricted systems, presents less control and accountability. Additionally, there are likely fewer obstacles in accessing data (DTCC, 2016; ECB, 2016; ROBECO, 2016b). Establishing the appropriate systems in terms of openness and availability will provide specific systems the ability to find unique marketplace venue to meet varying needs (Government Office for Science, 2016).

**Technology.** Immutable transaction histories claim to be a permanent recordation of transactions. However, as the ECB explained, that is not necessarily true for all distributed ledgers. A DLT structure can allow for data alterations, adjustments, or even reversals. In a restricted distributed ledger, the owner(s) establishes the ledger setup, including the potential for

reversing of transactions. The ledger can also allow for instantaneous or delayed verification protocols (ECB, 2016). As seen in recent hacks, administrators, if available, offered to make such an adjustment. Unrestricted systems lack that direct authority to make such a reversal, instead requiring a majority consensus to adjust the ledger (Johnson, 2016; Stafford, 2015).

### **Limitations of the Research**

The information examined indicates that many industries support this technology and are making efforts to incorporate it into business practices. At the same time, there is still much work and examination to conduct (SWIFT, 2016). There are not enough use cases available within the financial sector to allow for widespread integration therein, especially considering the extensive regulations and oversight. However, the industry is considering various potential uses for the technology, with anticipation of discovering additional potential use cases in the future. There are also public and private groups forming in an effort to confront limitations, identify undetermined characteristics, and progress the technology forward (Morgan Stanley, 2016).

**Security and fraud.** One area requiring additional research involves security, including understanding the extent of software vulnerabilities. Information and data security is a common concern among businesses. At this time, businesses and regulators do not know enough about the technology to address those concerns adequately (OCC, 2016; WFE, 2016). There are broad generalizations regarding DLT and its impenetrable security, including statements that fraud cannot occur within a DLT environment. However, hacks of the DAO Hub, Bitfinex, Mt. Gox, and others are all instances wherein these environments experienced security vulnerabilities, resulting in large-scale fraud and theft of customer funds. The DAO Hub operated precisely according to its code; however, it was flawed code. This programming flaw facilitated a multi-

million dollar diversion of assets, and left customers with little option for recourse (Johnson, 2016; KPTX, 2016).

Ensuring security and resiliency against cyber threats is essential (ECB, 2016). Privacy and security rely on and encompass a variety of factors. While the distributed nature of the technology provides a means to recover from devastating failures and data losses, it also requires extensive and persistent system maintenance, security monitoring, and updates. Data partitions typically do not exist within these systems, meaning that problematic data or comprised nodes have the potential to affect the entire network. Regarding privacy, smart contracts may also disclose information that should otherwise remain confidential. A smart contract acts upon on pre-determined criteria, information embedded within the contract. Such information may include proprietary data. Additional security and protective features are required in order to prevent non-competitive admissions or disclosures (SWIFT, 2016).

DLT systems are imperfect and contain programming flaws (Stafford, 2015). Software is vulnerable to programming flaws. If a system's code contains a flaw or other software vulnerability, it affects the entire system and all participating nodes. While it is possible that restricted systems will inhibit validation of fraudulent transactions, the possibility of programming errors, and thus potential fraud, remains and requires consideration and monitoring (SWIFT, 2016)

Much of the research lacks substantive deliberations on fraud and security. At the same time, other sources provide extensive technical and computer science-based deliberations. These sources are difficult for a non-technical population to consume. For instance, Neil Koblitiz, a professor of mathematics, and Alfred Menezes, professor of combinatorics and optimization provided a lengthy and technical analysis regarding the bold assumptions of cryptography, the

mathematical-based technology underlying blockchain's security. Their paper addresses various mathematical theories of cryptography and debunks some of the theories upon which blockchain claims to be secure. Their paper goes beyond merely providing an overview of security features and fallacies as it centers on complex mathematical theories (Koblitz & Menezes, 2010).

**Immutability.** One of the prominent features of DLT is the immutable transaction history, a verified, unaltered, and uncompromised accounting. Yet, this is not always the case. DLT is a computer code, which is modifiable (Johnson, 2016). In instances of bifurcated data, different nodes within ledger or system hold different data sets rather than maintaining unified information. The result is various access points holding inconsistent sets of data. These inconsistencies remain spread throughout the system until there is a global adjustment to all participating nodes (SWIFT, 2016). In instances of fraud, the possibility and need for a correction of transactions comes to the forefront. In either situation, the solution requires a main authority to address and correct the information across the network. It also requires that the immutable and permanent transaction history becomes impermanent, calling into question one of the key features of the technology (Johnson, 2016; Siegel, 2016).

Immutability is not necessarily a system failure or software concern; however, it does necessitate additional layers and safeguards to battle fraudulent activity or other errors (Johnson, 2016). Today's financial marketplace requires reversibility to account for mistakes, inappropriate transactions, or other inaccuracies (DeRose, 2016). To account for this reversibility, there must be some form or means of adjusting the transaction history. The technology must address these requirements before its integration into the financial marketplace. If the technology is too complex to account for this characteristic, then that must be accounted for (Johnson, 2016).

**Regulation.** There is agreement that DLT is not currently regulatory compliant and that regulations are its biggest obstacle when encountering the financial marketplace. Some of DLT's promising features go against current regulations, such as the pseudo-anonymity of transactions. Additionally, there is agreement that the technology's output may be out of compliance for a variety of reasons, including the potential for cross-border information sharing, privacy and transparency limitations, and AML and KYC requirements, as competing jurisdictions maintain varying levels of privacy and data-sharing laws. Although much of the research addressed regulatory limitations, there is agreement that these limitations should not halt exploration (Brainard, 2016; DTCC, 2016; OCC, 2016; ROBECO, 2016b).

### **Recommendations**

There is extensive opportunity to expand and develop DLT in many market sectors. The technology has the potential to increase efficiency on various levels within and beyond the financial marketplace. While there are limitations to the technology's current usage within the financial sector, those limitations should not hinder innovation. It is important to move forward with research and development efforts, realizing that progress can take significant time. Industries should be prepared to make necessary and appropriate changes, understanding that changes are for the best, and advance with innovation (Brainard, 2016).

No single technology can be a solution for every problem. Any new technology requires additional measures and collaboration to investigate strengths and weaknesses. Having this knowledge will encourage forward movement and provide optimal circumstances for those using the technology. Any changes that incorporate DLT will take time to integrate into today's systems (SWIFT, 2016).

## **Moving Forward**

As the research moves forward, there needs to be an agreement among technology developers and users regarding all aspects of the technology, including acknowledgement and consideration of both benefits and pitfalls. It is equally important to define and consistently use the same terms. In this regard, cooperation must extend beyond a single industry to include input from the major participating industries and technology programmers and users. This will allow for a deeper understanding of the technology and, thus, establish the best and most appropriate means of utilization.

As the technology continues to advance, it will address changing consumer demographics and needs. U.S. government regulators, such as the OCC, are striving to encourage these advancements and developments so long as those advances are regulatory compliant and protect consumers. To that extent, regulators need to be aware of new trends and cooperate with the industry to promote long-term benefits and relationships rather than stifle innovation (OCC, 2016). Non-financial firms are in a better position to enhance the technology as there less regulations with which to contend. These circumstances will create an environment ready for research and create a path from which to move forward (WFE, 2016).

**Consistency.** There needs to be better defined and more consistency used terminology. For instance, much of the DLT research focuses on blockchain, with many consumers associating blockchain with Bitcoin. This collective grouping of terminology needs clarification. DLT and blockchain are related, but are dissimilar. There needs to be stronger distinctions between the vocabulary, including component parts, forms, and varieties of DLT. One way to do this is with a better understanding of the technology. In addition to identifying what the



technology is, the research must include what the technology is not. It is important to remain consistent and cognizant about both the technology's capabilities and limitations.

The system's structure, in terms of its permission level, will determine the functions of various system components. Exploration will overlap between the various components, as the features are interrelated. As presented, restricted and unrestricted systems each rely on consensus validation, decentralization, and transparency but those components will manifest in different ways. Each of these features is limited and controlled in a restricted system whereas an unrestricted system is open and experiences less and control. Grouping all features and functions into one generic system is harmful to development efforts as it limits and misrepresents the technology. Segregating reviews to account for various features within different permissioned structures will aid future communications, understanding, and implementation.

**Use cases.** Use cases will be an effective means to understand the technology and recognize how it works in real-time and real-life scenarios and applications. Working in smaller sets of data and within confined systems will provide for more controlled investigations and exploration. Being able to focus on smaller, defined use studies will provide the ability to understand and fix systems prior to widespread integration. Administrators can track and monitor progress, control functions, and resolve system failures or deficiencies (Brainard, 2016).

Similarly, non-financial firms will further enhance research and development efforts, as there are fewer regulations (OCC, 2016; Wong, 2016). Exploration of systems can continue with limited fear of regulator interference or adverse action. Additionally, specific to the financial sector, technology companies offering these technologies and services may want to avoid subjecting themselves to regulations. Consequently, those technology firms may determine to

offer technical support services rather than become regulated financial marketplace participants, thereby avoiding strict regulatory obligations (Morgan Stanley, 2016).

**Security and consumer protections.** Research efforts should expand to include security and consumer protections concerns. Reported thefts in DLT systems often left customers without recourse. Though some customers reported losses to the Federal Bureau of Investigation or other cyber-crime authorities, not all customers were able to do so (KPTX, 2016). Consumers need clarification regarding recourse after a hack, compromise, or erroneous transactions. Unrestricted systems lack a central authority with the ability to resolve these issues. In the financial sector, firms will focus on restricted systems, as those systems will be able to address security, accessibility, privacy, and other concerns. SWIFT (2016) proposed a central certification authority as a third party whose responsibility includes administration of public and private keys. While having a central authority is helpful for administration purposes or dealing with theft or compromised accounts, it negates the technology's proposed elimination of third parties.

References regarding the potential for fraudulent transactions such market manipulation, misappropriation, embezzlement, or trade-related misconduct is largely missing from the research. Identifying and addressing multiple types of misconduct and fraud within a DLT environment is important for consumer protection. Although trade execution, settlement, and clearing functions do not currently utilize DLT, there is a desire to do so (DTCC, 2016). These areas require intense examination to establish feasibility as well as remedial protocols. This exploration may reveal limitations, especially those centered around the current stance on immutability and reversibility. Those limitations are essential to the conversation of whether and how DLT will fit into the financial marketplace. Equally important is creating solutions and remedies.

Security protocols are not exempt from problems. A programming flaw or software vulnerability in a distributed system affects every nodes within the system, leaving the entire network susceptible. In these scenarios, the distributed feature may not fully negate a hack because every node contains the same flaw (SWIFT, 2016). There are also concerns that small-scale compromises are trials for bigger or more intense attacks (KPTX, 2016). Once a hacker understands the intricacies of a system, the knowledge is available for use in other systems.

There are varying perspectives on DLT's security features, some of which contradict recent headlines. While no system is fraud-proof, there are steps that can reduce the potential. Future examinations should require more in-depth analysis of complex issues, such as cryptography and hashing. Firms creating and relying on the technology must consider these factors and take necessary steps to mitigate potential fraud or theft.

## **Communication**

Throughout the entire research and development process, open communication is essential. All active participants from public and private sectors, including technology developers and users will have a significant role in the technology's development, utilization, and implementation. Communication efforts need to encompass a variety of criteria such as standards, security, and regulation (WFE, 2016). Maintaining open, constructive, and honest dialogue will encourage both marketplace participants and regulators in understanding and implanting the technology.

**Public and private collaboration.** Market participants and regulators need to work together to foster innovation and product enhancements for consumers. In order to do so, there needs to be an open dialogue. Such communication can manifest itself in the form of collaboration among local, state, and international communities. Communication should be in a

cooperative effort to create better performance, expectations, and consumer experiences and protections. The more participants and regulators communicate with each other, the more robust the industry will become (OCC, 2016).

Agreement between regulators and market participants requires not only open communication, but also consistent and prolonged information sharing. The two sides must work together to understand and evaluate developments and create best practices (WFE, 2016). The industry needs to consider and encourage improvement for the benefit of the public while also maintaining the ability to work with and handle law enforcement requests and regulatory requirements such as AML and KYC policies (Brainard, 2016).

As the technology progresses, public and private sectors need to work together to understand analytical frameworks and assess the benefits and challenges associated with DLT. Regulators' objectives include preserving financial stability while maintaining safe and reliable infrastructures. In doing so, regulators will need to understand and address the data in terms of consumer protections, financial inclusion and competition, and market integrity and stability. Guidance must be clear and concise. Additionally, regulatory efforts must be global given the global nature of the technology (Wilkins, 2016).

**Consortiums.** There are multiple consortiums working towards addressing research and development needs and firms are competing to move ahead. There is much interest in developing the technology, which offers a variety of solutions to the financial lace (Del Castillo, 2016). DLT will not provide the ultimate solution to all market problems. However, collaboration among fintech firms can create a product(s) that can facilitate market productivity and processes, while also accounting for legal issues and consequences (SWIFT, 2016).

Established consortiums are currently working to further the technology. R3 and the Hyperledger Project each involve numerous global financial institutions, wherein the associated firms collaborate with and among members to better understand the technology and provide methods of industry-wide acceptance and integration. Additionally, several financial institutions are working independently towards the same objective, including developing internal standards and procedures (Morgan Stanley, 2016). Collaboration will allow for smoother adoption of the technology, while international merit organizations can assist in establishing universal guidelines (SWIFT, 2016).

**Regulation.** Prior to establishing regulations and determining compliance, the industry and regulators need a better understanding of the technology and its long-term impact (SWIFT, 2016). The WFE stresses the need for global consistency and international guidelines. Various international regulatory organizations should work together to develop uniform approaches. Success requires consistent regulation and policies (FE Online, 2016). However, the regulatory issues go beyond any single technological issue. It extends to broader considerations of the current regulatory structure. Financial institutions must provide data when requested. Further, the financial institutions need to access, protect, and secure information at all times. The actual, technical means of doing so are less an issue than the outcome. The community needs to consider whether regulations should extend to incorporate the technology itself or merely continue to regulate firms' obligations regardless of utilized technology.

The financial marketplace should be driving innovation efforts. Simultaneously, regulators need to stay abreast of current market trends and developments. In doing so, they will better understand the new technology, its effect on the market, and how to achieve optimal performance. When they understand the technology and its impact, regulators will be in a better

position to create or modify existing laws and ensure operational consistency (FE Online, 2016). Regulators will not mandate the exploration of technology but rather respond to solutions (SWIFT, 2016).

Features of the technology have the potential to ease and assist regulators' responsibilities and mandates through DLT's ability to provide access to information. While this is beneficial for government processes and functions, it requires high levels of trust, which is currently lacking among regulators (ROBECO, 2016b). Any regulatory considerations should consider whether the adaption of current laws to new technology is more beneficial than creating new laws to address new technology and related concerns. Additionally, there is a question of what aspects require regulation compliance: the technology itself or the firms utilizing the technology. Given the potential cross-border information sharing, consideration must also include which government or entity is responsible for regulation and enforcement thereof (SWIFT, 2016).

**Privacy issues.** Related to regulation are issues of privacy. There is a tradeoff between sharing information and maintaining privacy (Brainard, 2016). Cross-border information presents a problem as jurisdictions maintain competing privacy and data protection laws. Proposed AML and KYC databases, which would hold voluminous consumer information across multiple nodes, provide unrealistic expectations regarding privacy and confidentiality. Further, it is unclear whether such a database would violate domestic and/or international privacy laws. In addition to consumer privacy issues, companies may fall victim to the loss of proprietary information, as the information becomes available to multiple parties.

Financial firms must prepare for system attacks, including intrusions of consumer information. The systems holding customer information, including AML and KYC records, need strong safeguards and security. Unrestricted systems will not provide the required security and

privacy (Morgan Stanley, 2016). The methods by which to provide such security need exploration in order to meet regulatory demands.

## **Implementation**

Implementation into today's silo environment is a primary concern. Siloes often create multiple complications within a company, including independent processes and lack of information sharing. Legacy systems may present problems for those attempting to integrate distributed ledgers. Companies should be cognizant that new technology can create or further emphasize existing silo environments. One way to prevent this is to start with small-scale use studies. Companies can begin using the technology within small sections of its processes, expanding to new business units while observing and correcting when problems arise. Through this process, management can determine the technology's feasibility as well as whether these new systems are reinforcing dysfunctional habits (Brainard, 2016).

Companies that do not take steps to ensure correct implementation run the risk of repeating history (DTCC, 2016). However, firms are attempting to create tools that will assist in efficiency, transparency, and security. These new tools are attempts to upgrade current systems rather than replace them, while solving current problems instead of creating new ones (Digital Asset, 2016). Industry-wide best practices and safeguards will enhance implementation and integration efforts (Johnson, 2016).

## **Future Research**

The examination of DLT is in its early stages. Developments, forums, and industry collaboration are underway to discover the technology's capabilities in a variety of services and market sectors. Technology firms, governments, and various business markets are looking at DLT as a transformative innovation, one with capabilities of easing processes and procedures.

However, specific to the financial marketplace, there is a variety of obstacles. Substantive deliberations regarding cybersecurity and consumer protection are not yet within the current research. However, many firms, such as Morgan Stanley and SWIFT, recognize the need for more research in these areas (Morgan Stanley 2016; SWIFT, 2016).

Companies such as SWIFT are focusing on research and development of the technology to address the concerns raised herein, including cybersecurity and privacy. Use cases within the financial marketplace and beyond will produce information regarding the technology and provide representations for future uses. Additionally, governments such as Estonia are expanding DLT uses within respective systems through providing expanded services to its citizens. Such services include tax payments and refunds, license and registration information, and filing documents (Government Office for Science, 2016). Non-financial marketplace insights will be valuable towards determining the technology's future as well. Forthcoming whitepapers and published research articles from various market sectors and industries will provide important information in the quest to understand the technology and deliver education in the endeavor to determine DLT's status within the financial marketplace.

### **Conclusion**

Distributed ledger technology has ignited a transformation in a variety of markets, including the financial marketplace. Its uses range from recordation of assets and business licenses to distribution of government services and benefits. While the technology faces limitations in regards to immediate utilization within the financial marketplace, there is a strong desire to overcome those limitations. DLT's potential benefit to increase efficiency and transparency are driving forces behind an industry-wide impetus of research and development.



Sociological circumstances typically dictate when, where, and how a group integrates a specific technology, rather than the technology or its capabilities (Koblitz & Menezes, 2010). There is a global determination towards integrating DLT, despite the current unknowns. As the public and private sectors investigate and explore capabilities, the technology will continue in its growth and integration within multiple market sectors.

Numerous resources are available that address and attempt to explain DLT and related technology. Financial-based firms are considering the technology as a means of improving transaction processes and contract execution. These firms face regulatory constraints, such as privacy laws, customer protections, and settlement criteria, which present limitations of thorough exploration. Non-financial firms, which face fewer constraints, are going forward with developing the technology. Lessons-learned in these environments will provide insights and information on how the financial sector can modify and fully utilize the technology to enhance and remain regulatory compliant.

The research provides wide-ranging information, facilitating analysis and utilization procedures. Cumulatively, the data provides comprehensive information and creates a trajectory for forward movement. DLT's current capabilities and uses are under exploration as the technology continues to develop. Security features and protocols are continuously facing examinations and tests, highlighting both strengths and areas for improvement. These tests are critical for the technology's development. However, given there are unidentified features, such as potential security vulnerabilities, it is best to conduct research in controlled and defined systems.

Implementation of DLT, specifically within the financial sector, will require extensive investigation and research efforts. There are strong proponents of DLT, despite limited use cases.

Governments and private sectors are incorporating the technology into their practices in an effort to increase efficiency, transparency, and reliability for a variety of operations. The financial sector faces limitations on current implementation practices; however, private firms are collaborating in an effort to overcome current and potential obstacles.

While widespread utilization within the financial sector is currently limited, financial firms and regulators alike find promise with the technology's capabilities. Smaller in-house or confined experiments are realistic means to discover problematic behaviors and system characteristics while also establishing potential solutions. Technological developments will also enhance consumer protections, including AML and KYC processes and regulations will continue to focus on maintaining market integrity. Addressing those concerns will create the path for successful incorporation and inclusion within the financial marketplace.

## References

- Blockchain Technologies. (2016). *Blockchain technology explained*. Retrieved from <http://www.blockchaintechnologies.com/blockchain-definition>
- Brainard, L. (2016, April 14). *The use of distributed ledger technologies in payment, clearing, and settlement*. Retrieved from <https://www.federalreserve.gov/newsevents/speech/brainard20160414a.pdf>
- Buterin, V. (2013, July 13). *Bitcoin is not quantum-safe, and how we can fix it when needed*. Retrieved from <https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150>
- D'Antona, Jr., J. (2016, January 26). *DTCC calls for leveraging ledger tech to solve market challenges*. Retrieved from [www.tradersmagazine.com](http://www.tradersmagazine.com)
- Del Castillo, M. (2016, April 11). *How R3 and major banks are building a new kind of distributed ledger*. Retrieved from <http://www.coindesk.com/r3cev-distributed-ledger-wall-street/>
- Deloitte. (2016). *Bitcoin, blockchain & distributed ledgers: Caught between promise and reality*. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf>
- Depository Trust and Clearing Corporation. (2016, January). *Embracing disruption. Tapping the potential of distributed ledgers to improve the post-trade landscape. A white paper to the industry*. Retrieved from <http://www.dtcc.com/news/2016/january/25/blockchain-white-paper>

- DeRose, C. (2015, October 28). *Private ‘Distributed Ledgers’ miss the point of a blockchain*. Retrieved from <http://www.americanbanker.com/bankthink/private-distributed-ledgers-miss-the-point-of-a-blockchain-1077435-1.html>
- Digital Asset. (2016). *Frequently asked questions*. Retrieved from <https://digitalasset.com/faqs.html>
- Dree12. (2014, April 19). *List of Bitcoin heists*. Retrieved from <https://bitcointalk.org/index.php?topic=576337>
- European Central Bank. (2016, April). *Occasional paper series. Distributed ledger technologies in securities post-trading*. Retrieved from <https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>
- FE Online Desk. (2016, September 11). *World Federation of Exchanges responds to ESMA DLT*. Retrieved from <http://www.thefinancialexpress-bd.com/2016/09/11/45440/World-Federation-of-Exchanges-responds-to-ESMA-DLT>
- Gelbstein, E. (2011). *Data integrity – Information security’s poor relation*. Retrieved from <http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation.aspx>
- Government Office for Science. (2016). *Distributed ledger technology: Beyond block chain. A report by the UK Government Chief Scientific Advisor*. Retrieved from [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gso-16-1-distributed-ledger-technology.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gso-16-1-distributed-ledger-technology.pdf)
- Hardy, Q. (2016, April 7). *A ledger for all*. The New York Times. Retrieved from <http://www.nytimes.com/2016/04/07/business/dealbook/ripple-aims-to-put-every-transaction-on-one-ledger.html>

Higgins, S. (2016, August 3). *The Bitfinex Bitcoin hack: What we know (And don't know)*.

Retrieved from <http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/>

Hinkes, A. (2014, July). *Blockchains, smart contracts, and the death of specific performance*.

Retrieved from <http://www.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci>

Johnson, R. (2016, August 22). *Distributed ledger technology: What we can learn from recent blockchain attacks*. Retrieved from <https://www.greenwich.com/blog/distributed-ledger-technology-what-we-can-learn-recent-blockchain-attacks>

Koblitz, N. and Menezes, A. (2010, March). *The brave new world of bodacious assumptions in cryptography*. Retrieved from <http://www.ams.org/notices/201003/rtx100300357p.pdf>

KPTX. (2016, October 6). *Cryptocurrency hacks: The biggest heists in blockchain history*.

Retrieved from <https://www.deepdotweb.com/2016/10/06/cryptocurrency-hacks-biggest-heists-blockchain-history/>

Kuchler, H. (2016, September 12). *Cyber attacks raise questions about blockchain security*.

Retrieved from <http://www.ft.com/cms/s/0/05b5efa4-7382-11e6-bf48-b372cdb1043a.html#axzz4K5Ex7AP7>

Lambert, J. (2016, August 10). *R3 tackles trade financing challenges with distributed ledger technology*. Retrieved from <https://r3cev.com/press/2016/8/10/r3-tackles-trade-financing-challenges-with-distributed-ledger-technology>

McLean, S. & Deane-Johns, S. (2016, April 5). *Demystifying blockchain and distributed ledger technology – hype or hero?* Retrieved from <https://media2.mofo.com/documents/160405blockchain.pdf>


- Miller, K. (2016, June 29). *Financial Stability Oversight Council identifies distributed ledgers as innovative, yet posing certain risks*. Retrieved from <https://www.virtualcurrencyreport.com/2016/06/financial-stability-oversight-council-identifies-distributed-ledgers-as-innovated-yet-posing-certain-risks/>
- Morgan Stanley. (2016, April 20). *Morgan Stanley Global Insight: Global financials / Fintech. Global Insight: Blockchain in banking: Disruptive threat or tool?* Retrieved from <http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf>
- Office of the Comptroller of the Currency. (2016, March). *Supporting responsible innovation in the Federal Banking System: An OCC perspective*. Retrieved from <http://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf>
- Reuters. (2016, August 15). *Can Bitfinex really impose a \$72 million theft on its customers?* Retrieved from <http://fortune.com/2016/08/15/bitfinex-bitcoin-hack-hong-kong-customers-law/>
- ROBECO. (2016a). *About us*. Retrieved from <https://www.robeco.com/en/about-us/>
- ROBECO. (2016b, May). *Distributed ledger technology for the financial industry. Blockchain administration 3.0*. Retrieved from <https://www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf>
- Sayer, P. (2016, June 20). *A blockchain 'smart contract' could cost investors millions*. Retrieved from <http://www.pcworld.com/article/3086211/a-blockchain-smart-contract-could-cost-investors-millions.html>

- Shubber, K. (2016, September 12). *Banks find blockchain hard to put into practice*. Retrieved from <http://www.ft.com/cms/s/2/0288caea-7382-11e6-bf48-b372cdb1043a.html#axzz4K5Ex7AP7>
- Siegel, D. (2016, June 25). *Understanding the DAO attack*. Retrieved from <http://www.coindesk.com/understanding-dao-hack-journalists/>
- Sier, J. (2016, June 20). *The DAO hack: \$US50 million lost*. Retrieved from <http://www.smh.com.au/business/markets/currencies/the-dao-hack-us50-million-lost-20160619-gpmke4.html>
- Stafford, P. (2015, July 14). *FT Explainer: The blockchain and financial markets*. Retrieved from <https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca>
- SWIFT. (2016, April). *SWIFT on distributed ledger technologies: Delivering an industry-standard platform through community collaboration*. Retrieved from <https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services>
- Wild, J., Arnold, M., Stafford, P. (2015, November 1). *Technology: Banks seek the key to blockchain*. Retrieved from <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64>
- Wilkins, C. (2016, June 17). *Bank of Canada Deputy Governor: Cooperation needed to advance distributed ledgers*. Retrieved from <http://www.coindesk.com/bank-of-canada-distributed-ledger-tech/>
- Wong, J. (2016, October 10). *Even the US military is looking at blockchain technology – to secure nuclear weapons*. Retrieved from <http://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/>

World Federation of Exchanges. (2016, August). *Financial market infrastructures and distributed ledger technology*. Retrieved from <http://www.world-exchanges.org/home/index.php/research/wfe-research>



## Appendix A – List of DLT applications in various business sectors.

<b><u>Economics and Markets</u></b>	<b><u>Government &amp; Legal</u></b>	<b><u>IOT</u></b>	<b><u>Health</u></b> 	<b><u>Science, Art, AI</u></b>
<ul style="list-style-type: none"> <li>• Currency</li> <li>• Payments &amp; Remittance</li> <li>• Banking &amp; Finance</li> <li>• Clearing &amp; Settlement</li> <li>• Insurance</li> <li>• FinTech</li> <li>• Trading &amp; Derivatives</li> <li>• QA &amp; Internal Audit</li> <li>• Crowdfunding</li> </ul>	<ul style="list-style-type: none"> <li>• Transnational orgs</li> <li>• Personalized governance services</li> <li>• Voting, propositions</li> <li>• P2P bonds</li> <li>• Tele-attorney services</li> <li>• IP registration and exchange</li> <li>• Tax receipts</li> <li>• Notary service and document registry</li> </ul>	<ul style="list-style-type: none"> <li>• Agricultural &amp; drone sensor networks</li> <li>• Smarthome networks</li> <li>• Integrated smartcity, connected car, smarthome sensors</li> <li>• Self-driving car</li> <li>• Personalized robots, robotic companions</li> <li>• Personalized drones</li> <li>• Digital assistants</li> </ul>	<ul style="list-style-type: none"> <li>• Universal EMR</li> <li>• Health databanks</li> <li>• OS Data Commons</li> <li>• Big health data stream analytics</li> <li>• Digital health wallet</li> <li>• Smart property</li> <li>• HealthToken</li> <li>• Personal development contracts</li> </ul>	<ul style="list-style-type: none"> <li>• Community supercomputing</li> <li>• Crowd analysis</li> <li>• P2P resourcenets</li> <li>• Film, dataviz</li> <li>• AI: blockchain advocates, friendly AI, blockchain learners, digital mindfile services</li> </ul>
<b><u>Crucial Blockchain Properties</u></b>				
<ul style="list-style-type: none"> <li>• Cryptolegger</li> <li>• Decentralized network</li> <li>• Trustless counterparties</li> <li>• Independent consensus-confirmed transactions</li> </ul>	<ul style="list-style-type: none"> <li>• Permanent record</li> <li>• Public records repository</li> <li>• Notarization time-stamping hashes</li> <li>• Universal format</li> <li>• Accessibility</li> </ul>	<ul style="list-style-type: none"> <li>• Communication (messaging)</li> <li>• Large-scale coordination</li> <li>• Entity ingress/egress</li> <li>• Transaction security</li> </ul>	<ul style="list-style-type: none"> <li>• Universal format</li> <li>• Large-scale multi-data-stream integration</li> <li>• Privacy and security</li> <li>• Real-time accessibility</li> </ul>	<ul style="list-style-type: none"> <li>• Large-scale infrastructural element for coordination</li> <li>• Checks-and-balances system for 'good-player' access</li> </ul>

List of DLT applications within various business sectors. (ROBECO, 2016b).