DISTRIBUTED LEDGER TECHNOLOGY:
Streamlined CDD Examination Process Through BLOCKCHAIN Application

WHY AUDITORS SHOULD EMBRACE NEW TECHNOLOGY

NELLA ZELENSKY, CAMS
### TABLE OF CONTENTS

1. **Executive Summary** ................................................................. 2

2. **Background** ............................................................................ 3
   2.1 Blockchain Technology Overview ........................................... 3
   2.2 Main Features of DLT ............................................................. 3
   2.3 Private vs. Public Networks .................................................... 5
   2.4 DLT Risks ........................................................................... 6
   2.5 DLT Benefits ....................................................................... 8

3. **Customer Due Diligence and DLT: Challenges and Opportunities** .... 9
   3.1 AML/CDD Regulatory Framework, Problems and Consequences .... 9
   3.2 Customer Due Diligence and its Key Elements .......................... 11
   3.3 DLT effect on CDD process .................................................... 12
   3.4 Objective Blockchain ID ........................................................ 14

4. **Impact of DLT and Blockchain ID Technology on CDD Audit** ........ 16
   4.1 Audit: Objectives and Regulatory Requirements ......................... 16
   4.2 CDD Testing Areas: Problems and DLT Solutions ..................... 16

5. **AML Risk Assessment and Audit Risk Model** ............................ 20
   5.1 Inherent Risk ....................................................................... 20
      5.1.1 Customer Risk and Special Considerations ......................... 20
      5.1.2 Product Risk ................................................................... 22
      5.1.3 Geographic Risk ............................................................. 23
   5.2 Risk Mitigation ..................................................................... 24
      5.2.1 Identification and Verification Risk ..................................... 25
      5.2.2 Detection and Monitoring Risk ......................................... 26
      5.2.3 DLT and Risk Assessment ............................................... 27

6. **CDD Audit Process and effect of DLT** ....................................... 29
   6.1 Planning and Scoping ............................................................ 29
   6.2 Fieldwork and Testing ........................................................... 30
   6.3 Recommendations and Reporting ............................................ 31
   6.4 Auditor Profession: The View Ahead ........................................ 31

7. **Conclusion** ............................................................................. 33
1. Executive Summary

We all are very fortunate to be living through the era of Internet and enjoying all the technological advancements of the last few decades, email, social media, mobile apps, e-commerce, smart TVs, and more. And just when someone might be wondering what’s is next, - it’s screamed from every post on LinkedIn and all TV programs: BLOCKCHAIN!

Dan and Alex Tapscott, the authors of the book "Blockchain Revolution," called blockchain technology "The next generation of the internet." Now, they said, in an increasingly centralized world, "The Internet of Things needs a Ledger of Things" that can help us to create digital relationships "that will reshape the world of business and transform the old order of human affairs for the better."

According to the Blockchain Research Institute, there are currently over 70 in-depth research projects on blockchain strategies and market opportunities in different sectors and industries. Billions of dollars have already been invested in the growing blockchain landscape, and there are numerous successful blockchain pilot programs. Finance and banking is, probably, where there is more at stake, specifically in the area of customer information management. Since application and development of blockchain technology is in its early stages, it is premature to say whether blockchain can handle the most complex processes and bring a future revolution in financial markets. One thing is for sure, however: blockchain technology is spreading around the world and making its mark in the finance industry space!

In this paper, we give a basic overview of blockchain technology, analyze its risks and key benefits applied to securities and financial markets, types of blockchain, its impact on Customer Due Diligence ("CDD"), and specifically how it could affect the CDD testing protocol, streamline auditing processes, and impact future of the profession of auditor. In the sections that follow, we also will cover how blockchain technology fits into the current regulatory framework and existing Anti-Money Laundering ("AML") rules and regulations, and how it might have material impact on Know Your Customer ("KYC") protocol. In addition, an area of special interest includes blockchain ID technology and its application along with standard blockchain implementations.

The intended audience for this report is compliance professionals, AML practitioners, internal and external AML auditors, and developers of blockchain platforms for customer information management. The goal is to raise awareness of this new technology and empower AML professionals and auditors to learn a process of blockchain application relevant to anti-money laundering and find out how blockchain technology, also known in the financial services industry as Distributed Ledger Technology, or DLT, can enhance customer due diligence.

This report is an initial contribution by the author in blockchain research for AML professionals and represents her dedication and intent to continue this work of covering the topic of distributed ledger technology and its impact on other areas in the anti-money laundering space. We all should be very savvy about blockchain innovation, understand its potential, and conform to changes imposed by DLT. This will be in line with efforts of the regulators to help us to stay abreast of fintech innovations and the opportunities and risks they may present, and will result in more knowledgeable and better educated auditors and superior exams. We will not adjust quickly but should put forth our best efforts towards it, because this is the only way to approach a changing situation: turn it to an advantage and improve your life and your career.
2. **Background**

2.1 **Blockchain Technology Overview**

Before we explore how distributed ledger technology might affect CDD and its examination process, the following section presents an overview of what blockchain is, how blockchain works, its features, types of distributed ledgers, their benefits, risks and limitations, as well as blockchain application in securities and financial markets.

Blockchain was first developed in 2008 and most widely used for virtual currencies such as bitcoin. It is a digital record or database stored on multiple computers in a network of trusted participants, so-called ‘nodes’. Those participants can make different entries on a record and no one node can control the information. It is a revolutionary way for information to be registered and distributed without any need to have a trusted middle-man to facilitate a transaction.

Users of a blockchain have identical and encrypted records and reach consensus about each entry at the same time and in a sequential manner using mathematical verification. As a result, this makes it impossible to argue about validity of a transaction. The larger number of nodes involved in a process and therefore larger number of validations, - the more secure the entire network. In the middle of March 2018, for example, the hash rate of the bitcoin network, - number of mathematical operations per second and a measuring unit of the processing power of a network, was 26,845,152 TH/s¹, which translates into 26,845,152 trillion calculations per second. The number is so large that as of this writing, we couldn't find any appropriate point of comparison.

2.2 **Main Features of DLT**

Since information on the blockchain is distributed on a peer-to-peer basis and there is no need for validation by a trusted 3rd party, **decentralization** is considered one of blockchain’s main features. Some argue that in terms of business application, this can result in cost cutting, better business function, customer service, creativity, innovation and the achievement of new levels of external collaboration.

Another prominent feature of DLT is the use of **cryptography**, a computer-based encryption technique which creates mathematical proof and provides a high level of security. The main functions of cryptography are confidentiality, integrity, and authorization. In and of itself, the technique is not something new. It is easy to think about cryptography and cryptographic keys using the base idea of keys to your safe deposit box: one key is your private key and the bank key would be considered a public key. Only use of both keys will open the door. But parties to a transaction on a blockchain have both keys, private and public. "The main purpose of this component of Blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys can be seen as a dexterous form of consent, creating an extremely useful digital signature. In turn, this digital signature provides strong control of ownership."²

In its simplicity, private key provides ownership authentication and the elimination of a need for sharing more personal information than necessary; therefore, they provide more security. But to transact, we need all those nodes to perform validation, and public key plays a role as a door-opener to the entire blockchain to participate in digital events. Each event is a piece of information necessary to transact and is presented as a block with a digital signature, timestamp, and any other relevant data. As soon as this information is transmitted to the entire network, the process of validation begins.

1. [https://blockchain.info/charts/hash-rate](https://blockchain.info/charts/hash-rate)
It normally includes validation from users of the network that the buyer and seller are the rightful owners of the assets. Confirmation is based on the entire history of records on the blockchain. This, of course, is a very simple description of how the whole process works, and verification protocols can be customized for different blockchains. Time taken for validation and recording may differ based on the type of verification method employed.

To achieve consensus, these methods are imperative for the entire DLT and are based on a clever cryptographic code, rather than placed in the trust of human beings, who may or may not do the right things. They are needed to prevent any service abuses and assure that no one participant can overpower the network, since any user can create multiple network addresses and use them for illicit purposes. The most well-known among different consensus processes are so-called ‘proof of work (POW)’, ‘proof of concept (POC)’, and ‘proof of stake (POS)’.

In a POW system, participants are required to do a lot of "work" and use tremendous amounts of electricity and computing power to find the next set of transactions. This involves solving many difficult mathematical functions. When a solution to a mathematical puzzle has been found, it is transmitted to the entire network. Other users should confirm that this new information contains only valid transactions and that the solution is correct. This is how a new block is created and a validator, who solved the puzzle, adds the new set of transactions to the existing ledger.
After confirmation is completed, data is encrypted through a cryptographic hash function which "takes an input (or 'message') and returns a fixed-size alphanumeric string."3 This alphanumeric string, the output, is called a 'hash' or 'hash value' and is viewed as a digital fingerprint. Encrypted information is permanently recorded on a blockchain network and all records are immutable and sequentially linked.

Immutability of information stored on blockchains is extremely important in connection with data security. It means that once information has been recorded on a blockchain, no one can change it. This is bad news for anyone with fraudulent ideas in mind since every user of a blockchain network has the same set of data and it is impossible to convince all of them to alter that data, especially following the same sequence. Immutability is considered an important benefit of blockchain networks since it provides an audit trail.

Since it is extremely difficult to calculate the alphanumeric text that each hash is associated with, and because it is extraordinarily unlikely that two slightly different messages will have the same hash, it is important to emphasize that the recorded dataset is immutable and cannot be modified. Any corrections may be made only by adding a new entry.4

Cryptography and decentralization assure protection of ownership rights and preservation of data in a censorship-free manner. But how to translate the terms of a transaction and contractual obligations between parties into a digital framework? The answer is the use of so-called ‘smart contracts’, - self-enforced pieces of code which assure execution of a set of transactional instructions on a DLT network, therefore providing clever automation of pre-determined and agreed-upon conditions. Smart contracts can be viewed as an additional layer on a blockchain, like an add-on. They have the capability to codify complex business, financial, and/or legal arrangements on a DLT network, make them enforceable, and decrease the number of errors. Even though smart contracts carry some novel risks, numerous industry experts consider the use of smart contracts a winning strategy.

2.3 Private vs. Public Networks

As we’ve already stated, blockchain was originally designed as an underlying platform for virtual currency. Specifically, it uses an open network in which anyone can download software, become a member, and use cryptographic keys. Every member, or node, can see the entirety of the network data without any restrictions. Open DLTs completely rely on their participants to validate and record transactions based on a prescribed protocol. There is not any central authority. Open networks are also known as ‘public’ or ‘permissionless.’

Another type of blockchain is private, or permissioned, wherein access to the information is restricted, as is who can join the network, who can transact on a blockchain, and/or who can build additional blocks of data. All members of a private network are known, but permissions for different participants can give them different levels of access to varying functions, such as viewing records, transacting, and/or making updates. Since participants are required to have specific credentials to operate on a private DLT, permissioned networks have the potential to maintain greater control over their users and significantly reduce the risk of illicit activity. That is why private blockchains are so suitable for the financial industry, with its high standards of confidentiality, privacy, transactional integrity, monitoring requirements, and automation. In addition, restricted ledgers provide an easier way for regulators to audit and examine.

4. Ibid
Even though private networks are still in the early stages of their development, there is a growing interest in development and adoption of private DLTs in securities and financial markets, which might make some functions and processes more efficient and less costly. In addition, permissioned networks have the potential to improve domestic and international markets infrastructure, increase and simplify complex interactions between different market participants, and therefore also have a major impact on interoperability between proprietary databases.

Currently financial institutions adopt distributed ledger technology using three major methods of deployment: internal teams, consortiums, and partnerships. “Although a distributed ledger can have an immediate positive impact even between two businesses, it derives more utility from network effects: The greater the number of users, the more valuable the technology is to all of them. Consortia allow companies to take advantage of blockchain network effects from day one, by providing a vehicle to create a governance structure around this collaboration, often among players that compete against one another.”

Since cooperation and collaboration between market participants is imperative for DLT success, consortiums are considered the most effective way in which many financial institutions participate in the development of new technology. Among the prominent names in the consortia landscape today are Hyperledger, Enterprise Ethereum Alliance, and R3, backed by the world’s largest financial participants. R3, for example, and a few of the largest member banks, have been working on a DLT-based shared KYC registry to place control of identity with its owner. Hyperledger, hosted by The Linux Foundation, is an open-source collaborative effort of leaders in finance, banking, and other sectors to create cross-industry blockchain platforms and a new generation of transactional applications.

2.4 DLT Risks

Distributed ledger technology has revolutionary potential for demanding financial services and banking industry to address some of the problems of legacy infrastructure, data management, and weaknesses in different financial processes. This technological innovation is referred to by many as ‘digital disruption,’ and, as any disrupter has its consequences, blockchain technology also has its risks and downsides which cannot be ignored. This in turn can cause various legal and regulatory challenges. In the section following, we will review in detail the risks presented by DLT, especially considering investigation and analysis of its potential applications by market regulators to assure consistency with the principles of investor protection and market integrity.

Among those unintended risks, where the system has a number of vulnerabilities is the issue of governance. As discussed in the FINRA Report, “Distributed Ledger Technology: Implications for the Securities Industry,” the lack of a central governing body has created concerns for the network, as participants must try to determine an approach to handling increased transaction volume. Therefore, a DLT network based on the use of trustless networks, wherein no party is responsible or accountable for the proper operation of the system, may present risks to markets and investors. The main logical question in operation of the network is who bears responsibility.

The report highlights the following regulators’ concerns:

- How will the governance structure of DLT be determined: by a single entity or a group of firms?
- Who will be responsible for ensuring adherence by participants to the requirements established for the DLT network?
- How would any potential conflicts of interest be addressed?
- How would any errors or omissions on the blockchain be reflected or rectified?

Another big concern with regard to DLT applications and its novel risks is the issue of privacy and therefore of providing appropriate levels of access to different network users. As emphasized in another report, "The Distributed Ledger Technology Applied to Securities Markets," by the ESMA, European Securities and Markets Authority, "the identity of a party to a transaction is, in most instances, not public, unless legal provision require the disclosure of this information. Therefore, it is of utmost importance that DLT networks are designed in a way that protects privacy when necessary." Regulators demonstrated importance of use of encryption and private keys only by authorized parties for transactions to prevent risk of illicit activities. Another big concern on the part of the regulators is the question of how transparent the data on a shared ledger will be among participants.

In addition to governance and information privacy, a critical consideration should be given to areas of data security and cyber risk, especially given the potential for network users across borders. Below are the concerns of domestic and international regulators and market participants regarding DLT security:

- How are the cryptographic keys protected from unauthorized access, modification, or loss?
- How is adequate protection against attacks provided?
- If a key is compromised, how will fraudulent transactions be identified and reversed? What party will be responsible for this?
- Who covers the cost of fraud?
- What kind of risk can be presented by a single unsecured node?
- What methods have been considered to enhance the security of assets?

Issues of data security are crucial to anti-money laundering and fraud prevention. As indicated in the ESMA report, “in the absence of relevant controls, those risks would be exacerbated as cryptography could be used to conceal identities and undertake fraudulent activities.” Customer data security should be a big consideration of any firm joining the DLT network. Issues concerning blockchain and AML, specifically customer due diligence, security and confidentiality of customer records and information, will be covered in depth in later sections.

While it is too early for experts to evaluate all the risks presented by DLT and its impact in securities and financial markets, in addition to the downsides covered above, there are another few channels of disruptions. These might include interoperability, use of common standards, and scalability. There is a need to ensure interoperability with existing systems and use of a certain level of standardization. This is a big concern of the regulators, and as stated by the ESMA, “this could drive some firms out of the market and lead to a monopoly-like situation with negative consequences on the cost and quality of the services.”

In turn, this might negatively affect fair competition and disrupt orderly markets.

10. Ibid
Because of interoperability concerns, it is of increased importance that DLT be deployed gradually. Without setting certain universal standards, integration of DLT into existing landscapes will be difficult to achieve. In addition, interoperability comes with a price, since it requires financial resources, expertise, and specific skill sets. Another challenge here is getting market participants working together and that is why industry consortiums play a major role in the adoption of new blockchain technology in financial markets.

The issue of integration in not only crucial regarding DLT and legacy platforms, but also DLT and existing regulatory frameworks, especially as technology is evolving and gaining more popularity. A major focus of industry experts is ensuring the regulatory compliance and mitigation of the risks presented by blockchain technology. FINRA emphasized that it “welcomes an open dialogue with market participants to help proactively identify and address any potential risks or hurdles in order to tap into the full potential of DLT, while maintaining the core principles of investor protection and market integrity.”

2.5 DLT Benefits

It will not be a fair analysis of potential applications of blockchain systems in financial markets, and specifically in the area of customer due diligence, without a review of its prospective advantages. As FINRA stated in its DLT report, these new technology systems “represent the potential to create a paradigm shift for several traditional processes in the securities industry through the development of new business models and new practices.” Regulators and market experts agree that DLT applications can have a positive impact on post-trade processes, make them more efficient, and reduce costs.

Decentralization, cryptography, and the use of smart contracts as main features of DLT have the potential to bring number of benefits. It is crucial that those benefits be in balance with novel and existing risks and limitations of such a new technology. Below are listed some advantages presented by DLT in securities markets:

- **Faster speed**
- **Immutability of records**
- **Enhanced security**
- **Enhanced reporting**
- **Increased data quality**
- **Simplified onboarding**
- **Instantaneous settlement and clearing**
- **Time-stamped, sequential audit trail transaction records**
- **Enhanced data management capabilities**
- **Enhanced traceability of transactions**
- **Simplified business transactions**
- **Self-regulation**
- **Increased transparency**
- **Additional efficiency**
- **Fraud reduction**
- **Enhanced risk management**
- **Greater access to services**
- **Enhanced customer experience**

12. Ibid
Improved data quality and simplified onboarding as potential DLT benefits, can positively impact customer identity management, which is a significant function of CDD. Distributed ledger technology can help financial institutions with their basic KYC onboarding requirements and provide increased transparency, security, and cost-efficiencies. It also gives clients the opportunity to manage their global identity and relevant documentation by using a single interface.\(^\text{13}\)

David Rutter, CEO of the R3 consortium, comments: "The growing complexity and cost of KYC compliance requirements presents a major challenge for banks on-boarding new clients and is having a negative impact on those client relationships. Distributed ledger technology can provide a unified view of clients whilst also significantly reducing costs and time spent verifying identity."\(^\text{14}\)

It is of great importance for all compliance and audit professionals to understand that a trend of annually increasing compliance, and therefore AML budgets across the entire financial industry, has reached its peak and is no longer rising.\(^\text{15}\) Automation and new technology play a major role in this process. According to a report from Quinlan & Associates, “\textit{From KYC to KYT},” distributed ledger technology has the potential to bring $4.6 billion in annual AML cost savings, almost 1/3 of the current spend.\(^\text{16}\)

Some of the above benefits directly relating to the subject of this paper will be additionally covered in the next section. It is important to emphasize that blockchain systems may improve and streamline the above processes under absolute conditions in which the appropriate means of control and continuing testing are in place.

\section*{3. Customer Due Diligence and DLT: Challenges and Opportunities}

As stated prior, this paper is intended to review DLT’s potential to create a whole new process of customer due diligence and how surveillance and audit professionals will approach this new function. In the sections that follow, we provide a basic overview of CDD as a center of the financial transaction lifecycle, the current regulatory framework, KYC/CDD as an area of significant regulatory focus, key points of an effective CDD program, and the impact of advanced Blockchain ID technology on customer due diligence.

\subsection*{3.1 AML/CDD Regulatory Framework, Problems and Consequences}

Since 1970, when the Congress of the United States passed the \textit{Bank Secrecy Act}, sometimes referred to as an ‘anti-money laundering’ ("AML") or as "BSA/AML," the financial industry has been working in certain areas to detect and prevent money laundering. Today, in a post-9/11 era, when new laws and regulations are enacted combating financial crimes which cover a wide array of illicit activity, things are more complex than ever and require significant funding. Anti-money laundering costs across the entire financial sector have been escalating for a number of years and related penalties are on the rise. There is no month that passes without different financial institutions and individuals being censured, fined, suspended, or barred by regulators for AML-related issues.

\begin{footnotesize}
\begin{enumerate}
\item \url{https://www.finextra.com/newsarticle/29747/global-banks-and-r3-test-dlt-for-kyc-services}
\item Ibid
\item \url{https://www.quinlanandassociates.com/wp-content/uploads/2016/12/Quinlan-Associates-From-KYC-to-KYT.pdf}
\end{enumerate}
\end{footnotesize}
Since 2009, US regulators handed out over 16 billion USD to 13 banks, with most failings being about sanctions breaches.\(^\text{17}\)

AML remains a major focus of the regulators and one of the principal operational risks identified in the *FINRA 2018 Regulatory and Examination Priorities Letter*\(^\text{18}\). AML is in direct relationship with two other operational and financial risks: technology governance and cybersecurity. To highlight main existing AML shortcomings, it is very important also to refer to the *FINRA 2017 Regulatory and Examination Priorities Letter*\(^\text{19}\). Among major deficiencies covered in both FINRA documents, there were gaps in the following areas:

- data integrity problems
- failure to have AML programs actively tailored to a business
- alerts or exceptions parameters not sufficiently risk-based
- weaknesses in suspicious transaction monitoring
- inadequate investigations of potential suspicious activity
- weak monitoring of high-risk transactions
- inadequate CIP and CIP violations
- inadequate independent testing
- cybersecurity and protection of customers personal data
- operational breakdowns caused by new technological systems
- manual review process and high rate of false positives
- customer data management in silos
- outdated or inaccurate information
- incomplete and erroneous customer records
- lengthy due diligence analysis and investigation

Among the above indicated AML issues, data integrity, automation of data and new technology solutions are at the center of the attention of regulators and compliance professionals. As stated by Susan F. Axelrod, the former FINRA Executive Vice President of Regulatory Operations, at SIFMA 2017 Anti-Money Laundering & Financial Crimes Conference, "common AML violations were caused by bad data: gaps in data fed into automated surveillance systems and exceptions reports including firms’ failure to include a certain type of account or customer in a specific alert type. Automated data can be helpful in implementing an AML program, but data accuracy and integrity are crucial to the effectiveness of any automated system."\(^\text{20}\) New technology is "helping regulators and compliance departments strengthen their compliance functions by improving risk-identification processes to foster an environment where emerging issues can be addressed quickly. The ability to intake large amounts of data and use that data to generate meaningful analytics has enabled firms to surveil like never before. In the AML space, providers are looking at how big data can be leveraged to uncover risks and track the flow of illicit funds across borders."\(^\text{21}\)

The opinions of the regulators here are in unison with experience and the reality of market participants. Numerous surveys in financial sector show that data availability and quality, reliance on manual processes, and difficulty maintaining/updating existing IT infrastructure today are the top operational challenges related to financial institutions’ CDD/KYC programs. The highest priorities for financial organizations for the period of the next 12 to 18 months is improving data management and its quality, investing in new technology solutions, the process of automation, and a real-time assessment of onboarding.

To address AML challenges, it is crucial that cutting-edge innovative solutions be identified, tested, and implemented at broad scale. Distributed ledger technology can be the breakthrough which can leverage data, bring meaningful analytics, improve risk-identification processes, and quickly address existing and emerging AML issues.

By improving customer data quality, DLT could increase the effectiveness of customer due diligence, which is a foundation of any successful AML program to identify and mitigate money laundering activity and fraud. Many experts say that "knowledge is what the entire anti-money laundering compliance program is built upon. The more you and your institution know, the better money laundering abuses can be prevented." It is imperative that financial institutions know who their customers are, where they are, and who they do business with. Without this, it is impossible to have good quality data and therefore assure effective data use, management, monitoring and effective compliance with AML/KYC national and international regulations. In the financial industry as a highly-regulated sector, inadequate customer due diligence can be very costly.

### 3.2 Customer Due Diligence and its Key Elements

In the text that follows, we highlight the key points of an effective CDD program, problems associated with existing customer due diligence, DLT as a specific solution, and the impact of advanced Blockchain ID on CDD/KYC processes.

As defined in the *FFIEC BSA/AML Examination Manual,* "the cornerstone of a strong BSA/AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious."
Distributed Ledger Technology: Streamlined CDD Examination Process through Blockchain Application

- **Customer Identification Program (CIP):** Section 326 of the US PATRIOT Act requires “minimum standards for financial institutions that relate to the identification and verification of any person who applies to open an account.”  Those standards include: (1) identification and verification of persons seeking to open an account; (2) recordkeeping; and (3) comparison with government lists.
- **Basic Customer Due Diligence:** collection of information to verify customers’ identity and assess risks associated with those customers’ accounts.
- **Enhanced Due Diligence:** collection of additional information for higher-risk customers.
- **Ongoing Monitoring and Reporting:** continuing surveillance of account activity to identify areas of concern, cure deficiencies, and generate reports.

Another important regulation specifically in securities markets is **FINRA Rule 2090**, also known as “Know Your Customer (KYC).” It requires that “Every member shall use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer.”

Among new regulations affecting the AML landscape and specifically customer due diligence, is the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) Customer Due Diligence Requirements for Financial Institutions, issued on May 11, 2016 and commonly referred to as the **Final CDD Rule or Final Rule**. It is intended to strengthen and clarify existing CDD requirements for covered financial institutions and verify the beneficial owners of legal entity customers. The Final Rule constitutes a fifth pillar of an adequate AML program, joining the other four (namely internal controls, independent testing, designated compliance officer, and personnel training).

In addition to the above, a sound CDD program should include these 7 elements:

- **Full identification of customer and business entities, including source of funds and wealth when appropriate.**
- **Development of transaction and activity profiles for each customer’s anticipated activity.**
- **Definition and acceptance of the customer in the context of specific products and services.**
- **Assessment and grading of risks that the customer or the account presents.**
- **Account and transaction monitoring, based on the risks presented.**
- **Investigation and examination of unusual customer or account activity.**
- **Documentation of findings.**

### 3.3 DLT effect on CDD process

With all the challenges and complexity of customer due diligence today, as well as a rapidly expanding regulatory framework, distributed ledger technology has a huge potential to improve customer identification related regulatory obligations and simplify the entire AML/KYC compliance process.
One of the biggest benefits of DLT is increased efficiency of CDD functions. As FINRA stated in its report, “Distributed Ledger Technology: Implications of Blockchain for the Securities Industry”, “some market participants are exploring setting up a centralized identity management function, such that once the identity of a customer is verified by an entity on the network, that information may be made available to all parties on the network. The motivation here is to potentially eliminate duplication of efforts by various entities to verify customer identities…” This issue of duplication of efforts exists not only between financial institutions, since they are obligated to conduct independent KYC review on each prospective client, but also within a single firm. All of us as AML professionals know very well from our own experience how frustrating onboarding can be when clients have multiple accounts with the firm. As a result, account reps and operations people complain, and prospective and existing clients become upset, thus resulting in a negative customer experience.

The shared ledgers of DLT will not only eliminate the problem of data duplication between members of the network, but will allow for different CDD/KYC information to be uploaded to a central registry and exchanged between qualified users.

Another problem with existing CDD processes for which distributed ledger technology can provide an outstanding solution is the excessive manual processes that take place during onboarding, surveillance, and reporting, which are tremendously labor-intensive, very costly, and in the case of onboarding, can negatively affect turnaround times. DLT can drastically reduce manual processes regarding KYC review, identity and account ownership verification, sanctions screening, and risk assessment.

Use of smart contracts as one of the main features of blockchain technology can provide a great solution to another AML/CDD problem: the high percentage of false positives for suspicious activity, currently between 90 to 95 percent. The issue here is that current monitoring systems have thousands of data legs and are designed in verticals, and one vertical doesn’t communicate with another, therefore there is no instantaneous holistic picture of the entire customer account and its activity that is updated on a regular basis.

Another reason for a high number of false positives, as seen from FINRA exam findings, is poor data quality and incomplete transactional information. As a result, financial institutions must spend significant resources and manpower to process numerous alerts for legitimate financial transactions. Smart contracts can drastically reduce the number of false positives by attaching additional relevant data and pre-arranged conditions to transactional and payment instructions. Through embedded triggers, smart contracts have the potential to provide great automation of the transactions and their monitoring, reducing the number of errors.

Through embedded triggers, smart contracts have the potential to provide great automation of the transactions and their monitoring, reducing the number of errors.

Smart contracts can also provide a solution to another AML/CDD challenge when alerts or exceptions parameters are not sufficiently risk-based and systems fail to have a suspicious activity monitoring framework tailored to a business. They can improve existing reporting AML process with their post-facto nature and through their key data not being intuitively identified. Of course, coding errors in smart contracts present a certain level of risk which cannot be ignored.

An important element of potentially suspicious activity is the issue of traceability of transactions. Here, blockchain technology can enrich transaction-level information, which in turn results in greater transparency in transaction monitoring, could drastically reduce the number of false positives and manual reviews required by compliance teams to investigate suspicious transactions, and prevent fraud. The enhanced sharing and storing of the reference data would also make KYC and AML checks more robust and efficient.31

Another distinction of distributed ledger technology for processes of customer due diligence is its provision of certain advantages in comparison with existing systems in regard to security and resilience against a cyber-attack or a system breakdown. As it is stated in the ESMA report, “The distributed and shared nature of the system could facilitate the recovery of both data and processes in the case of an attack (assuming that not all the nodes are corrupted simultaneously). This could reduce the need for costly recovery plans. Sophisticated encryption techniques could also provide an additional layer of protection to pools of information stored on DLT compared to existing systems. Nonetheless, the risk of a cyber-attack would still need to be considered seriously in a DLT context.”32

3.4 Objective Blockchain ID

The main question of the entire CDD process using blockchain technology is how market participants can verify the identities of qualified parties in a transaction. Reliable customer identification is imperative for financial institutions engaging in any form of electronic banking or commerce. An effective authentication platform can reduce fraud and promote the legal enforceability of their electronic agreements and transactions. Customer interaction with financial institutions is migrating from physical recognition and paper-based documentation to remote electronic access and transaction initiation. The risks of doing business with unauthorized or incorrectly identified individuals in an electronic banking environment could result in financial loss and reputation damage through fraud, disclosure of confidential information, corruption of data, or unenforceable agreements.33

Financial institutions use various authentication techniques and methods: passwords, personal identification numbers (PINs), public key infrastructure (PKI), smart cards, different types of tokens and biometric identifiers. Multi-factor authentication is considered stronger and more reliable against fraud.

Today, identity verification in the US is a $3T market. There are numerous active DLT identity authentication platforms. One of the most prominent and unique is IBM project “Objective Blockchain ID (OBID).” As stated by Daniel Bingham, Associate Partner of Strategy & Market Development, who works with OBID, “if there is anything that creates more friction points in any given day and which is universally recognized as something that should be absolutely immutable, it is a person’s identity.”34

34. https://www.linkedin.com/pulse/objective-blockchain-id-daniel-w-bingham/
Objective Blockchain ID allows financial institutions with near 100% accuracy and scientific proof to confirm personal or business identity within a minute and assure a high level of data security which is cryptographically hashed. The ID is immutable and indexed on a blockchain for retrieval. Legal customers are linked through business transactions and party documentation to a natural person, which facilitates compliance with the FinCEN CDD Final Rule.

The uniqueness of OBID is that it combines various biometric techniques and so-called ‘cognitive load’ testing, an involuntary physiological response when the brain slows its thinking to create a lie, which now can be observed and measured. OBID incorporates and strengthens three essential parts of ID authentication: government documents (i.e. driver’s license, passport), customers’ own IDs (passwords, pin codes, security questions), and a person’s biometrics (i.e. facial recognition, ocular, fingerprint). The entire process of ID verification includes the creation of a “total person” and their validation which is indexed into the blockchain ID. Since this record is immutable and cannot be replicated in the DLT ecosystem, OBID as an ID authentication method has a huge potential to prevent identity theft and address other AML/CDD/KYC issues.

Through linking personal identities to transactional documentation, OBID can be used in various situations:

- Secretary of State business registration records
- Financial regulatory oversight
- AML/KYC account onboarding
- Confirming that internet accounts are tied to known persons
- Investment firms that want to minimize their exposure to multiple AML/KYC regulatory obligations
- Deploying an effective onboarding tool in high-risk money laundering geographic locations
- High dollar transactions
- Higher-risk customers and their transactions monitoring

In summary, OBID provides foundational and scientific objectivity to the blockchain ID process and offers reliability, accuracy, and security. It cannot be altered or duplicated. Once the ID is set up, an individual or business cannot get another ID. This in turn can significantly reduce AML-related issues. There is no need to wait until OBID will work together with other ecosystems. The technology doesn’t require any specialized hardware and the process can be completed any time, on any device, and anywhere in the world. Lastly, Objective Blockchain ID offers the opportunity to add multiple metrics to basic ID and therefore take away complexity from customer due diligence as a process.

Of course, no matter what method of ID verification financial institutions use, they all have independent obligations to comply with all relevant AML and customer identification rules and cannot outsource those responsibilities or relieve themselves from any regulatory obligations.
4. Impact of DLT and Blockchain ID Technology on CDD Audit

4.1 Audit: Objectives and Regulatory Requirements

If distributed ledger technology could make a case to attract billions of dollars of venture capital, the support of the biggest market participants, and tremendous attention of investment public, it is certainly a green light for regulators and examiners to have the issue of DLT on their agenda. As we described earlier, this concern is about technology risks, limitations, and benefits, how it optimizes financial processes and functions within the current market landscape, and, of course, how new blockchain technology interacts with the existing regulatory framework. If the first possible reaction of some in the compliance community was to hold their tongue, especially considering developments with bitcoin, confusion is and will be replaced with a very proactive attitude promoting understanding of the technology, IT education, interaction between regulators, and internal and public auditors sharing their challenges and best practices.

Possible changes in the regulatory landscape brought by DLT, especially in the long term, will impact how we, compliance practitioners, supervisors, and examiners, do business. This cutting-edge technology has the ability to enhance the supervision process, adjust examination objectives, and streamline the entire audit protocol. Auditing in turn will play a major role in assessing how well a financial institution will identify emerging issues regarding DLT and how those issues impact the institution’s AML activities.

Those of us in the compliance and audit industry know firsthand that the main objective of the examination process is to assess a financial institution’s BSA/AML risks, develop the examination scope, and document the plan. Auditor determines how effective a BSA/AML compliance program is and how it complies with the BSA regulatory requirements, including a review of risk management practices.35 From this specific angle, with a focus on mitigating regulatory risk exposure, we will set out our analysis of DLT’s impact on audit processes and specifically on examination of CDD/CIP/KYC function.

4.2 CDD Testing Areas: Problems and DLT Solutions

There are a few essential and mandatory elements of any examination protocol and required regulatory AML procedures: Customer Due Diligence as a cornerstone of a financial institution’s AML program, Customer Identification Program, Suspicious Activity Reporting, Recordkeeping, and Office of Foreign Assets Control.

CIP, with its objective to assess financial institutions’ compliance with statutory and regulatory requirements for Customer Identification Program is the implementation of Section 326 of the USA PATRIOT Act and, as stated in FFIEC Examination Manual, “requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements.”36 The purpose of the CIP is to form a reasonable belief that the financial institution knows

the true identity of each customer. “The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.”

In today’s world when the main question for any business is how you can trust a person, CIP and KYC processes could tremendously leverage upon distributed ledger technology, which can provide a solution to the problem of trust. One of the proposed benefits of DLT is found through obtaining the appropriate level of network access, as authorized users, internal, and public auditors can use the technology to view immutable customer ID records and all relative information on one ledger at once, without the need for email correspondence, attachments, print-outs, or back and forth communication. In addition, use of smart contracts include as a trigger the presence of all minimum required pieces of identifying information before an account can be opened and once customer ID verification becomes complete. Smart contracts will inject business logic into account-opening protocol and add automation to it. If, based on its risk assessment, a financial institution requires additional information for customers of higher risk, they can create an additional entry on a blockchain, and this could be done in a very timely manner with minimal effort or disruption and for the use of all qualified members of the network. This in turn will significantly reduce the number of incomplete and erroneous records and enable dramatic efficiency gain in the examination process.

As indicated by FINRA in its report, “Distributed Ledger Technology: Implications of Blockchain for the Securities Industry,” another of the proposed benefits of DLT is a time-stamped, sequential audit trail of transaction records. This will enable examiners to view on one ledger the entire transaction history and perform monitoring of account activity all in one place, in a logical sequence, with data immutability and provenance. No more records from the clearing firm, piles of transaction verifications from a trade desk, cross-referencing with manual trade blotters and AML reports. No more application and transaction forms or order tickets! Any of us who have ever been on either side of a regulatory exam or an independent audit knows very well what is involved, and thus should especially embrace blockchain technology because of how thorough, authentic, verifiable, and linked the nature of each block on a ledger is. DLT might simplify and streamline the examination process and automate auditing of records.

ID and transaction management through a blockchain will work in a new and revolutionary way opposite to the existing process. Once data set is verified, cryptographically hashed and put on a ledger, it has the potential to be shared among other authorized DLT network participants in the most secure and cutting-edge way. For each person, there is only one unique ID indexed on one ledger with the entire financial history of that person or business entity. It will be impossible to set up another ID for the same customer or alter the recorded data, even by the account holder. This will assure record immutability and authenticity. Financial institutions will not need to obtain customer information repeatedly when a new account is established or transferred, but simply through accessing a person or a legal customer blockchain record on a shared ledger, view it and make the appropriate changes as new entries. This way, through blockchain

For each person, there is only one unique ID indexed on one ledger with the entire financial history of that person or business entity.

instant access to customer identity and a full cycle of the money involved in a financial transaction, the auditor has the ability to have a panoramic view of the entire party’s data and cut through unnecessary noise. This in turn will allow auditors to assess customers’ prior relationship and make the appropriate connections between source and use of funds through the entire financial lifecycle of these customers. And here, DLT is not just information, it is quality of information! This is exactly what is now on a list of top challenges and priorities across the industry.

Part of the problem with suspicious activity is that as an internal process, it can be quite inefficient, because critical details about transactional information and account assets are frequently placed and recorded across multiple datasets within a financial firm, and very labor-intensive manual processes are needed to reconcile the data. We analyze the information, identify suspected criminal activity, and initiate investigation. In addition, we must review patterns of account activity, all related information, and customer financial relationships. This process can be very challenging.

When we get clean, immutable, and reliable data in one place along with automation of some functions of the examination process, it will help us better understand who our customers are, who they do business with, and ensure effective monitoring of customer transactions/accounts and identification and reporting of suspicious activity. Since smart contracts will inject business logic into each transaction, they will reduce guessing, elements of subjectivity, and manual involvement during the process of monitoring, which in turn minimizes the number of errors, saves time, increases consistency, and strengthens the internal audit function.

Improved CDD/KYC function through verifiable, immutable, and authentic DLT records will positively affect transaction monitoring and SAR preparation and filing. This can also drastically increase the timeliness and usefulness of SAR for law enforcement, especially due to the integrity of data flow and its quality. Today, data quality in SAR reporting is a big challenge. Through the improved function of conducting customer due diligence and monitoring of customers for suspicious activity, DLT can significantly help the auditors to review the reported activity against the essential elements of an underlying offense and therefore to determine if a report’s narrative sufficiently and competently supports the opinion of the reviewer about the underlying offense.

In addition, through improved quality of data and the submission of appropriate, relevant, and accurate information on SARs, distributed ledger technology can positively affect collaboration between financial institutions and law enforcement and play a significant role in combating and preventing fraud and economic crimes. How the entire protocol of SAR preparation and submission will be affected from the standpoint of technology remains to be seen and it is a fitting subject for a future paper.

Another essential and mandatory element of any regulatory exam or independent audit is recordkeeping. DLT networks that can be defined as a type of electronic storage media (ESM) may provide financial institutions the opportunity to maintain certain records on the network itself. Auditors, as a party with authorized and temporary access to the network, will be able to view those records and assess how the market participant complies with minimum recordkeeping and retention requirements, types of records that must be maintained, and periods of time that the financial institution should keep mandatory records. In addition, the immutability of data on a blockchain ledger, in our opinion, may force financial institutions to better comply with Write Once Read Many requirements (WORM), which refers to an archiving network's ability to store records in a non-rewritable and non-erasable format. This in turn will improve market participants’ compliance with Rule 17a-4 of the
Securities and Exchanges Act (SEA). Data sequentially recorded and time-stamped on a DLT ledger will allow financial institutions to meet another recordkeeping format condition: sequential labeling of the electronic storage media units and time-date records.\(^\text{38}\)

Since new accounts opening on DLT and all related functions are done electronically, there will be no need to convert books and records from one permissible format to another, for example, from paper to electronic. Here, an auditor will not need to test the procedures of the firm to verify the conversion process to preserve data integrity, nor compare paper originals with electronic versions to ensure accuracy. Since certain records relating to customer accounts must be retained for at least 6 years, this can have a significant impact on saving an auditor’s time and resources.

Even though some benefits of DLT could improve the compliance of financial institutions with their recordkeeping obligations, there are certain limitations and challenges that should be addressed. As FINRA indicated in its report, "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry," certain important factors should be considered:

- What information is maintained using the DLT network?
- What will be deemed as the physical location of the firm's records maintained on a node of a DLT network that may extend over multiple countries?
- What parties have control or access to the firm's records? What are their rights, obligations, and responsibilities related to those records, and how are they governed?
- What is the firm's (and other participants') level of access to the data, and in what format would it be able to view the data?
- How would the records be made available to regulators?
- How will the firm's traditional exception reporting, used to supervise transactions be generated from a DLT network?
- How will the firm protect any required records from tampering, loss or damage?\(^\text{39}\)

Benefits and the potential risks of distributed ledger technology will affect the scope of audit work and an auditor’s function and role which we cover in a later section.

Another significant element of CDD/KYC auditing is testing compliance with regulations of the Office of Foreign Assets Control (OFAC), which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals. Each customer name must be checked against the U.S. Government’s lists of known or suspected terrorists. Financial institutions also should determine if a customer is a Politically Exposed Person (PEP). OFAC sanctions require that each financial institution must reject certain transactions and block transactions of certain individuals and entities.

One of the objectives of independent testing, as defined in the FFIEC Examination Manual, is to conduct a comprehensive evaluation of OFAC policies, procedures, and processes, and to identify and review transactions and accounts for possible OFAC violations. "The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program."\(^\text{40}\)

---

Here, DLT, as transformative technology, can put the manual process of review out of business and significantly increase efficiency of the examination processes, since OFAC filtering and screening criteria could be coded in a blockchain through smart contracts or through other methods. Coding of OFAC requirements in DLT not only assures that new accounts are compared with the OFAC lists prior to opening, but provides ongoing OFAC check of transaction parties, as well as screening of higher-risk customers, products, services, and geographic locations.

Sanctions risk assessments, as part of enterprise-wide AML risk assessment, should be conducted on an ongoing basis and be reassessed at least every 12 to 18 months, or sooner if there are any changes of a material nature. Through access to a DLT ledger, an examiner as an authorized user could monitor all the transactions and relevant data to assess the structure of a financial institution's OFAC compliance program and how adequately it addresses its risk profiles as determined by the risk assessment.

5. **AML Risk Assessment and Audit Risk Model**

Evaluation of adequacy of the BSA/AML risk assessment process and risk profile of a financial institution is one of the primary objectives of examination procedures. A risk-based approach requires each financial institution design a system of adequate control to address money laundering and terrorist financing it may be facing. Auditors determine whether the bank has covered all risk areas, including any new products, services, or customers, entities, and geographic locations. Part of examination is also to determine if an institution's process for a periodic review and update of its BSA/AML risk assessment is adequate.\(^\text{41}\)

5.1 **Inherent Risk**

The audit risk model for AML risk assessment consists of two essential elements: (1) *quantity of inherent risk* (the risk before controls are applied): customer risk, product risk, geographic risk; (2) *quality of risk mitigation*: detection and monitoring risk, identification and verification risk, compliance risk, and regulatory/prior audit risk. Inherent risk is reduced by control effectiveness and results in *residual/AML audit risk*, i.e., risk that remains after preventive methods of control are applied.\(^\text{42}\)

5.1.1 **Customer Risk and Special Considerations**

A major inherent risk for each financial institution is *customer risk*. Addressing customer risk is a central piece of the customer due diligence protocol and the entire AML compliance program of a financial institution. Customer risk is a risk associated with customers and/or businesses due to the nature of their business, occupation, size, legal organization, or anticipated transaction activity. Customer risk is a major potential risk during money laundering layering or integration stages. Higher risk customers occur when financial institutions and legal vehicles (e.g., offshore banks, trusts and private investment companies) offer confidentiality and intermediary services.

Why know your customer? There are three major reasons: KYC failure may lead to regulatory non-

---

\(^{41}\) https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_006.htm

\(^{42}\) Acams.org ACAMS Advanced Certification Risk Assessment - The Foundation
compliance, financial loss, and reputational loss. To mitigate customer risk, first and foremost financial institutions should adopt account opening procedures that allow them to determine the true identity of customers and to develop an understanding of normal and expected activity for customers’ occupation or business operations. They also should set identification standards customized to the risk posed by particular customers.

Customer risk rating models as a part of enterprise-wide risk assessment play two significant roles:

- **It is a consistent method for differentiating among individual risk areas;**
- **It determines the level of diligence required:**
  - Low risk (“simplified” or “standard” due diligence)
  - Medium risk (“simplified” or “standard” due diligence)
  - High risk (“enhanced” due diligence)
  - Prohibited customer

As stated in the FFIEC Examination Manual, banks "should monitor their lower-risk customers through regular suspicious activity monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), management should reassess the customer risk rating and follow established bank policies and procedures for maintaining or changing customer risk ratings.”  

Under the current market infrastructure, most of the CDD information is confirmed by information-reporting agencies, through banking references for some larger accounts, phone interviews with the customer, and sometimes visits to the customer's place of business. Among other steps may be getting third-party references or researching Internet or commercial databases.

As we've already covered in this paper, deployment of cutting-edge and innovative distributed ledger technology may assist the financial institution in completing its responsibilities under applicable CDD/KYC regulations. Since all data related to a specific customer is indexed on a ledger in the format

44. Ibid
of immutable and authentic records, and smart contracts encapsulate business logic in each financial event and add different coding in DLT for different financial circumstances, blockchain networks can help to identify potential customers, transactions, and accounts, especially when this concerns high-risk customers. DLT can assist in monitoring high-risk activity, conducting investigation, and streamline the process of customer risk review and examination. Automation of certain CIP/KYC processes through a blockchain ledger has the potential across the industry and through numerous networks to have access to millions of individual profiles, as well as profiles of legal customers, which are especially important considering the upcoming FinCEN CDD Final Rule going into effect in May 2018. The blockchain might provide solutions to appropriate profiles and identify ultimate beneficial owners, updating risk scoring for ongoing due diligence and decreasing the amount of manual and labor-intensive review necessary on the customers and the risks they pose. Here, of course, there are numerous issues in a rapidly changing regulatory landscape regarding how DLT meets regulatory requirements while improving efficiency in monitoring the right transactions and investigating the right clients.

Under the condition that DLT has no issue of interoperability, it has the potential to afford a financial institution the ability to navigate seamlessly around client relationships, accounts, and transactions across a variety of product lines and systems. This may play a paramount role in mitigating customer risk with special considerations and deliver fast, reliable, and efficient access to relevant data regarding governmental entities, embassies, public figures, charitable organizations, trusted entities and high-risk entities.

High-risk customers are required to conduct Enhanced Due Diligence (EDD) where understanding of their expected transactions and ongoing monitoring of their activity is a matter of significant importance. Here, a regulator or examiner might have access to a broader range of information already being recorded on a ledger. A detailed audit trail and the self-regulated nature of each recorded financial event will play a role of business intelligence and become a valuable feature for conducting EDD, which in turn may enhance compliance.

5.1.2 Product Risk

Next after customer risk, among the types of inherent risk in the AML audit risk model is product risk: this risk is associated with the nature of products or services offered. Such products and services typically:

1. favor anonymity or involve third parties,
2. support high-speed movement of funds,
3. support high transaction volumes,
4. involve cross border transactions,
5. involve cash, monetary, or bearer instruments.

An effective AML program has systems in place to determine what products and services, which a financial institution offers, might expose it to money laundering or terrorist financing. These can be internet accounts, private banking, stock brokerage services, annuities, or insurance products. Assessment of product risk as an inherently risky area is an essential part of surveillance functionality and will continue to be a priority in the examination process.

Product risk should be reviewed for relative importance to other risks and in the management of the entire risk profile of the business. When different risk categories are summed up, it gives a 360-degree view of a customer's risk profiles. Product risk for a small foreign private firm and the same product risk for a well-established local business may be two different things.

The more high-risk products a financial institution offers, the higher its risk rating should be. Deep
understanding and monitoring of high-risk products and mitigating the AML risk they present is a very complex task, particularly if a customer and especially a legal customer has a number of accounts and uses numerous products and services on an ongoing basis. Current challenges with product risk in existing CDD/KYC landscape include an issue of high concern for the reputation management of a financial institution.

More regulatory standards and future compliance obligations require the use of cutting-edge technology to address product risk and put in place appropriate measures for its control and mitigation. It is too early to assess the full potential of DLT as an innovative solution for mitigation of different types of AML risks, since the technology is in its nascent stage. However, blockchain ledger as an immutable and authentic record of each financial transaction, therefore reflecting each product and type of services, will be a single true data source for regulators and other interested parties in addressing product risks, key issues, and challenges. Also, blockchain technology might optimize or even streamline product risk rating, since smart contracts will instill business logic into each transaction and can apply to DLT different coding for different types of products and services. Embedding risk rating at the level of DLT can significantly simplify surveillance and examination processes, enhance monitoring of high-risk activity, and demonstrate ongoing compliance efforts.

5.1.3 Geographic Risk

Geographic risk is another type of inherent risk which might significantly expose a financial institution to money laundering and terrorism financing, especially in countries with inadequate anti-money laundering control. It is evident that a customer from a geographic location which is not cooperating in global money laundering efforts inherently presents a higher risk to financial institution. There are several major factors contributing to the lack of cooperation of some countries in the international fight against money laundering and terrorism financing: loopholes in financial regulations, no or inadequate regulations or supervision of financial institutions, inadequate customer identification requirements for financial institutions, excessive secrecy provisions, lack of efficient suspicious transaction reporting, lack of identification of the beneficial owners of legal and business entities, obstacles to international cooperation, and inadequate resources for preventing and detecting money laundering activities.46

Developing DLT applications can assist the financial industries in meeting their obligations towards mitigating geographic or country risk and ensure the best overall results in compliance with anti-money laundering and customer identification programs. This might be an effective solution to identifying factors that contribute to the type of risk, and, through ongoing monitoring, to better guard against money laundering, especially related to laundering of proceeds from corruption.

Since there can be only one identity profile on a ledger for an individual or a legal customer regardless of where they are in the world, this might provide a solution to the issue of trust and put a financial institution at ease with questions like, “Are you who you say you are?”, “Are you where you say you are?”, and “Will you do what you say you will be doing?” So, next time Mohamed Ahmed, who is a neurosurgeon in the US, will not be confused with a person of the same name from a country or a region that may present a heightened risk of money laundering. Identity profiles on a ledger will be linked to jurisdictions which may be associated with higher levels of corruption and in turn through automation will contribute to more effective risk assessment and reporting of suspicious transactions.

46. ACAMS Certification Examination 5th Edition
Authentications of records with private key cryptography provide a powerful ownership proof. Through authentication and then obtaining a permission, blockchain technology has the potential to solve the problem of trust which is on everybody’s mind. Having proof of ownership and authorization, regulators and auditors can operate in a new digital reality. They can use DLT to assess how effective a financial firm is in detecting corrupt assets moving through the network and to improve prevention of conversion of corrupt assets into a usable format. Here, distributed ledger technology is capable of tightening and enhancing money laundering control and reducing geographic or country risk. This in turn can protect the integrity of the entire financial industry, improve international AML efforts, and effectively implement all FATF Recommendations against laundering of proceeds of corruption.

In addition, Blockchain ID as a type of DLT can objectively mitigate geographic or country risk through eliminating the problem of flawed passports and driver’s license issuance in all countries across the globe. If scientifically proven and immutable identities are attached to each account and each transaction, it is certain to become more difficult to move money undetected and be involved in corruption-related activities in the first place. This might be good news for the entire international anti-money laundering community, regulators, and other interested parties.

Dealing with geographic or country risk, risk scoring can be put into DLT using corruption measurement indexes based either on specific jurisdiction or specific factors. Most famous here is the Corruption Perceptions Index (CPI) which provides a ranking of over 180 countries and is published by Transparency International, the global coalition against corruption. Even though currently DLT is not utilized as an anti-corruption tool, immutability and transparency of information recorded on a ledger, as well as different coding put into DLT regarding risk scoring, make it difficult for bad actors to manipulate the data for their illicit purposes and therefore reduces types of risks associated with fraudulent activity. This also includes sanctions risk, which should be reviewed on an ongoing basis and be reassessed by financial institutions at least every 12 to 18 months, or sooner if there are any events of a material nature that occur.

5.2 Risk Mitigation

The quantity of inherent risk as a risk associated with customers, products, or geographic areas is measured with no consideration of the existing system of control and which by default cannot be transferred away. This is one part of AML risk assessment and its components. Another part of the audit risk model is quality of risk mitigation, which, after considering inherent risk, defines the residual risk.

Among components of AML risk mitigations are:

- **Identification and Verification Risk** - risk associated with the ability of the financial institution to form a reasonable belief that it knows the true identity of each customer;
- **Detection and Monitoring Risk** - risk associated with how financial institutions monitor, detect, and report unusual or suspicious activity;
- **Compliance Risk** - defined by how mature the compliance program is, which covers policies and procedures, risk assessment, compliance monitoring, testing, issue management, and training;
- **Regulatory/Prior Audit Risk** - refers to prior regulatory examinations or internal audits.

47. ACAMS Advanced Certification CAMS-Audit
5.2.1 Identification and Verification Risk

Identification and verification risk are in direct relationship with customer due diligence. They require a financial institution to have processes for obtaining and identifying customer information at the account opening stage, as well as procedures based on specific risks for verifying the identity of a customer. Different financial institutions demonstrate CDD/KYC/CIP/EDD/OFAC processes that show either mature control, and therefore low identification and verification risk, or controls that require improvement or even considerable improvement over ensuring that all required information and documentation is obtained, which increases this type of risk and in turn increases the residual risk. Failure to impose effective CIP/KYC protocol and therefore to mitigate identification and verification risk keeps a financial institution very vulnerable to money laundering, increased regulatory scrutiny, and potential imposition of monetary penalty for violating the Bank Secrecy Act (BSA) and USA PATRIOT Act.

Violation of CDD/KYC norms and AML measures can lead to substantial fines or administrative sanctions, not only because the violating financial institutions might show facilitation of transactions involving money laundering or financing of terrorism, but because of deficiencies in the financial institution's AML control measures. The objective of independent testing under anti-money laundering provisions of the USA PATRIOT Act, relevant rules and regulations established and enforced by the US Treasury, Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), is exactly to assess whether the financial institution has adequate CDD/KYC/CIP/OFAC control in place as required to combat acts of money laundering and financing of terrorism.

To comply with regulatory requirements regarding identification and verification risk, the testing includes a review of the following mandatory CDD/KYC components: customer identification, review of required OFAC and FinCEN lists, customer files for evidence of verification of identity and OFAC review, and books and records retention. Examination of these select areas can result in discovery of material findings and weaknesses, and when communicated to the management and properly rectified, will assist financial institutions in avoiding repeat occurrences in the future and significantly reduce residual risk.

Use of blockchain technology by market participants to enhance their CDD/KYC regulatory obligations may be a pathway to gaining a competitive advantage, even though there are numerous questions that should be addressed by IT teams, regulators, and auditors in connection to DLT deployment. Strategic implications of this new technology have the potential to change how companies approach and mitigate identification and verification risk and handle the most complex situations with higher risk customers, legal entity customers, and their multi-level ownership structure, as well as with customers with special considerations.

In time, DLT can be viewed as a game-changer not only for market participants, but also for regulators, examiners, and other interested parties. In regard to identification and verification of a customer, DLT will provide to the examiners much more data than they have access to currently. This can result in not just sampling testing, but review of the whole universe of data. Also, because of verification of each entry of a customer ID on a ledger, consensus among network users, and immutability of recorded information, DLT might provide a solution to the problem of data quality, which is a widespread industry issue. High-quality data in turn can secure more accurate findings identified during the testing. Additionally, since each customer or legal customer ID profile will be attached to each account and each financial transaction, an examiner will have the opportunity to track and review data in other fields and therefore to
have a complete look at a customer profile, providing a better assessment of identification and verification risk.

5.2.2 Detection and Monitoring Risk

Among the commonly-cited weaknesses regularly discovered during AML audits is the issue of risk assessment, which does not consider all major risk categories, specifically detection and monitoring risk, which are defined as an ability of the financial institution to monitor, detect, and report unusual or suspicious activity. This is one of the major AML risk mitigants and essential components of audit risk model. Market participants that show ongoing quality surveillance, effective case management, and mature processes of detection of suspicious activity and its timely reporting, have the lowest risk rating and can significantly reduce residual risk. Financial institutions without a fully effective detection and monitoring system, or which require significant additional measures of control, can substantially accelerate their own reputational, regulatory, and legal risk.

Testing how a financial institution handles detection and monitoring of suspicious activity as a part of its AML compliance program is a mandatory component of any AML audit and includes monitoring of customer transactions/accounts, identification and reporting of suspicious activity, reviewing of reporting files, the AML supervisor's record regarding the monitoring of any transactions or accounts, and related notes on follow-up or other findings.

During the process of assessing the quality of detection and monitoring risk mitigation, auditors expect to have and review certain types of evidence to help support the implementation of AML policies and procedures and to learn how a financial institution follows its risk metrics. The more evidence the auditor collects, the more of a solid base there is for examination findings of nonconformity, and therefore the stronger the confidence in the quality of recommendations. Here, blockchain technology can change the current protocol regarding how much data audit experts can review in a short time, given the number and complexity of transactions and financial activities. To take this a step further, for certain types of detection and monitoring testing, through use of DLT, regulators and examiners will no longer be limited to sampling but will be able to review the digital footprint of all financial activities for each customer and each account. This will allow examiners to concentrate their efforts on select risk areas which increase the odds of discovering shortcomings and examples of non-compliance. This tremendous benefit of blockchain technology can greatly increase the quality of exams of financial institutions with lack of effective surveillance and which require substantial additional control to mitigate detection and monitoring risk.

Additionally, the horizontal governance structure of DLT networks will afford regulators and examination staff the ability to view all relevant data to better support investigations, case decisions, and suspicious activity reports, increase quality of monitoring, and instantly communicate with compliance and surveillance personnel. In the examination landscape, DLT might offer a better experience for examiners, greater convenience, and the opening of new opportunities for exploring use cases in protocol for detection and monitoring risk.

Consensus processes, which include confirmation of each financial event by blockchain network participants simultaneously, might reduce the necessity of having intermediaries, reduce the number of
errors, and, therefore, simplify the examination process for transactions monitoring. Of course, it might also present the issue of possible ledger manipulation if network users are eager to facilitate fraud. This might trigger potential regulatory challenges related to adoption and deployment of distributed ledger systems.

5.2.3 DLT and Risk Assessment

Risk assessment is viewed as a foundation of the entire independent testing framework and a major component in the evaluation process of the quality and effectiveness of a financial institution's BSA/AML program. It is a backbone of any adequate AML compliance program and a core of the examination process. Even though every financial institution has been required to perform and document a written BSA/AML risk assessment, there are still grey areas and a lack of specific guidance regarding how risk scoring should be applied. As we specified earlier in this paper, total risk score is determined by multiplication of risk factors for certain type of risk and appropriate relative weightings of these risk factors. Risk scoring can serve as a valuable and objective measure of risk assessment and a key to better understanding and evaluating a financial institution’s risk exposure.

Potential DLT applications can offer regulators and auditors numerous benefits in providing testing of BSA/AML risk assessment, CDD/KYC/CIP compliance, and reviewing a financial institution’s risk assessment as a part of AML independent testing frameworks. This in turn can assist examiners in determining how a financial institution’s AML practices coincide with its written policies, procedures, and processes, and therefore address an issue of compliance risk - another risk mitigant.

Smart contracts, as one of the main DLT features, and their ability to embed business logic in each transaction, can bring and apply this idea to any need for a trustworthy system of record. This includes the possibility to connect international AML standards, country laws, regulatory provisions, and specific company policies and procedures. They can also significantly enhance sanctions risk mitigation through effective and ongoing OFAC name screening. Of course, reliance on linked technology may have associated with security limitations and this should be addressed.

DLT can bring a whole new digital reality to the examination process when auditors, through configurations of blockchain technology, will be able to disseminate new typologies and risks discovered during the testing process, recommend specific adjustments to control measures, due diligence and enhanced due diligence protocol, and help financial institutions to more effectively and in a timely manner detect, report, and prevent potential financial crime and illicit activity.

As we covered earlier, the deployment of distributed ledger technology can significantly reduce types of inherent risk - customer risk, product and service risk, and geographic risk, and through effective identification, verification, detection, monitoring, and other control measures, will significantly reduce the financial institutions’ residual risk. Since specified client activity can be embedded in smart contracts, this might trigger a specific risk factor upon the conditions of such an activity having been met. This in turn might provide a robust solution to the testing of the design, completeness, and execution of AML/KYC risk assessment and therefore determine if risk assessment properly reflects money laundering risk exposure and is tailored to the specific CDD needs of a given financial institution. This will afford an auditor the ability to better identify deficiencies and gaps in existing control measures and make appropriate recommendations for improving AML compliance programs.
While blockchain technology will be gradually settling into place, regulators and independent auditors will be adjusting their testing protocols accordingly. Based on DLT’s potential benefits, authenticity, and the immutability of network records and use of smart contracts, distributed ledger systems can assist an examiner to help him or her better identify features that might increase or decrease inherent risk, analyze elements that contribute to risk assessment, and improve the quality of risk mitigants. This in turn can afford examiners the opportunity to be equipped with better data analytics when reviewing financial institution’s CDD/KYC risk assessment, to know in-depth who its customers are, prepare adequate AML audit plans, and deliver better recommendations regarding where residual risk falls in the institution.

DLT can also provide a positive influence on another very important segment of AML risk assessment and development of a risk model: its audibility. One of the biggest problems here is the financial industry-widespread issue of poor data quality, which arises from duplication of records, records that are incomplete, inaccurate, or have conflicting data, and records which are frequently placed elsewhere besides an easily accessible place. Poor data quality makes auditing more difficult and has a negative influence on key audit aspects, specifically their objectivity and their validation of risk models considering regulatory requirements regarding model development, implementation, use, and control. Since quality of data is viewed like other types of risk, CDD risk models developed based on poor data quality can have more limitations and lead to poor business and strategic decisions, weak AML control, non-compliance, and, therefore, possible financial losses.

Since each customer record in DLT presents a chain of all events in connection to that customer in one dataset, in an immutable format and a sequential manner, it can provide a solution to the problem of poor data quality and therefore improve objectivity as a key audit consideration in the development of a risk model. Good data quality can also afford market participants and other interested parties the ability to supplement the results of their model performance with other information and data analytics, adding minimum risk. In addition, consensus among blockchain network participants for each entry on a ledger based on powerful cryptographic code has the potential to make a network a self-regulated system, which can make a positive impact on key audit elements, as well as on managing and monitoring risk models. This positive implication of DLT on auditability of risk assessment can be a game-changer for the entire process of testing BSA/AML risk management and the evaluation of its integrity and effectiveness. Of course, practical applications of distributed ledger technology and its implications on risk modeling is a topic for another white paper, which we may consider writing.

6. CDD Audit Process and effect of DLT

Risk assessment review is a significant part of the audit process, specifically regarding the planning and scoping as a first stage of the examination protocol. Its other two steps are fieldwork and testing, as well as recommendations and reporting. It is clear that the fast pace of technological changes and application of
Distributed Ledger Technology: Streamlined CDD Examination Process through Blockchain Application

blockchain technology in the securities and financial services industry in time will make examiners adjust their audit model and impact all stages of the audit process.

6.1 Planning and Scoping

Other than review of risk assessment, a big component of the first stage of the examination process is understanding the financial institutions’ operations and applicable AML regulatory requirements and expectations, and determination of an audit objective. As we previously discussed in this paper, and as it is stated in the Anti-Money Laundering Examination Manual, the overall objective of customer due diligence examination is to "assess the appropriateness and comprehensiveness of the customer due diligence policies, procedures, and processes for obtaining customer information and assess the value of this information in detecting, monitoring, and reporting suspicious activity." Current scoping and planning processes include understanding the audit coverage and the quality and quantity of transactional testing, finding areas requiring greater or lesser scrutiny, and identifying when expanded examination procedures may be necessary.

Blockchain technology has the potential to simplify onboarding processes, ensure instant access to sufficient customer information, and minimize the amount of inaccurate data. It also has an ability to assist in setting up and adjusting risk profiles, especially for higher-risk customers, and therefore to improve the effectiveness of ongoing monitoring or suspicious activity.

All these potential benefits of DLT come with numerous additional concerns and risks, which auditors should address. In addition, distributed ledger systems themselves as an innovative technology requires including testing when determining audit objectives and scope. This obviously will require enhanced knowledge and engagement from the auditor with regard to DLT as new technology over maintaining the traditional approach.

Blockchain technology has the potential to simplify onboarding processes, ensure instant access to sufficient customer information, and minimize the amount of inaccurate data.

Among new issues and challenges brought forward by deployment of DLT are those which might specifically affect planning and scoping stages of the audit process:

- How could compliance with applicable CDD/KYC regulatory requirements and expectations be ensured using DLT?
- How is DLT platform maintenance ensured?
- Who determines DLT protocol?
- How might any gaps in DLT functioning for collection and sharing of data and reporting purposes be identified?
- Does the DLT platform provide auditors with access to relevant data in real time?
- Is all information required by regulators available in blockchain ecosystems?
- How do authorized parties of the network attain the appropriate access level?
- What are the provisions of access to the network?
- How is trustworthiness of network participants determined?
- How often is customer information verified and tested?
- How does a financial institution ensure CIP data protection and confidentiality?
- Are there any factors outside of DLT affecting customer data transparency?
\begin{itemize}
\item \textit{How does a financial institution address risk of use, management, and storing of private and public keys? If a key is compromised, who will be responsible and how will illicit transactions be traced and reversed?}
\item \textit{How does a financial institution establish and maintain supervisory and surveillance in a DLT platform?}
\item \textit{What will be the evidence of review and monitoring by authorized compliance staff?}
\end{itemize}

Above is just a short list of concerns specifically related to DLT deployment which in time might impact examination protocol and make regulators and auditors adjust their testing framework and their choice of in-scope items. Those additional questions will help the auditors to better understand their business operations, review the results of previous internal audits and regulatory exams, make a comparison, and conduct planning sessions with financial institutions’ AML Compliance Officers and other key personnel.

6.2 Fieldwork and Testing

The center piece of \textit{fieldwork and testing} as a next stage of audit processes is to review applicable AML/CDD policies and procedures, select their key provisions and test them for operational application. With DLT deployment, relevant rules and regulations could be coded in a blockchain system through smart contracts. Thanks to the code, which allows embedding of those regulations in a DLT, auditors will be able to have a much deeper look at how financial institutions’ operations coincide with their policies and procedures and applicable AML requirements and expectations, and thus better assess financial institutions’ compliance with CDD/KYC/CIP laws and regulations. This in-depth review in turn has the potential to identify some gaps in existing controls and reduce AML residual risk.

Another big advantage of using smart contracts in the audit process is their ability as a piece of self-executing code to automate operational processes and to reduce the number of errors. This gives examiners an opportunity to work more effectively with large volumes of data within a short period of time and through automation to review the total universe of data and not just use sampling.

Of course, these new exam techniques, through the use of smart contracts, might simplify audit fieldwork and testing, but a glitch in the coding can present a new type of risk and through data distribution and sharing features can affect participants of the entire network and possibly facilitate dissemination of errors. Concerns regarding flawed coding should be addressed, specifically: what measures are used by financial institutions to successfully mitigate this risk and what methods are employed in the operation of smart contracts. In addition, instillation of universal coding standards could mitigate the risk of smart contract errors and failures and make DLT more adoptable for compliance and examination purposes.

Throughout this paper, we highlighted the very important issue of differentiated and multiple levels of access to the DLT network by different types of market participants. Regulators, auditors, and other interested parties are not an exception. Through either being one of the nodes in a DLT platform or through having access to a node and private and public keys, they will be able to collect and consolidate relevant data during testing in real time from a verifiable ledger as a single source of true information. It is important to emphasize that access to DLT will obligate examiners to follow a number of requirements like any other network trusted party, act strictly according to their role and function, and follow all provisions of access to the network.

One of those requirements is about transparency, the need to ensure privacy, customer identification, and transaction history data protection. As a solution to this challenge and through the use of cryptography, DLT could keep on each node only part of the full ledger. Also, certain data sections on a ledger could be blocked and therefore assure only limited access to network users with different levels of security clearance. This technique could be viewed as a digital version of providing auditors redacted documents, currently...
used during testing protocol. Through appropriate code, it will transfer required terms of access into computational elements, possibly minimize unauthorized access, and improve compliance with requirements of privacy and data protection.

6.3 Recommendations and Reporting

After reviewing the applicable policies and procedures, preparing initial gap analysis for a management, and testing the existing methods of a financial institution's control and risk mitigation, the final step in the examination process is preparing recommendations and reporting. By having access to all relevant CDD/KYC data in the entire population of records on a blockchain and therefore having a full view and better understanding of a financial institution's operations, an auditor has the potential to present compliance deficiencies in much greater detail and supply verifiable and sequential evidence to support the exam findings. Equipped with clever automation and the ability to evaluate Anti-Money Laundering and Know Your Customer processes in real time, examiners could concentrate on matters that require immediate attention, increase the odds of uncovering issues of non-compliance, and suggest safeguards to prevent fraudulent activity.

One of the big advantages of a distributed ledger system is that through having access to one of the nodes, auditors can instantly communicate with the AML Compliance Officers and other key personnel to review the results of exam findings and discuss specific provisions of AML compliance programs related to the use of blockchain technology and their proper implementation on a firm-wide basis. In addition, communicating an exam’s recommendations in real time can result in immediate action to remedy deficiencies and strengthen an organization's AML/CDD compliance process where key components probably will be a topic of how the financial institution can ensure compliance with regulatory requirements in each DLT use case.

Since DLT could streamline collection and consolidation of relevant data during the examination, it also could potentially simplify the process of reporting work and the procedures performed during the audit and communicating findings after an in-depth testing. However, given the novelty of DLT and its application in securities and financial services industries, it remains to be seen if reporting through blockchain technology will be superior over the existing framework.

6.4 Auditor Profession: The View Ahead

Even though we don't expect major changes in the current regulatory infrastructure because of blockchain application, we all should become very DLT-proactive. Today is the best time to rethink our careers as surveillance and audit practitioners with DLT in mind and roll up our sleeves in anticipation of the significant future impact of this cutting-edge technology on financial markets. We should be very well-prepared to become a compliance pro of a new era.

Within the next five to ten years, distributed ledger systems will not only affect the entire testing framework and its components, but also the main core, the breadth and depth of auditor as a profession, and will also reshape and refine processes such as how we will approach compliance testing in the future. DLT will not eliminate need in our profession, but certainly it will change our job description. Since deployment of blockchain networks can bring powerful influence upon financial markets and in time transform the industry, it will also create a whole new competitive marketplace among compliance professionals and will
present new mandatory requirements for us to understand technological trends and innovations and become subject matter experts in order to stay ahead of competition.

So, how will the auditor profession of the future look like? Two words: TECHNOLOGY and DATA! Since DLT has the potential to simplify and streamline the audit protocol and thus put certain compliance processes out of business, our focus will be shifted towards performing other functions, specifically: leveraging fully artificial intelligence, being involved in high-order work like counter-fraud analytics and entity resolution, going after fake companies, and becoming an integral part of data mining. What will make the auditor to stand out and give him/her a pathway to gaining a competitive advantage is his or her ability to detect unseen patterns hidden in the numbers by creating models and testing whether those patterns hold up. If we know how to do this and develop good data mining skills, it is possible to discover new intelligence that could change our approach to anti-money laundering, customer identification, and due diligence for better outcomes. Our new role is not to be someone who can explain what went wrong after the fact and do in-depth review, but through clever data mining, to gain advantage, be more proactive, predict the situation in advance, and advocate for the appropriate course of preventive action. Through working with data which is more diagnostic and prescriptive, auditors and surveillance professionals will be able to empower organizations to significantly shape AML processes relevant to their business needs and therefore greatly reduce their risks, predict potential money-laundering fraud and illicit activity, strengthen financial institutions’ reputation and make tremendous positive impacts on AML wellbeing of our entire society and its future.

The future is bright, and it is the Future of Creativity! Are you ready?

7. Conclusion

As beneficial and revolutionary as distributed ledger technology could be, it also carries with it a tremendously disruptive force for financial markets, their post-trade operations and services, AML/CDD/KYC infrastructure, regulatory frameworks, and compliance testing protocol. And even though it is too early to really assess the potential benefits, risks, and unintended consequences posed by the
Distributed Ledger Technology: Streamlined CDD Examination Process through Blockchain Application

As the emergence of DLT, it is evident that blockchain technology is here to stay and gradually will become a reality for all market participants, a significant game-changer in the entire securities and financial services industry, and a strong focus of all regulators across a globe.

Since DLT in time will become a dominant model for key financial processes including anti-money laundering, customer identification, and ownership recording and validation, it will also increase complexity for examiners and compliance personnel in the long run and bring additional requirements to their jobs for specialized knowledge and skills. Technology-driven innovations in a blockchain ecosystem will anticipate you becoming a new player in the world of compliance and audit, assume you are tactically and strategically advanced, and consider business-as-usual no longer acceptable.

This paper shows why it is so important to gain this advantage and empower AML practitioners to learn a process of blockchain application relevant to AML examination and testing. It is about the hows and whys and makes the case for significant investment into your knowledge about DLT and its use in AML world, specifically for customer identification and due diligence. This report takes you step-by-step through the process of blockchain deployment, allowing you to get immediate comprehension of how DLT is applied in financial markets and why this cutting-edge technology is the financial industry's winning ticket to effective AML and CDD processes.

In summary, in regard to audits and the audit process, different members of the compliance and surveillance community are sure that deployment of DLT in financial markets will not bring significant regulatory changes in the short term. But as the blockchain ecosystem becomes sufficiently developed and widely used, it will require regulators to adapt their compliance and testing models and possibly add disclosure for financial institutions being "DLT compliant." But, of course, this is tomorrow. Hopefully, by that time, regulators and examiners will have gained expertise with distributed ledger systems through collaboration with different compliance and specialized IT professionals and have a clear vision of how to deploy blockchain along with compliance infrastructure and make it a winning strategy.

We strongly hope that after reading this paper, you will take the following ACTION STEPS:

- Reassess where you are on your career path;
- Make a lasting commitment to learning the distributed ledger system and its key implementations;
- Enhance your professional knowledge and qualifications;
- Have a clear idea of how to change your business practice to keep up with the accelerating pace of technological changes;
- Keep yourself abreast with DLT-related market developments;
- Have adequate visibility over the competition;
- Show the right attitude, be known, and succeed!

Good luck, and as one clever man said, let's, through a blockchain, “make the world a village again!”
This page is intentionally left blank