Challenges and opportunities for Auditing with Blockchain

Abstract—This paper studies the Distributed Ledger Technology [DLT], commonly referred to as ‘Blockchain’, and its impact on business transactions and audit processes, in general. The target audience of this paper includes Corporates, who are evaluating DLT for replacing their legacy applications and Auditors, who will be required to audit decentralized applications. The paper appeals to not only stakeholders who consume the work of auditors viz investors, analysts, regulators, and general public, but also stakeholders who are impacted by the speed of transactions viz customer, suppliers etc. The paper talks about the opportunities and challenges that adoption of DLT presents for operations team and auditors, alike. The study also considers the current research and development done in the field and describes how DLT has the potential to improve the efficiency of transactions and the audit process; and enable increased degree of assurance. This paper also provides the readers with a litmus test to assess the potential of introducing DLT in their business processes and further provides them a set of considerations to design a business case and implementation strategy. This paper gives a fair understanding of the audit considerations and potential changes to the audit procedures. Our study also concludes that DLT may drive a paradigm shift in auditing by transforming it from a post facto activity to a continuous activity, which will enhance the audit efficiency and degree of assurance by many folds.

Keywords: DLT, Blockchain, Trust, Risks, Implementation

1. INTRODUCTION

As defined in their publication ‘FinTech Note No.1’, the World Bank Group defines Distributed Ledger Technology as a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants. Distributed Ledger Technology is often implemented in the form of “blockchains” which can be defined as a digitized, decentralized, public/restricted register of all transactions. Each block corresponds to a set of transactions. The most recently completed transaction gets recorded and added to the existing chain of blocks in the chronological order. The market participants get an opportunity for tracking transactions thus eliminating centralized controls [1]. DLT can be divided into permissioned and non-permissioned systems. In a non-permissioned DLT, each node in the network has access to the copy of the Distributed Ledger, which can be downloaded automatically. In a permissioned DLT, only authorized node has access to the copy of the Ledger. This enables the authentication of the record by the entire community using the Distributed Ledger instead of a single centralized authority. Another benefit of the Digital Ledger Technology is its immutability with the use of sequential hashing and cryptography in synchronism with the decentralized structure. Every data block in the ledger is linked to the previous block by a cryptographic algorithm called a hash, with the linked blocks forming a chain – hence the name blockchain. This make it virtually impossible for any party to unilaterally alter any data on the ledger. However, in non-permissioned DLT, any account user can create multiple network addresses that is, perform a “Sybil attack” to cast multiple votes to validate the data updates or get involved in denial of service for legal transactions.

In real world, there exist many systems which are potential cases for decentralization using DLT. For instance, the central banks tend to modify the exchange rates by excessive buying and selling for various reasons ranging from making profits to achieving a policy objective. The presence of such a linear centralized system where a currency can be devalued or valued internally by a single control body poses a serious threat of compromise on the transparency. Introduction of Distributed Ledger Technology (DLT) addresses these issues.

2. LITERATURE REVIEW

The concept of blockchain emerged for the first time when Satoshi Nakamoto(true identity still a mystery) published a paper which never was submitted formally to a peer-reviewed journal [2]. The paper talks about Bitcoin, a cryptocurrency but the underlying technology Blockchain has shown immense potential for adoption in different fields since then. In our research paper, we are studying the changes Distributed Ledger technology will bring to Auditing. From an auditing point of...
view, we have taken the understanding of the regulatory and compliance mandates involved in the auditing of DLT in financial services from there R3 reports Applications of Distributed Ledger Technology to Regulatory & Compliance Processes [3]. R3 CEV is a DLT company which is funded by 70 global financial institutions pursuing the research and development of DLT in financial services sector. ESMA Discussion paper The Distributed Ledger Technology Applied to Securities Markets, mentions about the technology in the financial services, challenges and shortcomings of this technology, regulatory framework in the EU legislation [4][17]. Peters and Vishnia in their paper Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges have mentioned latest regulatory changes and requirements that developed in recent years. They have also given a review of different trading venue types and operations, such as Lit, MTFs and Dark pools, as well as the Limit Order Book Model which is the backbone of most exchanges. Australian Stock Exchange has already implemented and replaced their CHESS trading system with Blockchain. This has been elaborated in their consultation paper ASX’s Replacement of CHESS for Equity Post-Trade Services[5].

3. UNDERSTANDING DISTRIBUTED LEDGER TECHNOLOGY

A. Definition

Research and development efforts were ongoing on a decentralised ledger, with multiple authorized writers and a group validated transaction recording mechanism, but some problems remained to be solved until Satoshi’s publication of the whitepaper on the Bitcoin Blockchain. The accounting mechanism for Bitcoin transactions created considerable interest in due course of time and became the talk of the town as the biggest names of the technology and BFSI industries began investing in the research and development of this technology. The key features of the DLT worth attention are distributed ledger, consensus mechanism and use of cryptography.

1. Distributed Ledger: The decentralized nature of recording transactions sets DLT applications apart from the conventional client-server architecture of application design. This is perhaps the best way to keep records and not concentrate all controls with a central body or system. The nodes get an updated copy of the ledger as soon as a new block is generated and added to the Distributed Ledger.

2. Consensus Mechanism: Consensus mechanism lies at the core of DLT and ensures that the transactions entering the ledger are vetted for authenticity from origin to execution. In the distributed ledger, any node can propose a transaction to be added to the Distributed Ledger which is then validated by a node selected on the basis of the chosen consensus mechanism. Establishing consensus (i.e. validation mechanism) on the transactions also avoids any conflicts on the Blockchain as each transaction is timestamped as soon as it is validated. Some examples of consensus mechanism are proof-of-work, proof-of-stake, delegated proof-of-stake, zk-SNARK and Byzantine fault tolerant [BFT]. The consensus mechanism and sequencing protect against the aforementioned double-spend problem.

In Proof of work (PoW), non-invertible hash functions are used. In this, each validator available in the network will select authorized pending transactions. After selecting, the validator adds the set of transactions to the ledger and the updated version of the ledger is used as an input to the hash function. The new ledger is sent to all users in the network. The users in the network verify if the update only contains authorized transactions and the validator found the solution to hash function correctly. If the conditions are agreed, new version of ledger is used as a starting point for the rest of the pending transactions[2].

In Proof of Stake (PoS), validation rights are assigned to users based on their stake in the system. The measure of stake in system is different for different DLTs. Some of the possible measures of stake of the validator are the number of native tokens owned, number of particular native tokens, assets given as collateral or the reputation of validator in the restricted DLT network [2].

3. Cryptography: Cryptography is the key enabler of distributed ledger and trust-less consensus on the distributed network. The nodes are able to transact and validate transactions in the distributed ledger through the use of cryptographic hash functions and public key infrastructure encryption. At this stage, the readers should familiarize themselves with the simple yet robust concept of Merkle trees[2].

New transactions are collected in the new data part of a block (as shown in the figure 1), copies of each transaction are hashed, paired with hash, hashed and paired again and hashed again, until a single hash remains. This set of transactions, paired and hashed, is referred to as a Merkle tree. The length of blocks can be fixed at the time of setting rules for the first or ‘genesis’ block of the blockchain.

The blocks are signed with a digital signature, which connects the sender to the asset/value of the block, just like physical signatures on a contract. DLT uses ‘public key cryptography’ for digital signatures, which is a common method that is used in a wide array of other applications, such as HTTPS internet protocol. Network participants each have a private key, which is used for signing digital messages and only known by the individual user, and a public key which is public knowledge and is used for validating the identity of the sender of a transaction, by the validator of the transaction.

These three concepts help explain the fundamentals of DLT. The process by which data is recorded in a blockchain-based distributed ledger is by forming an immutable ledger of ‘transaction blocks’ in chronological order that contains encrypted values (hash function) of the transactions added to the ledger, a proof-of-X (predefined proof as per the selected consensus mechanism), and a digital signature of the hash by the sender’s private key, and public keys of the sender and the intended recipient of the transaction.

4. Study and Analysis-DLT

A. Current State of DLT implementation across industries

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times.

According to a study conducted by Accenture Consulting, (Banking on Blockchain: A value analysis for Investment Banks), financial institutions can save 70% on Central finance reporting, 50% on Business and Central Operations and 50% on Compliance with the implementation of Distributed Ledger Technology[6].

CLS, the largest provider of Foreign Exchange settlement and risk mitigation services, is one of the founding members of the Linux Foundation’s HyperLedger project. HyperLedger is an open source project where industry majors are collaborating together to build a cross-industry blockchain synergy [7]. Few big names associated with the project are IBM, CLS, Citi, JPMorgan, American Express, Accenture, Cisco, Daimler etc. CLS developed a project with IBM backed by blockchain technology for bilateral payment netting of foreign exchange trades in more than 140 currencies for buy and sell sides of the institutions [8]. The platform CLS has developed will be used for improving liquidity in currencies like renminbi and the rouble initially and not for the core settlement system of CLS, because launching core business products on untested technology is a high-risk strategy [8].

Cobalt, a startup working on blockchain based FX post trade settlement system claims it will reduce costs and risks by 80% with its solution. The startup has already found dominant market players as riders for its blockchain backed bandwagon of innovation. Cobalt is planning to start testing it’s platform with 22 major banks and traders, Bank of America, Union Bank of Switzerland (UBS), Deutsche Bank, and Merrill Lynch, to name a few.

CitiGroup, Deloitte and DCG backed startup, SETL aims to create a blockchain based platform for settlements and payments [9]. SETL has come up with a solution which will improve efficiency of settlement and payments processes, reduce the costs of trades, reduce the involvement of multiple systems in asset ownership transfers, streamline the processes across asset classes, provide more accurate and just in time data on asset movement and industry transactions. Last but not the least, it provides a single view of post trade data that will help in efficient and low cost analysis of past trends in trades and transfers [9].

NEX group has overhauled its post trade services vertical and created cloud based solution which will use blockchain and artificial intelligence to reduce costs and risks for complete transaction lifecycle. The company recently began allowing clients to test the platform. NEX Infinity serves a single view for clients and third-party providers to access the post-trade services of the firm. It also centralizes the view of the information for all trade and portfolio processing requirements throughout the transaction lifecycle.

Nasdaq came up with Linq blockchain ledger technology with help of a startup, Chain.com to perform and record private securities transactions. Citi Bank collaborated with Nasdaq to create a distributed ledger to record and transmit payment instructions which also uses the same underlying blockchain technology. The salient feature of the solution is it reduces the challenges of liquidity in private securities as it has streamlined payment transactions between various market participants. However, the technology has not been mainstream for Banks for the time being. Right now, the distributed ledger is also perceived as a way of facilitating alternate payment mechanism if traditional settlement system sees a disruption.

Australian Stock Exchange (ASX) has decided to utilize distributed ledger technology based solution for post trade clearing and settlement activities. Blockchain startup Digital Asset Holdings has developed the solution under consideration for Australian Stock Exchange. Through a series of systematic investment, ASX has acquired an equity of 8.5% in Digital Asset Holdings as well. Infact, Australian Stock Exchange has decided to replace its 20-year-old and proprietary Clearing House Electronic Subregister System with distributed ledger after considering its wider application across different sections of the market. After two and a half years of rigorous brainstorming on the DAH’s solution, ASX has finally decided to move to distributed ledger completely from CHESS. ASX is expecting to reduce cost and lead the innovation by synchronising finances with the introduction of blockchain technology[5].

Japan Exchange Group is working with IBM to evaluate the IBM’s open source blockchain project HyperLedger for trading and settlement in low liquidity markets. A consortium of thirty-three financial institutions have come in agreement with JBX to collaborate to assess the potential of distributed ledger technology in capital markets landscape [12].

The inherent benefit of implementing such a transaction system was that it ensures confidentiality and improves throughput performance at the same time. The performance boost is achieved as only the interested parties are executing the transactions. Another important benefit of the new approach is that the transactions can be executed in parallel and relaxation in the rigid consensus process which needed to happen on all nodes of the network initially.

Korean Stock Exchange has come up with a Blockchain based platform for trading equities of startups in open market. KSX has been exploring the opportunity to leverage blockchain technology in the new context since 2015, and has launched Korea StartUp Market(KSM) with blockchain as the underlying platform developed by a startup named Blocko. Blocko has come up with a Blockchain-as-a-service(BaaS) platform named Coinstack. The platform will enable document and
authentication services for cross reference with the information provided to the platform by Korean Banks.

Moscow Exchange (MOEX) has managed e-voting for bondholders via blockchain solution based on NXT distributed cryptographic platform at the National Settlement Depository (NSD), a member of MOEX. MOEX joined HyperLedger project in 2016 and was first such financial institution from Russia.

Santiago Exchange is the first financial institution in South America to implement blockchain technology. Santiago Exchange has partnered with IBM to build a solution for its short selling system for securities lending.

TMX Group announced a prototype based model with blockchain as the underlying technology. The prototype will be designed for its subsidiary Natural Gas Exchange(NGX) [13].

The solution will enable tracking of natural gas flows at delivery locations with the help of distributed ledger technology by enabling transparency in delivery and payment processing.

B. Assessing Business Impact of Distributed Ledger Technology

In this section we have suggested ways to assess the existing business processes and carefully determine the feasibility and need for DLT adoption. In order to envisage potential use cases of the DLT, readers should bear in mind that the intrinsic quality of DLT is that:

- Increases Confidentiality: DLT based applications enable multiple parties who do not fully trust each other to safely and directly share a single database without requiring a trusted intermediary.

- Enables Disintermediation: All participants in a DLT network see all of the transactions taking place.

While some readers may argue that this leads to trade-off of confidentiality to achieve disintermediation, these qualities make DLT the technology of choice for applications which may function on a shared database architecture as against conventional centralised databases.

Further, use-cases of DLT may be determined largely in the following 4 Types:

1. Financial applications or asset transfers: The Distributed Ledger implemented for financial systems may solve problems of double spending and fraud in case of asset transfer. This combined with the security of a decentralised ledger make up for a viable use case for applications where movement or allocation of physical assets is not practical and there are no settlements / reconciliation required in case of DLT.

2. Tracking of authenticity: In scenarios where the origin, transit and destination/consumption of any product/asset is required to be tracked, DLT applications could come into play by generating a token at the origin of the product/asset through an authorised channel and by an authorised party. The state of this token changes as and when the tracked product/asset changes owners and reaches its final destination. Such scenarios may be easily found in consumer products and financial services industries.

3. Record keeping for inter-party transactions: In business processes where transactions occur between parties which do not trust each other and outcome of business processes are dependent on the existence and timing of such interactions. Since the parties are no-trusted, having a DLT application in place will ensure availability and immutability of the record of transactions. While designing such applications, the decision makers should consider the timing, nature and extent of data shared across to all parties.

4. Multi-party shared ledger: This scenario is difficult to implement and rare in occurrence, but may lead to higher savings in operational complexities and costs. In scenarios where vast volumes of data are recorded, accessed and analysed, a DLT applications could be deployed to store a portion of the data and supply whenever unauthorised node makes an authorised request. Having such implementation shall ensure that redundant copies of the data is available and the application is failsafe. The extent and amount of data to be stored on a single node should be carefully determined while designing such applications.

While applications of DLT can be numerous, they should first be assessed basis the above categories and if they do qualify to be feasible, they should be presented to the management in the form of a business case and implementation strategy. Considerations to bear in mind while designing the business case and implementation strategy are detailed in the following section.

C. Implementation Considerations and Challenges

In order to decide on the feasibility of implementing a DLT solution, following aspects should be considered by decision makers.

- Governance: This is perhaps the least researched and most talked about topic of DLT where players of the ecosystem seldom do not reach a consensus. Several research papers have focused on ways to maintain decentralization in terms of the entities that enforce the rules, although in more general distributed ledgers it is still very much an open question how to incentivize participants to help maintain the ledger. Further, more clarity is required on the roles of the players / nodes in DLT.

- Privacy: One of the simplest solutions is to send transactions to only those participants with whom you trust the associated details; this is akin to the sharding based solutions. Even here, however, it is still important to consider privacy, as transactions may be shared beyond the initial set of participants, or it may be necessary to hide certain details from one participant but reveal them to another. The nature and extent of data/transactions stored on the DLT based application play a key role in deciding privacy considerations. This may lead to overheads in terms of cost of implementation and cost of regulatory compliances and certifications.
Compliance: In certain applications, it may be sufficiently important to provide full auditability (for example, to satisfy regulatory requirements) that we cannot help but increase the storage load of participants. Especially in consumer applications, however, a relatively compelling case can be made that is not actually necessary to store every transaction, as — for example — we are unlikely today to want or need to meaningfully examine someone’s coffee purchases from early 2010. Application designers and architects should carefully consider the need to store and reproduce data while designing the proposed applications.

Cost-effectiveness: The consensus mechanism, storage requirements, architecture and related algorithms have a direct bearing on the cost of implementation of the proposed application and hence these factors should be carefully considered while executive decisions are taken on the implementation of DLT based applications.

Scalability: The biggest hurdle for fully distributed ledgers is the insistence that every node in the network needs to agree on the full state of the entire ledger. This means that distributed ledgers cannot and do not scale in terms of their ability to process growing numbers of transactions (throughput) while still ensuring that users do not have to wait for their transactions to be included (latency). This is precisely because of this requirement that every node must agree on every transaction, as it means the more transactions are in the system, the longer the nodes must wait for them to flood the network.

Interoperability: Within the realm of platforms based on blockchains, the idea of a sidechain provides a simple way to translate actions from one blockchain into another: i.e., to have transactions published in one ledger have an effect on another ledger. The security of these sidechains has been relatively unstudied to date, however, and while they have attracted significant attention they have not yet seen much adoption. The need for sidechains should be identified in proposed applications and considered in the design and architecture.

Consensus mechanism: The natural issue that arises in such an increasingly crowded landscape is how to distinguish between these solutions and pick the one that is best for a given application. Do you need a DLT, blockchain, or just a database? Maybe an Excel spreadsheet is sufficient for what you need to do? Do you need full public verifiability (and if so, why)? Even if someone could specify a list of necessary properties, it is not still not clear which current platforms support which properties, and to what extent?

Transaction Management: As more and more mainstream applications of tokens and wallet are being proposed, it becomes imperative that a mechanism be devised to protect the integrity of the user’s data while also be humanly possible to remember and move across systems. It is also still an open problem to identify solutions in which one could regain access to lost funds with the same ease with which users currently regain access to accounts for which they have forgotten the password. The proposed applications should make transactions simpler and reduce possibilities of loss of stored assets / value. The designers should assess the impact and workflow of sharing keys.

Agility: Eventually, computers may become powerful enough that can crack the algorithms being used to implement Distributed Ledger. Let us assume will not be considered secure. Maybe quantum computers will come along soon and allow anyone who has one to break in say Bitcoin’s underlying Blockchain by forging ECDSA signatures or by breaking hashing function SHA-256. While there will likely be sufficient warning before either of these events to give the developers time to switch to more secure alternatives (and anyway the problem would go far beyond distributed ledgers!), there is an argument to be made for providing users with multiple options even today, just as is done with systems such as TLS. As with TLS, however, agility can enable dangerous attacks, so significant caution is needed in both how it is implemented and in which cryptographic primitives are supported. Perhaps because they are unencumbered by the ideological mindset frequently encountered in cryptocurrencies, industry-led distributed ledgers are much more agile. In Corda, for example, an individual user can pick from a selection of available algorithms when forming a contract. Hyperledger Fabric allows participants to put their own consensus protocol. The proposed application of DLT should carefully select the factors which constitute the consensus mechanism and related algorithm.

Usability: In the current state, the DLT technology lacks nice interfaces and certainly needs expert knowledge to work on. Thus making its adoption limited to few. This, however, is the case with any new technology which enters the market and grows with the right ecosystem of developers, designers and consumers. The proposed application should be user friendly and robust at the same time[10].

5. UNDERSTANDING AUDIT

Audits performed for companies may be classified largely into the following 2 categories:

5.1.1. Internal Audits

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. (IIA)These audits are risk based audits, generally performed by and internal independent audit function reporting to the audit committee, as part of the board. The subject matter of these audits is the business processes which are carried out in the course of the business for the company, and the systems used to carry out these processes and transactions. The role of internal audit is to provide...
independent assurance that an organisation's risk management, governance and internal control processes are operating effectively.

Internal audits are based on risk of process failure to stop, detect and/or correct process non-compliance and fraudulent activities within the company. The internal audit reports are not meant for public consumption and are generally produced to the audit committee as part of their corporate governance proceedings.

The core principles of internal auditing, as described by (IIA) are as follows; they articulate internal audit effectiveness and they should all be present and operating effectively:

- Demonstrates integrity.
- Demonstrates competence and due professional care.
- Is objective and free from undue influence (independent).
- Aligns with the strategies, objectives, and risks of the organization.
- Is appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement.
- Communicates effectively.
- Provides risk-based assurance.
- Is insightful, proactive, and future-focused.
- Promotes organisational improvement.

5.1.2. Financial Statements Audit

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is “Heading 5”. Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one tier. Financial statements audit should be perceived more than just an exercise by the auditor to check that sampled transactions have been accurately recorded in a general ledger. However, performing a test of accuracy of a transaction is just a small part of the audit—and only a fraction of an audit’s value.

In the context of preparing and auditing financial statements, a recorded transaction is only considered valid if it is supported by evidence that is relevant, reliable, objective, and verifiable. Enhancing confidence and trust in a set of financial statements is a much more robust and complicated task that requires the expertise, judgment, objectivity, and skepticism of an external auditor. A critical question is not just whether a transaction was accurately recorded, but also whether and how the transaction should be presented in the entity’s financial statements. The system of trust between a management team that is using an entity’s resources and the investors who provide those resources is based on the faithful representation of that entity’s performance in the financial statements.

Ross L. Watts commented on this in Corporate Financial Statements, A Product of the Market and Political Processes: “the origins of accounting... are probably to be found in the need of an ‘accounting’ officer to render a statement of money and other assets received... There was a need for a check on the honesty and reliability of subordinates.” Watts further termed “the idea that the purpose of accounting is to check the honesty and reliability of agents as the ’stewardship’ concept.”

At least for the foreseeable future, only an appropriately trained and skeptical professional can provide adequate assurance to contribute to this delicate system. Regardless whether financial reporting is executed predominantly by human or machine, both can, and will, have errors if left unchecked.

The public looks to external auditor CPAs to enhance trust in the companies they audit. CPAs practice under strict regulations and standards, and are independent of the entities they audit. CPAs apply objectivity and professional skepticism to provide reasonable assurance whether an entity’s financial statements are free of material misstatement, and whether a company’s internal controls over financial reporting are operating effectively.

The auditing of financial statements of a company is preceded by a crucial step of assessment of the integrity of the systems being used to record transactions that impact financial reporting and how business system controls i.e. automated controls or internal controls over financial reporting [ICOFR] have been implemented. The auditors design appropriate testing methodologies for automated controls and general computer controls according to their judgment and degree of confidence. These procedures are generally a combination of inquiry, inspection, re-performance and observation. The outcome of this initial assessment has a bearing on the audit approach to be followed while auditing the significant accounts from the company’s general ledger.

From the perspective of business systems, the financial statements audit is carried out on 2 types of controls i.e. Business System Controls and General Computer Controls. The systems that have a direct impact on the significant/material accounts of the company’s general ledger and have a direct impact on the financial numbers being reported, are considered for the systems audit. Let’s take a closer look at the nature of auditing of system controls:

Business System Controls: These are automated controls which have been implemented in a business system to support a business process. These controls are responsible for preventing and/or detecting process non-compliance. Since these controls are built into the system’s configuration, all transactions processed through a particular system are impacted by these controls. Such controls are generally audited by an inspection of the system configuration in conjunction with the configuration change logs. If these controls are implemented through non-standard methods like hard-coding, then auditing approach is adequately modified to establish whether the control had been operating in the expected way or not.

In cases where multiple systems feed financial information to the general ledger, the interfaces are audited to ensure the integrity of the data flowing through the application interfaces. These interfaces may carrying out real-time transaction processing or
batch processing. Audit approach is shaped according to the nature of the interface and input/output files.

**General Computer Controls:** General computer controls are implemented on the computer systems underlying business applications. These systems may be largely viewed as servers, databases and infrastructure support applications. Controls implemented on these systems are largely classified into the following 4 domains; each of these domains generally include a set of preventive, detective and corrective controls.

a) Access to Program & Data: Controls in this domain are designed around the management of user access to the business applications, servers, databases and other IT components. Privileges given to users, segregation of duties, super user access, timely disabling of accounts and periodic reconciliations are some of the key aspects covered by controls in this domain.

b) Change Management: This domain deals with changes related to changes being implemented in the configuration and code of business applications being used to run business processes. Authorisation of changes, testing, user communication and segregation of duties are some of the key aspects covered by controls in this area.

c) Program Development: This area deals with the development or acquisition of new business applications and induction into the existing business environment. Data migration and integrity, user communication, authorisation and UAT are some of the key aspects covered by controls in this domain.

d) Computer Operations: These are lower risk controls which provide a view on the pervasive controls on the overall management of IT components operating in the company. Backups, timely execution of batch processing (this is crucial if there are batch related application interfaces), incident management and network related controls are key areas of focus in this domain.

In the event of failure of key controls in any of the above domains, the audit is required to exercise judgment whether the failure impacts the implementation and operation of any of the business system controls. If it does, the audit of the related business process if performed using substances techniques which ensures increased effort for the auditor and auditee and hence increased overall audit costs.

5.2. **More efficient auditing**

Business systems can be configured to write transactions on to the Distributed Ledger post validation through the pre-defined consensus mechanism, depending on the parties and risk involved in the transaction, audit procedures may be designed to account for the immutable nature of such transactions recorded on the Distributed Ledger.

For auditing a transaction, the auditors select a sample data and perform audit on it. Moreover, audit is generally performed on the past data. With the advent of DLT, the data is validated by an independent network before being recorded on the Ledger. This additional validation point improves the data integrity and also provides an opportunity for real-time audits.

In the new dynamics, Auditor can become one of the nodes of the Distributed Ledger and can verify the transaction at the time of execution. Also, as the data is on a digital platform it is possible to verify all the transactions on the network with a piece of code. In other words, the conventional sample based audit which happens much later can be replaced with population based and just in time auditing. Also, this will simplify Auditor’s job as there will be increased transparency and less redundancy because of single version of a transaction for all stakeholders. In turn, a big portion of manual audit processes will be reduced to improve the overall efficiency of the audit.

Another big advantage is Distributed Ledger can have an built-in native audit trail. In it’s database system, the deletion of one node in a database will lead to synchronization of data from other data nodes. The data will be corrected and integrity of the data is restored. The data redundancy in Distributed Ledger database is very useful in restoring data. In addition, the audit trail will provide an end-to-end transaction details with recipient information. This blockchain ledger can also be interfaced with other external systems to perform various operations.

**Current scenario: Post facto auditing**

**Proposed scenario: Real time(continuous) auditing**

![Diagram showing proposed changes after DLT implementation](image)

5.3. **Challenges associated with DLT Audit**

However, it should be noted that the audit procedures will require a review of the code of the Distributed Ledger and will give rise to the need for the CPAs to upgrade their knowledge of the DLTs. Additionally, this will also give rise to situations where platforms may be used, which do not have wide acceptance and support available (and hence not known to CPAs)[18].

From the requirements of the Internal Control – Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission, to the requirements of the Securities and Exchange Act of 1934 and Sarbanes- Oxley, it is incumbent...
upon management to establish and maintain adequate internal controls over financial reporting. This system of internal controls includes management documenting a thorough understanding of the systems, processes, and general computer controls (GCCs) that management is relying on for purposes of their financial statement preparation, regardless of the type of underlying technology. When Distributed Ledger technology is adopted as part of the financial reporting process, management and the auditor will need to understand the setup and design of the Distributed Ledger itself. It is natural to expect that a significant amount of audit evidence may only be available in electronic format with Distributed Ledger Technology. As the evidence is available in digital format, auditors may find it impractical to obtain sufficient appropriate audit evidence from only substantive procedures. This, in turn, would result in external auditors testing operating effectiveness of relevant internal controls related to the Distributed Ledger to address the accuracy and completeness of information used in the financial statements.

Despite these complexities, Distributed Ledger technology offers an opportunity to streamline information flows between an entity and its external auditor. Today, information is typically exchanged through an iterative process. In a Distributed Ledger world, in addition to the GITCs described above, the external auditor could have real-time data access via a read-only node on the Distributed Ledger to obtain information required for the audit. This could benefit and enable the audit of the future profoundly.

Further, with the deployment of Distributed Ledger, data structuring and digitization, management and auditors could deploy automated tools with analytics and cognitive capabilities, which could process the supporting documentation in near-real-time and send alerts to authorized members of the management and audit team. This could further improve the pace of the financial reporting and audit processes by giving auditors access to evidence required to test selected transactions. It could also reduce the potential for source documentation to be altered or changed.

It is evident that permissioned (private) Distributed Ledgers and networks will flourish in enterprise applications and will handle certain types of transactions. In this more likely scenario, capital markets, regulated or unregulated, will still require an entity to keep a set of financial statements that compiles information from Distributed Ledger networks and other unconnected ledgers (e.g. entity specific subledgers and enterprise resource planning systems) and to be presented in accordance with a set of generally accepted accounting standards.

5.4. Risks Associated with DLT

Just like all other technologies, DLT is currently evolving and readers should exercise judgment in assessing risks to such an emerging technology. In this section, we have examined the technology risk and controls considerations related to DLT.

For the purpose of studying risks associated with DLT applications, we should consider the following components of the applications and then assess risks around each of these components:

- Base operating system of each node
- Hardware of each node
- Configured instance of a suitable blockchain platform (like Hyperledger, Quorum, Ethereum etc.)
- External databases, web servers, FTP servers, used to access nodes

DLT applications may be largely classified in two types; those built on public Blockchain and those built on private Blockchain. The risks and controls associated with such applications vary depending upon factors such as choice of platform, consensus mechanism, transaction logic, authority of nodes etc. Additionally, the platform used to build DLT applications carries certain inherent risks, which need to be accounted for, while conducting risk assessment. Moreover, the front-end applications which are used to parse transactions and triggers for smart contracts, should also be assessed for technical risks.

Readers should understand that while Blockchains do provide transactions security and integrity, they do not necessarily provide security of the keys stored for transactions. The distributed architecture of DLT applications caters to protect any loss of cryptographically sealed data, but if account information (used to seal the data) is stolen, then the value stored on the Blockchain is compromised. Hence security controls should be carefully designed for Blockchain applications and risk assessments carried out periodically due to evolving threat landscape.

The risks associated with DLT applications may be largely classified as follows:

1. Inherent Risks: These are risks which are associated with the platforms used to build the DApp and other peripheral systems, which have a direct impact on transaction processing on the Blockchain.
2. Transaction Risks: These are risks which, if exploited by a threat, may lead to compromise of transaction integrity and unauthorised transactions on the Blockchain.
3. Smart Contract Risks: These are risks associated with the logic coded in the self-executing smart contracts and the oracles which are used to feed triggers to smart contracts.

Few examples of key risks associated with the DLT applications are:

- Risk of integrity of the platform used to build the application.
- Risk of attack on the infrastructure used to host data and nodes.
- Risk of abuse of privileges, in a permission Blockchain.
- Legal & regulatory risks and jurisdiction issues.
- Risk of liability of any losses incurred due to transaction compromise on the Blockchain.
- Risk of increased energy consumption due to inappropriate consensus mechanism.
• Risk of high latency on network due to inappropriate choice of platform.

![Figure 3. Factors for risk assessment](image)

6. CONCLUSION

The parameters suggested to design use cases are industry agnostic and implementation perhaps will need industry specific customizations when proof-of-concepts are presented to the management. That said, the use case shall still fall under one of the categories described in this paper. Distributed Ledger Technology can shapeshift the kind of auditing practices across the auditing landscape. The auditing methodology can move closer to absolute assurance as opposed to reasonable assurance by enabling population based auditing (replacing sample based auditing approach). Moreover, the Auditing process can be continuous if Auditor becomes one node of the Distributed Ledger against the conventional sample based audit which happens much later. In lieu of the efficiency and transparency DLT can bring into the industry, the task of Auditors will be simplified and streamlined as there will be a single view of a transaction for all stakeholders. The DLT technology has the potential to automate auditing processes maintaining the conformity with regulations. The road ahead on technological front looks fairly promising but organisations are moving forward with caution, as switching to a new technology will be a high risk strategy as technologies take time to mature.

REFERENCES

centre/understanding-how-blockchain-works-and-why-it-will-transform-
fx/
-esma50-1121423017-285.pdf
consultations/ASX-Consultation-Paper-CHESS-Replacement-19-
September-2016.pdf
services/articles/investing-in-blockchain-technology-with-SETL.html
[10] Murdoch, 10 S. (December 14, 2017), Top Ten Obstacles along Distributed Ledgers? Path to Adoption, Sarah Meiklejohn, December 14, 2017
blockchain
technology/
releases/Deutsche-Boerse-presents-blockchain-concept-for-risk-free-
cash-transfer/2883236
blockchain-technology-and-security
2016/how-blockchain-will-impact-accountants-and-auditors

ASIA '18 - 35