A Reasonable Assurance Framework for Distributed Ledger Technology Systems: A Risk Assessment Approach

Abstract: With many businesses either adopting Distributed Ledger Technology (DLT) applications or considering their implementation for those enterprise processes which potentially could materially impact financial statements, auditors will soon be asked to reasonably assure DLTs. We propose a generalizable framework which an auditor can follow to provide reasonable assurance of a DLT, and which considers its risks to the enterprise. The framework is developed with a Design Science Research (DSR) approach and entails risk assessment, controls identifications, controls procedures evaluations, and controls weaknesses analysis. It discusses the generic distributed ledger technology space but uses examples specific to blockchains. This paper contributes to the evolving research in the DLT domain and appears to be the first to propose a risk assessment-based reasonable assurance framework for DLT systems. It is anticipated that this research will be of great interest and value to auditors, accountants, regulators, business owners, and academics. An ability to understand and evaluate these complex DLTs and their potential risks will benefit an auditor. Business owners will benefit from obtaining a holistic understanding of the risk and controls dimensions of DLT systems.

Keywords: Blockchain, Digital Currencies, Audit, Risk Assessment, Controls Evaluation

Introduction
Businesses from many domains are developing Distributed Ledger Technology (DLT) applications, in the form of digital currencies (Facebook 2019[^1]), blockchains (XX), and smart contracts (XX). These DLT

[^1]: [https://libra.org/en-US/white-paper/](https://libra.org/en-US/white-paper/)
applications or their implementation may influence those enterprise processes which potentially could materially impact an enterprise and its financial statements, and auditors will soon be required to reasonably assure these DLTs. This assurance entails an assessment of the DLT application that is reasonable and not absolute in authority, given the context of the audit. This reasonable assurance would provide a risk assessment of the DLT application regarding its potential impact on the enterprise and its financials and the controls in place to mitigate such risks.

We propose a generalizable framework which an auditor can follow to provide this reasonable assurance of a DLT, and which considers its risks to the enterprise. The framework utilizes a Design Science Research (DSR) approach and entails risk assessment, controls identifications, controls procedures evaluations, and controls weaknesses analysis (NIST 2012). It discusses the generic distributed ledger technology space but uses examples specific to blockchains.

This paper contributes to the evolving research in the DLT domain and appears to be the first to propose a risk assessment-based reasonable assurance framework for DLT systems. It is anticipated that this research will be of great interest and value to auditors, accountants, regulators, business owners, and academics. An ability to understand and evaluate these complex DLTs and their potential risks will benefit an auditor. Business owners will benefit from a wholistic understanding of the risk and controls dimensions of DLT systems.

The research methodology used in this paper is design science research (DSR). The paper follows the DSR approach introduced by Hevner et al. (2004) and Peffers et al. (2007). Other AIS research using the DSR approach include Geerts (2011), Nehmer and Srivastava (2016) and Appelbaum and Nehmer (2017). This paper uses Geerts (2011) application of DSR which categorizes the methodology into six major processes. The six phases are:

1. Problem identification and motivation
2. Define the objectives of a solution
3. Design and development of an artifact which meets (some of) the solution objectives
4. Demonstration of the solution
5. Evaluation of the solution
6. Communication of the problem and the solution (usually an article)

This paper is presented as follows, based on a DSR approach: First, the DLT approach or problem is identified and motivation for this research is explained. Then we discuss the objectives of a solution, based on the typical audit process and the National Institute of Standards and Technology (NIST) guidelines for the examination of information systems (NIST 2012). Thirdly, we then disclose the design and development of the artifact, which entails the following steps: obtain an understanding of the DLT application, conduct an assessment of the risks associated with the use of this DLT, identify the threats to the organization’s assets and their vulnerabilities, the likelihood of occurrence and subsequent impact to the firm, identification of mitigating controls, and the overall framework for this process. In the fourth section, we discuss potential demonstration use cases for this framework. Fifth, we evaluate the framework, followed by a discussion of any issues evolving from the use of this artifact. Finally, we conclude.
1 - Problem Identification and Motivation

DLT Components

Our analysis of DLT is based on Nakamoto’s original paper on Bitcoin (Nakamoto 2008) as interpreted by Appelbaum and Nehmer (2019). We study these papers to arrive at an understanding of the core components of distributed ledger technologies (DLTs) in a generic sense. We derived our components from those papers but generalized to DLT systems as a whole using a variety of validation processes and not only that proposed by Nakamoto. We then consider the derived components as our basis in modeling the risks and threats which should be identified when auditing DLTs. The components which make up the DLT process are as follows:

1. There is no trusted third party required, instead the network is peer-to-peer or proprietary.
2. New transactions are timestamped and hashed in some way.
3. The hash algorithm is designed to provide some form of transaction validity.
4. The record, the hashed chain of transactions, cannot be changed without redoing the validation process.

First, as a design requirement for whatever system is using the DLT, avoidance of using a third-party countersigner or oracle must be preferable from a design point of view. Use of a third party in the design must impose a cost or add risk to the system under design. The rest of the process is largely required to provide a level of trust between the peers on the network that substitutes for the lack of a third-party trust guarantor. This is done in two principle ways: timestamping individual transactions and hashing the transaction sequence or block using an algorithm with special properties. The transaction types which lend themselves to this type of processing must have certain properties. Usually they are either an asset or record of an asset or they are a type of economic contract. The transaction sequence then either shows the record of ownership of the asset or the record of contractual obligations fulfilled to date in the execution of the contract, such as the number and timing of mortgage payments already made on a mortgage contract. So, the timestamp provides a recorded ‘history’ of the asset or contract. In the case of a proprietary network, the proprietor, usually the firm which has created the DLT application, must incur the risks associated with not using a third party or a per-to-peer network. Usually, this risk can be born because the application in for internal use and the existing IT controls provide sufficient risk reduction.

We now consider the validation process. This process varies greatly over the implementations and proposed implementations of DLT applications. We leave an in-depth analysis of the major forms that DLT validation processes are taking as the technology evolves to a future work. Here we propose three components that any process must have:

1. It must create or help to create a record of the sequence of transactions (timestamp) thereby aiding the validating of transaction provenance.
2. It must have some feature or features which decreases the risk of the transaction sequence
being tampered with.

3. It must include some process to verify individual transaction read from the DLT.

2 - Define the Objectives of a Solution

Audit Requirement

“With all these exciting innovations, it is important to remind ourselves that the advent of emerging technologies does not change the fundamental financial reporting framework. If an emerging technology is being used to meet financial reporting of internal control requirements established by the federal securities laws, then auditors need to understand the design and implementation of that technology.” – PCAOB Board Member, Kathleen Hamm

If DLT applications are being used as part of the process of preparing financial statement or internal control reporting requirements, the auditor will need to not only understand the design and implementation of the DLT, but also assess the audit and business risk that this DLT may pose to the entity. The auditor cannot assign a level of risk to the DLT without this understanding. The risk assessment process is as follows (Louwers et al 2018):

\[ AR = IR \times CR \times DR, \]

Where AR is audit risk should be set by the auditor to a low level. IR or Inherent Risk is the probability that, absent internal controls, material errors could enter the reporting process. CR or Control Risk is the probability that the controls established by the entity will not prevent material errors. DR or Detection Risk is the probability that the auditor’s own tests will fail to detect any material errors.

NIST Guidelines

In order to build a reliable framework based on established principles, we reference the concepts and terminology adapted from the NIST’s Special Publication 800-30 (NIST 2012) for an evaluation of inherent risk. According to NIST (2012), an inherent risk assessment should identify:

- threats to organizations (i.e., operations, assets, or individuals);
- vulnerabilities internal and external to organizations;
- the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and
- the likelihood that harm will occur.

---

2 Remarks made during a key presentation at the 43rd World Continuous Auditing & Reporting Symposium, November 2018, Newark, NJ., USA.
This research incorporates each of the above elements and an analysis of those elements, along with example internal control activities and procedures for addressing their associated inherent risks.

We designate a low, moderate, or high level of likelihood to each inherent risk of a process. The likelihood of inherent risk is dependent on the characteristics of the asset in question. However, it may vary from organization to organization based on complexity and purpose, and on the extent of reliance that the organization places on the relevant asset.

**Inherent Risks:** Inherent risks are those that are present, prior to implementation of controls, in relation to the use of DLT across any relevant organization processes.

**Threats and Vulnerabilities:** Threats and vulnerabilities are how any inherent risk may present itself. Examples of specific threats and vulnerabilities have been linked directly to the assets being evaluated within the process.

**Likelihood and Impact:** Likelihood and impact are expressed as a highly generalized estimate, related to specific threats or vulnerabilities. Overall, this is a difficult component to estimate given considerations for human behavior and does not represent all possible company or individual circumstances. This is the largest judgement-based component of this framework.

**Internal Control Activities and Procedures:** These are suggested specific activities, procedures, and protections that potentially mitigate the outlined threats and vulnerabilities tied to DLT inherent risks.

If we look at a revised version of the components of a DLT, then we have the following set of four:

1. There is no trusted third party required, instead the network is peer-to-peer or proprietary.
2. It must include a validation process which creates or helps to create a record of the sequence of transactions (timestamp) thereby aiding the validating of transaction provenance.
3. The validation process must have some feature or features which decreases the risk of the transaction sequence being tampered with.
4. The validation process must include some process to verify individual transaction read from the DLT.

We now take each of these components and analyze them with respect to their inherent risks and threats and vulnerabilities. We will return to risk and likelihood and impact as well as the internal controls in more detail in the next section. The auditor will have to consider the design of the DLT regarding the elimination of a trusted third party. First, there is the question of whether a trusted third party was needed in the first place. If not, then the design may have some redundant security features but it should not be too risky. If a third party or some advanced security is required. The auditor will need to assess how well the design of the DLT and its implementation addresses the security concerns required in this case. The major threats are that there is a motivation by actors to tamper with the recording of the transactions. The vulnerabilities are through the design and implementation of the specific DLT. The risk to the sequencing or timestamping are in the design of the algorithm or process which ensures that the transactions are sequenced in a way which matches the requirements of the
system it is implementing. For example, if the business process requires a time sequence of transactions, then the design must provide for that, possibly through timestamping. The main threat here is lack of competence either on the part of the DLT’s designers or on the part of the audit team. If the sequencing process is standardized or provided through a software provider in a standard package, then the audit firm can familiarize itself with that process and in effect certify it (or not) for future audits. The vulnerabilities are lack of appropriate skill sets at the client or in the audit firm.

The risk of the risk of tampering is very direct. The threat is that the ledger is compromised in some way which the auditor will not be able to anticipate and test for. The vulnerabilities will lie largely in access to the DLT architecture as a whole and the soundness of the validity process as designed and implemented. Standardized solutions will be less expensive to audit from the client’s perspective since auditors can spread their knowledge of the particular validity process across many clients. The risk to the final component, verifying individual transactions, is that the transactions read off the DLT are incorrect. The major threats are tampering and inadequate design of the validation process. The vulnerability here is that the auditor may not perform adequate testing of the DLT on a system level. That is, individual components 2 and 3 may be working but the result is still incorrect. The solution to the auditor’s dilemma in obtaining audit evidence from a DLT is to adequately address each of these risks.

3 - Design and Development of an Artifact Which Should Meet Solution Objectives

Figure 1: DLT Audit Methodology (adopted from Louwers et al 2018)

What follows is a detailed explanation of the six steps of the DLT Audit Methodology in Figure 1:

1. Identify DLT Application

Purpose Identification
In this stage, the auditor should obtain a clear understanding of the organization’s purpose for adopting the DLT. Is the DLT the most efficient and effective option for the purpose at hand?
DLT Identification
The auditor should understand the specific DLT application and that the DLT represents the most effective and efficient solution possible to the organization. The auditor must determine the boundaries of the DLT application within the scope of the audit.

2. DLT Risk Assessment
Inherent Risks: These were discussed in the previous section. Risks that occur due to the nature of this process and cannot be removed without drastically changing the process. Inherent risks are those that are present, prior to implementation of controls, in relation to the use of DLT across all applications. An example of several such risks (Table 1) would include hacking, reliance on third party platforms, complexity, fraud, and error. Some of the following additional risks to be evaluated could also be inherent:

Complexity Risk:
Complexity risk is the threat that stems from the complexity of the data and the DLT application. If either component is too complex for both the IT staff and for the auditor to understand, the possibility for unanticipated DLT results increases. Much of this risk is driven by the validation process used in the DLT application. To assess Complexity Risk, the auditor might ask:

- Is the goal of the DLT so complex that it cannot be evaluated for any elements associated with error, integrity, or security?
- Is the incoming data so complex that it cannot be evaluated for direct or indirect attributes that historically have been associated with error?
- Is the DLT design and processes so complex that it cannot be examined for any elements associated with error?
- Is the DLT result so complex that any direct or indirect associations with error cannot be explained?

Information Risk:
Information risk is the risk that arises from the use, development, operation, involvement, influence, and adoption of information systems and its accuracy and completeness implications within a business. This risk largely arises from the fourth component of the DLT as outlined in Section 2 above. The essence of information risk from an auditing perspective is that the data being transferred, processed, digested, analyzed, and reported might not represent the substance of the underlying physical events and that it would not be neutral, free of bias and error. The International Accounting Standards Board’s Conceptual Framework for Financial reporting (IFRS) (2018) states that “to be useful, financial information must not only represent relevant phenomena, but it must also represent the substance of the phenomena that it purports to represent.” Substance, in this instance, refers to the underlying circumstances, applications, and context of the event or phenomena that the financial information reflects. Furthermore, both ‘relevance’ and ‘faithful representation’ are mentioned as fundamental qualitative attributes for the financial information that are relevant to the financial statements and their users (IFRS 2018, p 6). That is, such information is relevant because it is “capable of making a difference in the decisions made by users” due to either its confirmatory or predictive aspects. It is faithfully representational because it is “complete, neutral, and free from error” (IFRS 2018, p 6). Therefore, the IASB’s Conceptual Framework
provides the context for examining DLT from an accounting and auditing perspective.

Additionally, COBIT 2019 states that “Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processes in accordance with defined objectives” (ISACA 2019). DLT applications should be transparent, reliable, and traceable regarding any representation of physical assets. An auditor checklist for Information Risk in DLT might look as follows:

- Does the goal of the DLT contain any elements associated with physical asset attributes?
- Does the incoming data contain direct or indirect attributes that historically have been associated with error or fraud?
- Does the DLT design and processes include any elements associated with error or misrepresentation?
- Does the DLT result include any direct or indirect associations with error?

Financial Risk:

Financial risk is associated with financing applications and may include company loans and other obligations that could be subject to default. The assumption is that if the company experiences a loss in revenue, it may default on these debt instruments or shareholders/bondholders may experience an investment loss. This risk stems from the unknown potential for financial loss and the uncertainty of its depth (Horcher 2005). Loss of revenue streams resulting indirectly from problems stemming from DLT may pose a financial risk to the entity. An evaluation for DLT Financial Risk might look as follows:

- Does the goal of the DLT contain any elements associated with error or fraud that may impact the business’s finances?
- Does the incoming data contain direct or indirect attributes that historically have been associated with error or fraud and which might negatively impact the business’s finances?
- Does the DLT design and processes include any elements associated with error or fraud and which could potentially negatively impact the firm’s finances?
- Does the DLT result include any direct or indirect associations with error or fraud, and which might negatively impact the firm’s finances?

Decision Risk:

Decision risk is the potential that a management or operational decision is not in alignment with firm strategies and mission. Decisions made during the entire DLT development process could point to decision risk if they are not in alignment with firm strategies and objectives. This risk is largely driven by the degree of agility present in the choice of a validation process for the DLT. Is that choice sensitive to changes in business conditions? In most cases the answer is likely to be “no.” Questions regarding DLT Decision Risk may present accordingly:

- Does the decision to use DLT contain any elements subject to error or fraud?
- Is the decision to use particular incoming data associated with any direct or indirect attributes that historically have been attributed to error or fraud?
- Does the DLT design and processes include any decisions associated with error or fraud?
- Does the decision to accept a DLT result include any direct or indirect associations with error or fraud?

**Execution Risk:**
Execution risk is the possibility that the firm’s processes and actions are not aligned with its decisions. If the DLT were to execute the process with unexplainable results that conflict with firm decisions, this deviation would pose an execution risk. This risk is largely associated with the fourth component of the DLT. Execution risk evaluation questions should cover:
  - Does the execution of DLT contain any elements associated with error or fraud?
  - Is the execution of the DLT in alignment with defined firm objectives and strategies?

**Regulatory Risk:**
PwC defines regulatory risk as “the risk of having the 'license to operate' withdrawn by a regulator, or having conditions applied (retrospectively or prospectively) that adversely impact the economic value of an enterprise.”³ Complications due to unexpected DLT issues may result in investigation and censure from regulators and authorities. With DLT, regulatory risks may be higher as guidelines, frameworks, and regulations are immature. For example, the SEC has just recently published a guidance, but this is not authoritative regulation⁴. The Commodities Futures Trading Commission (CFTC) has determined that digital currencies such as bitcoin are commodities⁵. To evaluate regulatory risk of DLT, the auditor should ask:
  - Does the goal of the DLT contain any elements associated with error or fraud that may negatively impact the business’s compliance with regulations?
  - Does the incoming data contain direct or indirect attributes that historically have been associated with error or fraud and which might negatively impact the business’s compliance with regulations?
  - Does the DLT design and processes include any elements associated with error or fraud and which could potentially negatively impact the firm’s compliance with regulations?
  - Does the DLT result include any direct or indirect associations with error or fraud, and which might negatively impact the firm’s compliance with regulations?

**Legal Risk:**
Legal risk is the threat of financial or reputational loss that can result from lack of awareness or misunderstanding of, ambiguity in, or reckless indifference to, the way law and regulation apply to your business, its relationships, processes, products and services.⁶ Legal risk is similar to regulatory risk, but

---
³ https://www.pwc.com/la/en/risk-assurance/regulatory-risk-management.html
⁴ https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets
⁵ https://www.cftc.gov/sites/default/files/idos/idos/public/@itenforcementactions/documents/legalpleading/enforcementorder030618.pdf
⁶ https://www.ey.com/Publication/vwLUAssets/ey-legal-risk-2-show-you-are-in-control/%24FILE/ey-legal-risk-2-show-you-are-in-control.pdf
broader in scope, in that any parties with perceived grievances regarding a DLT application may also sue for damages and loss due to injustice or fraud. An auditor might want to ask the following questions about the legal risks of DLT:

- Does the goal of the DLT contain any elements associated with error or fraud that may subject it to lawsuits?
- Does the incoming data contain direct or indirect attributes that historically have been associated with error or fraud and which might subject it to lawsuits?
- Does the DLT design and processes include any elements associated with error or fraud and which could potentially lead to lawsuits?
- Does the DLT result include any direct or indirect associations with error or fraud, and which might potentially lead to lawsuits?

Threats and Vulnerabilities

Threats:

Threats are how these DLT risks present themselves to assets of the organization, either directly or indirectly. Examples of specific threats and vulnerabilities have been linked directly to the assets being evaluated within the process:

- Complexity of DLT
- Transparency of DLT
- IT Security Practices of DLT Applications
- Collusion (Over 50%)
- Oracle Paradox of DLT
- Privacy Concerns
- Hacks/Malware
- Lack of Authorization
- 3rd Party Platform Reliance

Assets:

Assets in this framework are the exposed components of the system or process. These assets entail:

- Data/Physical Transactions
- DLT Design & Components (coins, wallets, tokens)
- DLT Results
- People

Vulnerabilities:

Vulnerabilities attempt to identify how susceptible the organization is to these threats that present themselves to the organization’s operations, assets, and people.

Likelihood and Impact

This component addresses how likely these threats are to occur, and this assessment is context, domain, and entity specific. Here we attempt to grasp to what extent these threats could impact the financial statements at a material level.
3. Identify Mitigating Internal Controls

In this stage we attempt to identify the controls designed to mitigate these risks and threats and if these are operational and/or enforced. The Evaluation Framework is helpful at the stage to map the asset type to its inherent DLT risks, threats and vulnerabilities, likelihood and impact, and mitigating internal controls (Table 1). The number label of each inherent risk is carried to its corresponding threats, likelihood, and internal controls. The Inherent DLT Risks are evaluated and assigned a value ranging from 0 for low risk to 1 for high risk. The DLT Internal Controls are individually examined to assess a value for Controls Risk, ranging from 0 as a high risk value and 1 as a low risk value. So to illustrate, with the asset/process of People, the first IR listed is 1 – Poor DLT Familiarity. Then the auditor would calculate the values for Threats/Vulnerabilities and Likelihood/Impact, and average these to arrive at the IR Risk Score. The auditor would then evaluate the corresponding control, 1 – IT Staff Expertise, for various conditions, and applying an average score for those conditions to arrive at a CR assessment for that control only.

The Evaluation of Inherent DLT Risks Framework

| Asset Or Process                      | Inherent DLT Risks:                                                                 | DLT Threats and Vulnerabilities                                                                 | Likelihood and Impact                                                                 | IR Risk score (0 is low risk to 1, high risk) | DLT Internal Controls (Phase 4) | CR Risk score (0 is high risk to 1 is low risk) |
|--------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------|----------------------------------|--------------------------------------|
| Financial/Physical Transactions      | 1-unexplainable 2-not understandable 3-Error 4-Fraud 5-Data Prep issues 6-Privacy Concerns (GDPR) 7-external data 8-hacking 9-Access Controls | 1,2-complex, messy data and transactions 3-errors in data not identified 4-fraud in data not identified 5-inadequate data pre-processing 6-data violates GDPR mandates 7-lack of data provenance 8-data was hacked before access 8-upload data streams hacked 9-Access controls not enforced | 1,2 -moderate to high likelihood & high impact 3-moderate likelihood & high impact 4-moderate likelihood & high impact 5-low to moderate likelihood & high impact 6-moderate to high likelihood & high impact 7-high likelihood & moderate impact 8-moderate likelihood & moderate impact 9-moderate likelihood & moderate to high impact | (these are the points of examination in Phase 4) 1-data has been examined with descriptive statistics and scrubbed/wrangled 2-descriptive statistics and exploratory analytics 3-data has been corrected/cleaned 3-anomaly detection 4-data has been examined with descriptive statistics 5-data is flagged for data prep issues 6-data is examined for GDPR issues and modified if |
| DLT Design & Components | 1-not explainable 2-not understandable 3-design encourages fraud 4-error in design 5-not correctable 6-rely on 3rd party algorithms 7-hacking 8-access controls | 1,2-too complex to explain 1,2-design execution is opaque 3-design enforces error or fraud 3-design creates error or fraud 4-design magnifies errors 4-design creates errors 5-design is uncorrectable 5-do not know where corrections should be made 6) lack of design provenance 7) lack of security 8) lack of access controls enforcement | These ratings are DLT application specific | (These are the points of examination in Phase 4) 1,2,3,4,5-IT staff receives updated training with emphasis on error correction/fraud detection 1,2,3,4,5-continual efforts are made to convert the DLT to explainable DLT 1,2,3,4,5-reperform the DLT process 6,7-audit the open source/3rd party platforms (SOC2 type report) 7-business-wide internet security training 8-access permissions embedded in |
| DLT Results | 1-not explainable 2-not understandable 3-errors 4-fraud 5-not correctable 6-hacking 7-access issues | 1,2-results are unexpected 1,2-unjustified results 3-results hide errors 4-results enforce fraud 5-results are not easily corrected 6-results data sets not stored securely 7-lack of access controls enforcement | These ratings are DLT application specific | (These are the points of examination in Phase 4) 1,2,3,4,5-results evaluated for issues of accuracy, error, and fraud 6-input and output control totals captured and measured 7-access permissions enforced for all circumstances |
| --- | --- | --- | --- | --- |
| Persons (executive, management, designers, auditor) | 1-poor DLT familiarity 2-lack of firm strategy 3-poorly defined firm policies 4-lack of oversight 5-3rd party algorithms 6-IT development practices 7-access management issues 8-shared roles and responsibilities | 1-poor understanding of DLT 2-poor understanding of firm strategy 1,2,3-not sure if DLT aligns with firm strategy/ethics 3-unfamiliarity with firm policies 4-lack of governance and oversight over DLT development 5-over reliance on 3rd party developed DLT algorithms 6-no established guidelines for IT development and integration 7-access controls not established nor enforced 8-scarce staff | 1-Moderate to high likelihood & moderate to high impact 2-low to moderate likelihood & high impact 3-moderate to high likelihood & high impact 4-moderate likelihood & high impact 5-moderate to high likelihood & high impact 6-low to moderate likelihood & high impact 7-moderate likelihood & high impact 8-low to moderate likelihood & high impact | (These are the points of examination in Phase 4) 1-IT staff expertise 2-frequent review of firm strategy from a fraud prevention perspective 3-frequent review of firm policies and procedures 4-review of regulatory examinations in DLT relevant and sensitive topics 5-review of 3rd party DLT apps for error and fraud 6-Developed and adhered to DLT procedure |
7-access controls have been defined and are consistently enforced. Clearly defined rules and responsibilities that are consistently enforced.

Table 1: DLT Inherent Risk Assessment, Threats, and Internal Controls Evaluation Guideline (where the inherent risks are numbered and these numbers relate to the corresponding Threats, Likelihoods, and Controls).

4. Test Controls

This step involves observation and analysis. There would be questionnaires to be completed based on the auditors’ observations, discussions, and analysis. A sample of questions concerning controls around persons expertise would be as follows:

Persons Control Issue #1: Poor DLT familiarity / IT Staff Expertise

1. Has the IT staff received training in blockchain and smart contracts?
2. Where did this training occur?
3. How did this training occur?
4. Is there a formal measure of competency?
5. When did this training occur?
6. Is this training documented?
7. Has the IT staff received training in blockchain and smart contract coding?
8. Where did this training occur?
9. How did this training occur?
10. Is there a formal measure of competency?
11. When did this training occur?
12. Is this training documented?
13. Has the IT staff received training updates in these areas?
14. Where did this training occur?
15. How did this training occur?
16. Is there a formal measure of competency?
17. Who does the IT staff consult with regarding issues beyond his/her expertise?
18. Has the IT staff hired outside consultants for assistance in resolving issues?
19. How were these experts vetted?
20. Are any individuals that access the blockchain code lacking in training (what are the access controls)?
5. Detailed Examination
The auditor would select a sample of DLT transactions either based on Exceptional Exceptions (Issa et al 2018) or another more traditional sampling approach. The Exceptional Exceptions approach requires that all DLT transactions be analyzed, where exceptional exceptions (items that meet certain criteria) are targeted for detailed examination (Issa et al 2018).

6. Reasonably Assure the DLT Application
The auditor provides an evaluation at a reasonable level of assurance of the DLT application. This would be an evaluation score based on the assessment of Inherent Risks, Control Risks, and Detection Risks. Going back to the risk assessment model in Section 2, where the Audit Risk (AR) level is determined by the auditor in advance, we can provide a risk score for both the inherent and control risks. The Detection Risk (DR) is calculated based on those numbers. So, looking at the following model AR = IR x CR x DR, where AR is set to .05, the evaluation score of Inherent Risk (IR) should be higher if material misstatement is likely to occur from the use of DLT, and the score for Control Risk (CR) should be lower if material misstatement is likely to occur from the use of DLT. As a guideline, it can be said that:

Inherent Risk: 0 to 1, where 0 equals low risk from DLT and 1 equals a high risk, with variations between
Control Risk: 1 to 0, where 1 equals low risk that the controls would not mitigate the IR of DLT and 0 equals a high risk that the controls would not mitigate the IR of DLT.

4 - Demonstration of the solution

We hypothetically demonstrate this assurance process for the asset of People and the controls regarding Staff Expertise. Here is a high-level view of the Persons for the Inherent Risk of Poor DLT Familiarity (Table 1, Persons, #1):

**Asset or Process: Persons**

Inherent DLT Risk (IR): Lack of DLT Expertise
Threat/Vulnerability: Poor Understanding of DLT
Likelihood and Impact: Moderate to high likelihood & moderate to high impact

Internal Controls DLT Risk (CR): IT Staff Expertise

The auditor will evaluate the IR based on the Threat/Vulnerability and Likelihood/Impact scores, which should be closer to 1 if there is a high likelihood if a material misstatement can occur due to the use of DLT, and closer to 0 if there is a lesser likelihood that a material misstatement can occur. The auditor could use the questionnaire presented earlier to evaluate the CR score, where the lower number indicates a likelihood that the controls will not detect a material misstatement due to the use of DLT and the higher number indicates the opposite condition. For Control Risk, after labeling each CR question with a decimal between 0 and 1, the auditor will compute the average score. For Inherent Risk, the auditor will score Threat, Vulnerability, Likelihood, and Impact with a score between 0 and 1 and compute the average.
As an illustration, imagine a firm that is utilizing DLT to process commercial real estate transactions. Sales staff, marketing staff, IT staff, and legal staff are all involved with this process. The auditor is mandated to evaluate the DLT technology as the amounts concerned are material to the entity’s financial statements. AR is established to be 0.05. The following numbers are derived during the examination:

Asset or Process: People

Inherent Risk: Lack of DLT Expertise

Threat: .5
Vulnerability: .4
Likelihood: .7
Impact: .8
Average IR score: 0.6

Control Risk: IT Staff Expertise (where 1 is highly unlikely that a material misstatement will occur)

1. Has the IT staff received training in blockchain and smart contracts? .9
2. Where did this training occur? .9
3. How did this training occur? .9
4. Is there a formal measure of competency? .5
5. When did this training occur? .3
6. Is this training documented? .9
7. Has the IT staff received training in blockchain and smart contract coding? .4
8. Where did this training occur? .4
9. How did this training occur? .8
10. Is there a formal measure of competency? .9
11. When did this training occur? .3
12. Is this training documented? 1.0
13. Has the IT staff received training updates in these areas? .4
14. Where did this training occur? .4
15. How did this training occur? .4
16. Is there a formal measure of competency? .9
17. Who does the IT staff consult with regarding issues beyond his/her expertise? .8
18. Has the IT staff hired outside consultants for assistance in resolving issues? .8
19. How were these experts vetted? .5
20. Are any individuals that access the blockchain code lacking in training (what are the access controls)? .1

AVERAGE CR SCORE: 0.63

Risk score for this DLT application regarding Persons and their training:

AR = IR x CR x DR
0.05 = 0.6 x 0.63 x 0.132

Where [DR = AR / (IR x CR).]
For the DR score, a higher number closer to 1.0 indicates that we can afford less effective testing, whereas a number closer to zero indicates that more effective testing is required. In this instance where DR is 0.132, more effective and substantial testing is required for the risk of Lack of DLT Familiarity. This illustration covers only one component of Persons. This same process must be undertaken with all other Persons Inherent Risks, and the average score for each IR may be averaged or handled separately. The same process should be undertaken for each Asset/Process, to derive different levels of risk assessment. For new applications of DLT and/or applications that are highly complex and material, a fine-grained level of risk assessment would be expected.

5 - Evaluation of the solution
This framework for conducting a risk assessment of a DLT process is grounded in current prevalent audit methodology. We assume that auditors will soon be required to assess the risk of DLTs to a firm in the current audit environment. It could be said that Bitcoin and Blockchain are at the peak of the Gartner Hype Cycle.

DLT appears to be gaining traction in the financial services industry, and even governments are exhibiting interest in adopting blockchain for land records, identity management systems, health-care record, and elections. Given the ever-growing interest in Blockchain technologies within the business and government domains, it is inevitable that auditors will encounter their use during the engagement. The methodology developed and demonstrated in this paper is evaluated here against the current auditing standards and our interpretation of DLT. While this is a good start, a better evaluation approach would involve field testing with actual audit clients. Our demonstration is hypothetical. One of the biggest factors in that approach will be the risk of the accounts or disclosures which are affected by aggregations from DLT systems. It is possible in many cases that the dollar values will be small relative to other aggregation components in the values being audited. Additionally, this study did not consider “auditing around” DLT systems. There may be opportunities to use that planning approach as well. Auditing around the DLT may be viable for non-public entities, given that the PCAOB requires the auditor to understand complex technologies if they affect the financial statements. It is also uncertain to us whether DLT systems will have the impact on financial reporting systems that some predict, although this study assumes that there may be some components that are. However, many of the risks discussed are pervasive in financial reporting systems and so these aspects can be expected to remain important issues for the auditor for some time to come.

6 - Communication of the Problem and the Solution
Businesses and governments, which are audited by public accounting firms, are beginning to adopt DLT technologies for some components and processes. The audit profession will need to adjust itself to the phenomenon of Blockchain based on its current practice and evolve incrementally. Alles et al (2008) discuss these steps of adjustment – many steps of evolution are intertwined with business needs, management support, process adjustments, efficiency monitoring, and regulatory adjustments. These stages of technology adoption and regulatory changes could take years to
process. The big fear is that the audit profession may adapt too slowly in comparison to the pace of its clients, thereby becoming increasingly irrelevant and ineffective in an audit.

Concluding thoughts
With many businesses either adopting Distributed Ledger Technology (DLT) applications or considering their implementation for those enterprise processes which potentially could materially impact financial statements, auditors will soon be asked to reasonably assure DLTs. We propose a generalizable framework which an auditor can follow to provide reasonable assurance of a DLT, and which considers its risks to the enterprise. The framework is developed with a Design Science Research (DSR) approach and entails risk assessment, controls identifications, controls procedures evaluations, and controls weaknesses analysis. It discusses the generic distributed ledger technology space but uses examples specific to blockchains. This paper contributes to the evolving research in the DLT domain and appears to be the first to propose a risk assessment-based reasonable assurance framework for DLT systems. It is anticipated that this research will be of great interest and value to auditors, accountants, regulators, business owners, and academics. An ability to understand and evaluate these complex DLTs and their potential risks will benefit an auditor. Business owners will benefit from obtaining a wholistic understanding of the risk and controls dimensions of DLT systems.

References

Geerts, G. L. 2011. A Design Science Research Methodology and its Application to Accounting Information Systems Research. *International Journal of Accounting Information Systems*, 12(2), 142 – 151.

Hevner, A., March, S. T., Park, J. and Ram, S. 2004. Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75 – 105.

Horcher, Karen A. (2005). *Essentials of financial risk management*. John Wiley and Sons. pp. 1–3. ISBN 978-0-471-70616-8.

IFRS, 2018. https://www.ifrs.org/-/media/project/conceptual-framework/fact-sheet-project-summary-and-feedback-statement/conceptual-framework-project-summary.pdf

ISACA, 2019. http://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx

Issa, H., 2013. *Exceptional exceptions* (Doctoral dissertation, Rutgers University-Graduate School-Newark).

Louwers, T., Blay, A., Sinason, D., Strawser, J., and Thibodeau, J. (2018). *Auditing & Assurance Services*, 7e. McGraw-Hill Education, New York, NY.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.
National Institute of Standards (NIST), 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45 – 77.

Public Company Accounting Oversight Board (PCAOB), 2016a. “AU Section 150: Generally Accepted Auditing Practices” https://pcaobus.org/Standards/Auditing/Pages/AU150.aspx

Public Company Accounting Oversight Board (PCAOB), 2016b. “Auditing Standard No. 5: An Audit of Internal Control that is Integrated with an Audit of Financial Statements, Appendix C – Special reporting Situations.” https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5_Appendix_C.aspx

Sarbanes, P. (2002, July). Sarbanes-Oxley Act of 2002. In *The Public Company Accounting Reform and Investor Protection Act.* Washington DC: US Congress.