`

APPROVAL OF HONORS PROGRAM SENIOR PROJECT

Candidate

Han Jumashov

Project Title

Internal Auditing and De-risking Blockchain-based Environment Under a Global Regulatory Framework

This Senior Project is approved as acceptable

Project Director

Dr. Jackie Lewis

Committee Member

Dr. Gena Messer-Knode

Committee Member

Dr. Bill Yankosky

Honors Program Director

Dr. Bill Yankosky

Honors Program Assistant Director

Dr. Fred Sanborn

April 25, 2023

Internal Auditing and De-risking Blockchain-based Environments Under a Global Regulatory Framework

Han Jumashov

North Carolina Wesleyan University

Advisor: Dr. Jackie Lewis

December 6, 2022

Table of Contents

Abstract

Since its initial launch in 2009, blockchain has been a formidable technology with great potential that can disrupt many industries including but limited to financial, healthcare, media, transportation, and logistics. By mere definition, blockchain is an electronic ledger that stores records of transactions though it has many useful applications (Nitish, 2022). Scholars Furlonger and Uzureau believe that adopting blockchain will soon be a necessity rather than a choice (2019). Nonetheless, the adaptation of such an innovative technology comes at certain risks since 53% of respondents from a survey conducted by Deloitte in 2019 described their concerns over risks associated with blockchain (Matthew et al., 2019). Regardless of their concerns, the same respondents stated that adopting blockchain will be crucial for their businesses to remain competitive. Thus, this research paper will explore major risks associated with the blockchain and support the claim that implementing a global regulatory framework will help to de-risk them. This will be accomplished by gathering and studying peer-reviewed articles, books, and case studies

Introduction

Experts from Deloitte state that adopting any new technology depends on one's ability to manage the risks associated with it (Adam et al., 2021). In the 21st century where humanity lives in the world of technology the ability to adapt and manage new technology can be a key advantage. Although it has been over ten years since the first blockchain transaction was completed (January 3, 2009), the world is yet to (fully) adopt blockchain technology (David and Cristophe, 2019). One of the reasons why blockchain is taking so long to adopt is due to risks related to it, as shown in the surveys conducted by Matthew et al., in 2018 and 2019 (Figure 1). David Furlonger and Cristophe Uzureau describe blockchain as a disruptive technology on page 3 of their "The Real Business of Blockchain".

Furthermore, they state that despite blockchain's innovative nature, blockchain is not a completely new technology but rather a combination of several technologies that collectively disrupted the industry of transaction-based solutions (David and Cristophe, 2019). In their model of blockchain, there are five aspects that make up the technology: encryption, tokenization, immutability, decentralization, and distribution. By a simpler definition, however, blockchain is a ledger technology (usually decentralized) that is distributed peer to peer, making records of electronic transactions transparent and immutable (Nitish, 2022). Coming back to the definition offered by Furlonger and Uzureau, each of the five aspects of blockchain technology offers a variety of solutions making it so valuable. Hence, to better understand the risks introduced by blockchain, it is important to define each one of these aspects.

Fortunately, Furlonger and Uzureau provide a well-put description of each aspect (without regard to a specific type of blockchain i.e public, private, consortium, and hybrid, a.k.a permissioned) on pages 5 and 6 of their "The Real Business of Blockchain". Accordingly,

encryption is a functionality provided by blockchain via the usage of public and private keys that enable the secure recording of blocks. Moreover, as described by Furlonger and Uzureau, tokenization is a feature that can add value to digital items in form of tokens; hence, the process of creating value for digital assets is called tokenization. Indeed, this feature alone facilitated more effective functioning of digital markets (David and Cristophe, 2019). Next, immutability, as the name suggests, a feature that ensures the integrity of a transaction. This is accomplished via, time-stamped, cryptographically signed, and sequential addition of transactions to the ledger (David and Cristophe, 2019). Following, decentralization is an aspect of blockchain that makes it different from most of the network-based solutions (without regard to specific blockchain topology). As opposed to traditional network solutions, there is no central entity with total control over the network. Instead, each participant on the network retains a full copy of the encrypted node and they execute in accordance with the consensus mechanism unless all participants (or the majority) agree to do otherwise, which is known as forking. In essence, this feature of blockchain removes the need for governance by the third-party participant in a transaction (David and Cristophe, 2019). Last but not the least, distribution adds the ability for blockchain nodes to participate remotely without the need to be on the same network (David and Cristophe, 2019). In other words, nodes in different geolocations can still be part of the same network opening doors for global collaboration.

Furthermore, it is worthwhile to define blockchain topologies; specialists from KPMG India categorize blockchain into several categories such as private, permissioned (hybrid), and public, which are differentiated mainly based on their decentralization scope and access level (Mritunjay et al., 2018). To put it into perspective, cloud services could be brought as an example (analogy). One’s personal cloud drive (i.e, OneDrive, Google Drive) could be the

equivalent of a private blockchain. By means of which, one entity has total control over it. In contrast to it, a public blockchain is similar to a cloud instance that is publicly available – for example, most GitHub branches can be easily publicly accessed (forked) for better collaboration. However, the access level can be modified for the blockchain environment just like in a cloud environment. In other words, some parts of the blockchain will be open to the public whereas the private sector will be containing the control. This distribution is mainly used when blockchain is provided on a Platform as a Service basis.

Research Questions

This project will attempt to answer the following questions:

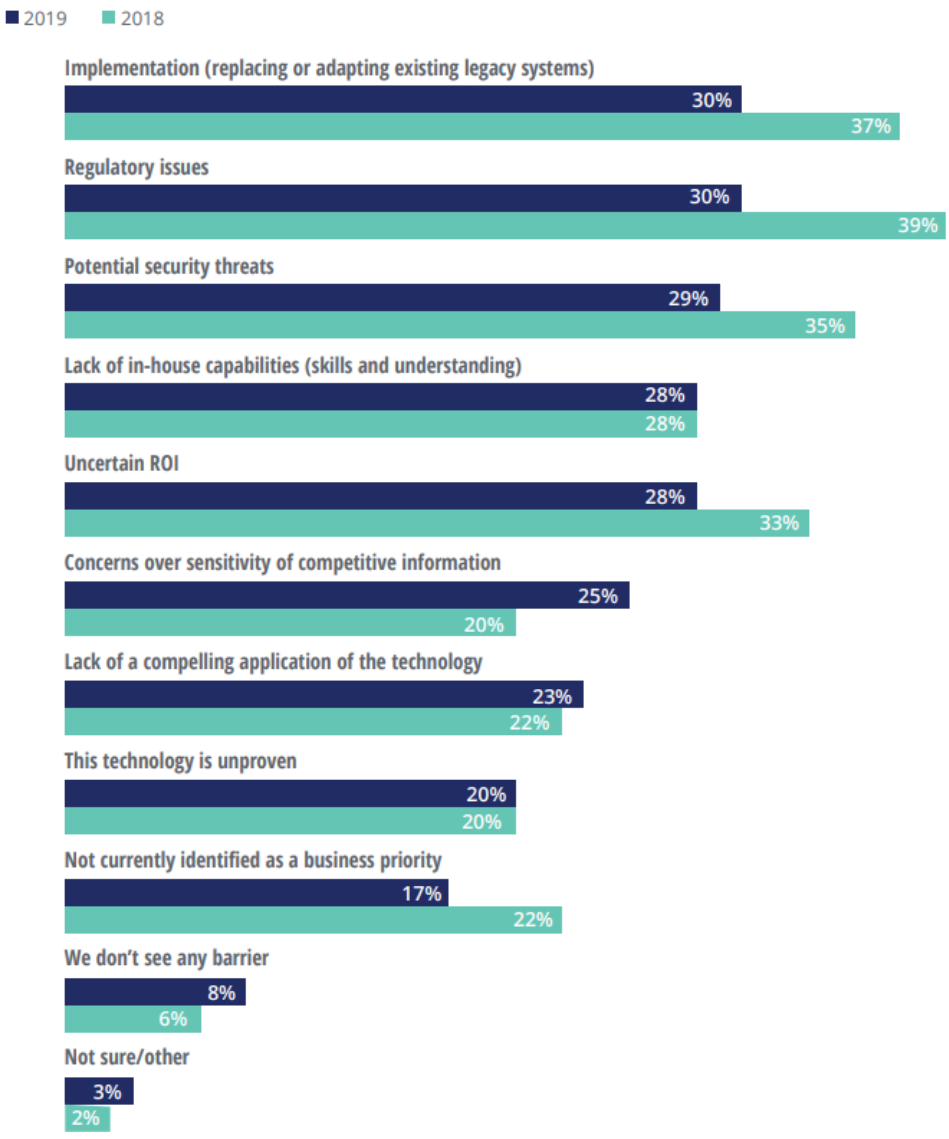
What are the significant risks associated with blockchain?

Should there be a global regulatory framework for blockchain?

Problem Statement

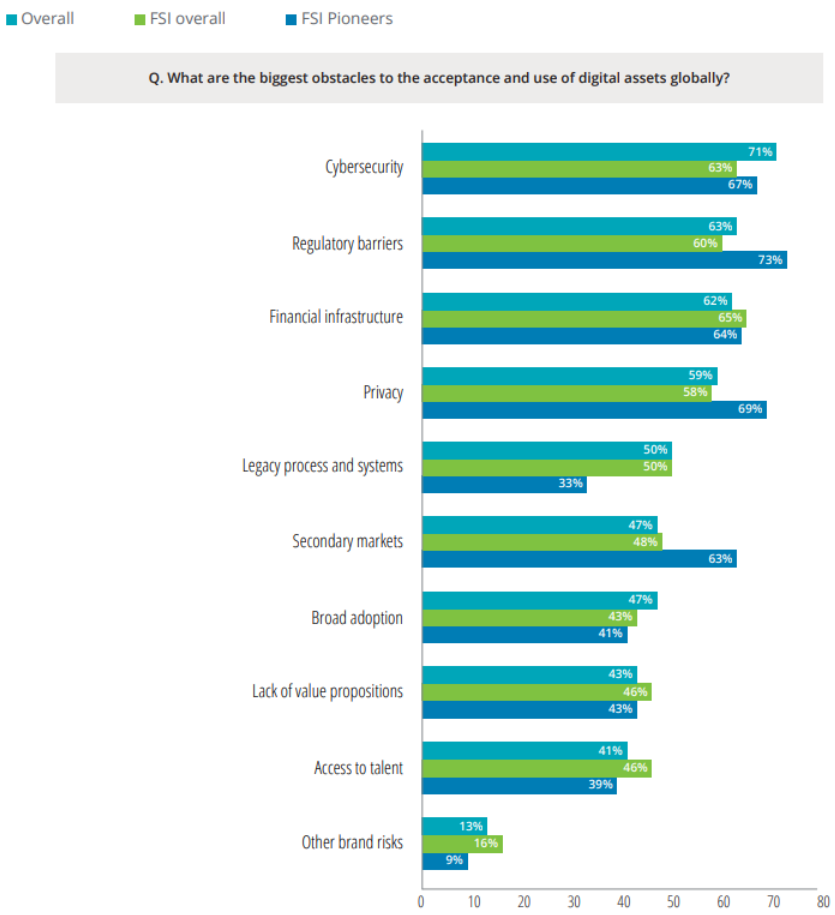
Despite all the possibilities introduced by blockchain solutions, most businesses are hesitant to adopt the technology due to its risks. Experts from Deloitte conducted a compelling study (Matthew et all., 2019) where they surveyed over 1386 senior executives in several countries to see what their thoughts were on blockchain adaptation. This survey also illustrates how the thoughts of those executives have changed over a year and compared the results of the 2018 and 2019 polls. On page 8 of their studies, Matthew et al., focus on a section that questions obstacles to greater investments in blockchain technology (Figure 3).

Figure 3. Results of a "Obstacles to Greater Investments in Blockchain" survey conducted by Matthew et al., (2019).



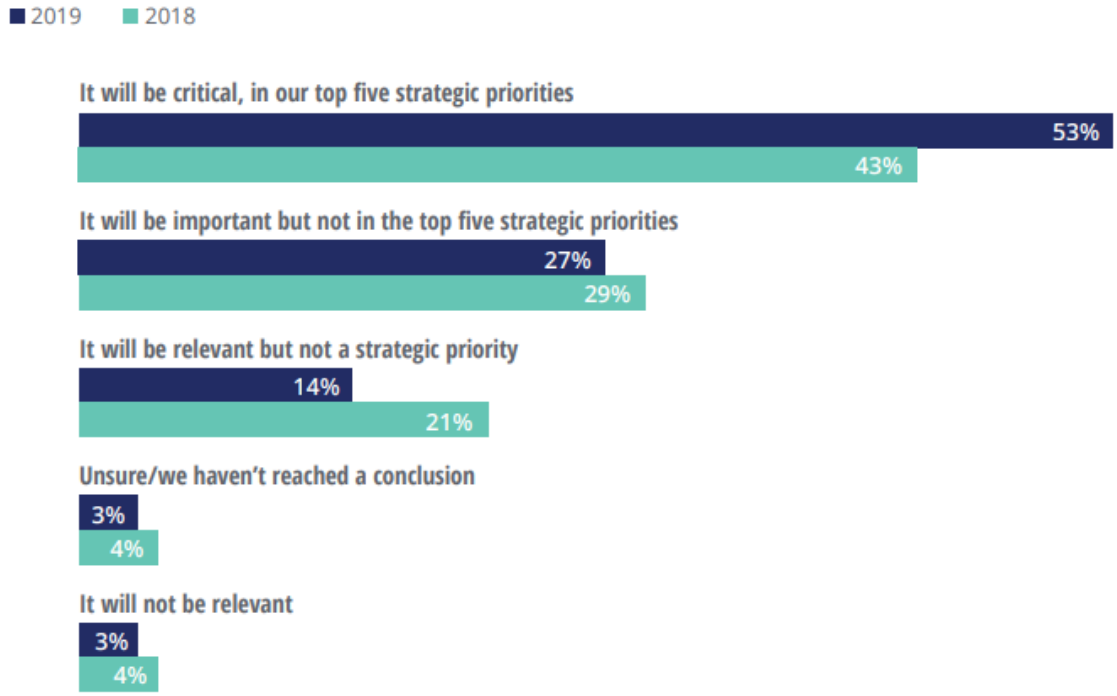
Although there is a general decrease in the numbers of respondents who see barriers to adaptation of blockchain, there are still great number of participants who are concerned about the risks (Figure 3). As seen on Figure 3, 30% (2019) – (2018) 39% of respondents are reluctant to adopt blockchain due to regulatory risks. Moreover, (2019) 29% - (2018) 35% of survey partakers indicated that they are concerned about the risks surrounding security threats. Furthermore, Mathew and Blythe et all., conducted another study in 2021 where 1280 senior executives from different countries were surveyed on their thoughts regarding bigger investments on blockchain (digital assets). Among those participants, Matthew and Blythe et al., have identified "Pioneers" – who are considered to be somewhat experienced in adopting blockchain technology (2021).

Figure 4. Survey conducted by Matthew and Blythe et al., in 2021 to find biggest obstacles to the acceptance and use of digital assets globally.



For the purposes of this study, only the results from the “overall” category will be applied (Figure 4). As illustrated in Figure 4, 71% of participants consider cybersecurity as a potential risk along with regulatory barriers – 63% (2021). Nonetheless, the same respondents from both surveys indicate that their businesses should invest more in the blockchain. For example, in the study conducted in 2019, 53% of respondents stated that blockchain has become a critical priority for their organization (Matthew et all., 2019). This was a 10% increase compared to the survey conducted in 2018 (Figure 1, p 52). And this spike in interest in blockchain has not slowed down since scholars Matthew and Blythe et al., claim in their 2021 study that businesses are still racing to define the future of blockchain technology (also referred to as digital assets) (2021). Hence, making the de-risking of blockchain more important than ever before to stimulate continuous investment in its development.

Figure 1. Survey conducted by Matthew and Blythe et al., to question the importance of blockchain adaptation (2021).



Methodology

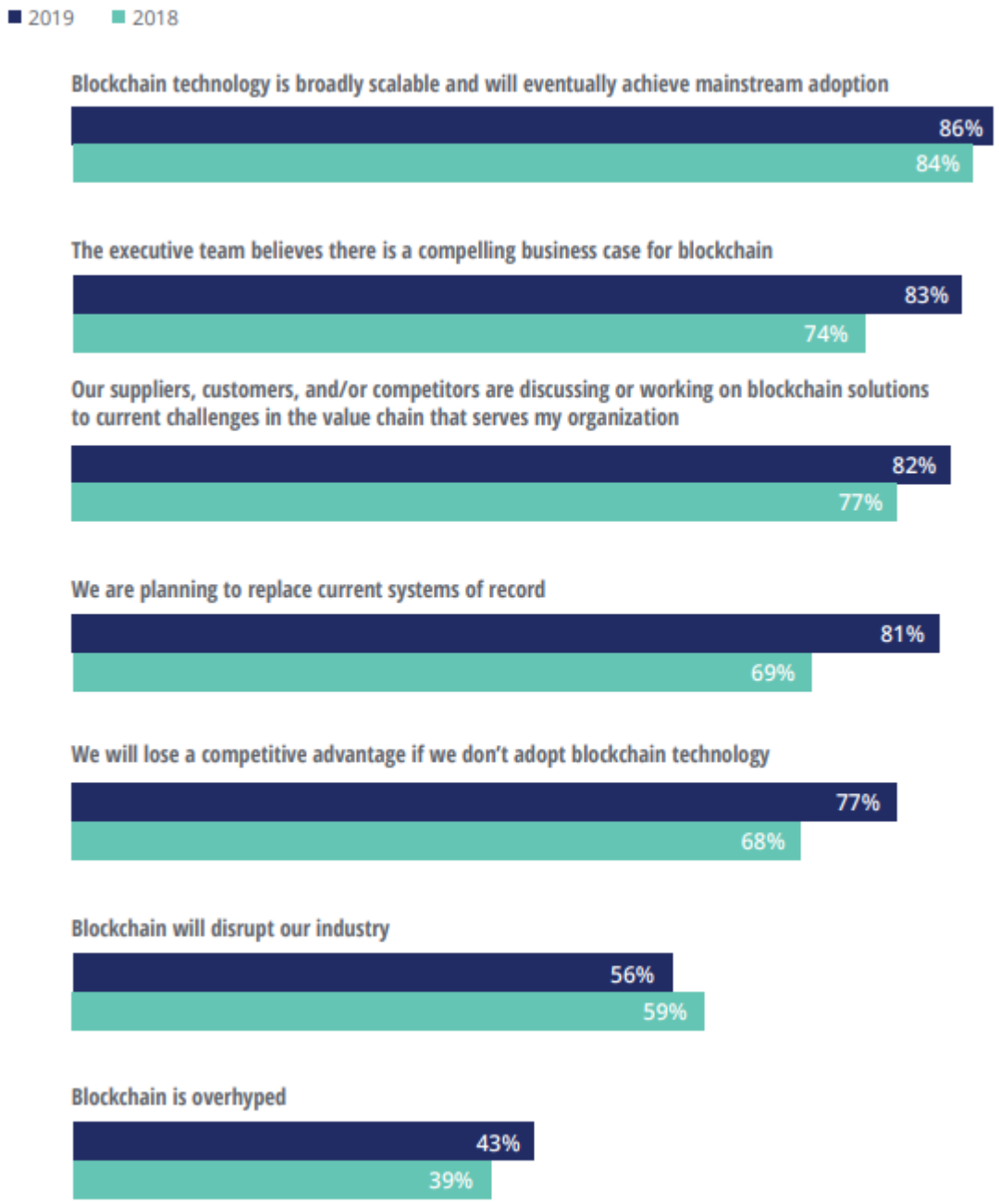
This research project evaluates data gathered from peer-reviewed articles, publications, books, and case studies; and information gathered from these resources is used to understand blockchain-based solutions and the major risks associated with them. This research will also use the data to support the claim stating that there is a positive relationship between de-risking blockchain-based risks and the development (implication) of a formal global framework for auditing blockchain-based solutions. This will be accomplished by evaluating major risks and de-risking them via the implication of the 2013 COSO Framework. To better understand the methods of real-world applications of blockchain-based risks, this study will also examine the case study completed by Distributed Bank LLC.

Literature Review

Advantages and Use Cases of Blockchain in Real World

One might assume that blockchain is only used for financial services such as cryptocurrencies. However, Mritunjay et al., from KPMG India stated that this is not the case and blockchain technology has gained popularity in other industries as well. Indeed, the use of blockchain-based technology introduced the potential to revolutionize the healthcare, automotive, telecommunication, media, entertainment, retail, and agriculture sectors (Kapur et al., p 4). For example, blockchain can help better track prescription drugs and prevent counterfeiting. It can also provide better data privacy because of transparent ownership, where participants of a transaction do not need to provide any additional information than necessary. Moreover, Mritunjay et al., highlight that blockchain can significantly improve global logistics by removing the need for paperwork filing and monitoring. Blockchain's ability to keep track of transactions and securely store the records will eliminate the need for repetitive human labor to do it manually. Hence, it is important to encourage further investment in blockchain and its development. This need is also reflected in a survey conducted by Matthew et al., (Figure A-25, p 42). As seen on the graph, 77% of respondents out of 1386 participants believe that not adopting blockchain will result in their loss of competitive advantage.

Figure A-25. Survey conducted by Matthew et al., to question the importance of adapting blockchain (2019).



To supply the demand for further investment, businesses should be able to face the risks associated with the technological miracles of blockchain. One of the ways to face the risks is to make sure that businesses are provided with adequate auditing resources as suggested by John

Ray III in his interview with CNBC regarding the FTX collapse – which was one of the biggest crypto platforms once valued at over 32 billion dollars (Rohan, 2022).

Major Risks Associated with Blockchain:

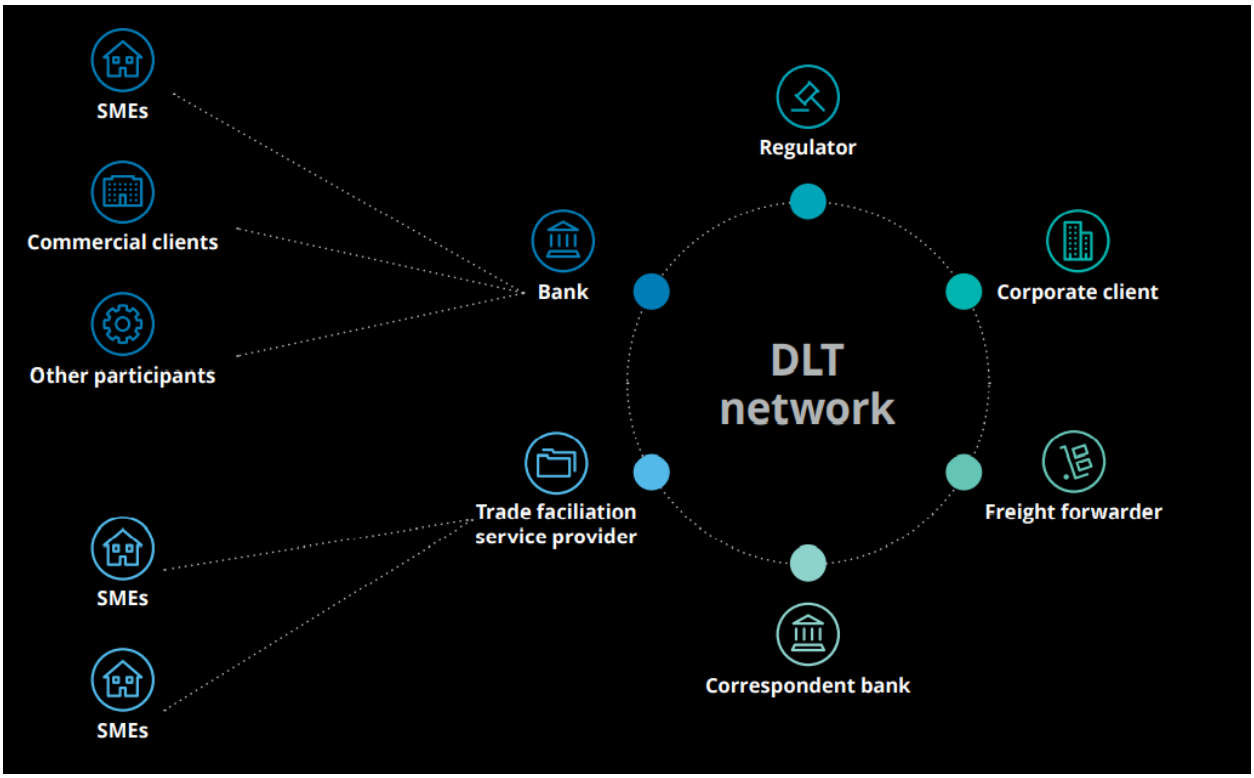
Since Effectively adopting a new technology depends upon managing the risks associated with it, it is paramount to understand them. This was the approach that Distributed Bank LLC (DBL) took when they decided to implement a blockchain-based solution for their international trade finance (ITF) (Adam et al., 2021.) Distributed Bank LLC is a bank with global operations and one of the first pioneers to implement blockchain-based solutions to prove a concept by creating a blockchain-enabled consortium composed of corporate clients, correspondent banks, trade-facilitation service providers, and regulators. The bank reasoned to pilot the solution due to its desire to differentiate itself from others in the market. This solution was entrusted to John Block – Distributed Bank LLC's internal auditor – who has a decade of experience with internal audit. John Block's main objective was to build an audit program to adequately address the potential risks presented by implementing the blockchain-based solution. As a result of the case study supplemented by further research the following areas were identified as the main risks associated with blockchain:

1. Governance
2. Change Management
3. IT Security and Operations
4. Penetration Testing
5. Data Integrity
6. Smart Contracts
7. BC and DR plan (business continuity and disaster recovery)

The following illustration depicts the usage of blockchain technology in ITF (Sandy et al.,

2019).

Figure 1. Illustration of usage of blockchain in ITF by DBL (Sandy et al., 2019).



1. Risks Surrounding **Governance** and Key Areas:
    - Approval & endorsement
    - Relevance and ongoing pertinence
    - Relevant governance committees
    - Controls over data-sharing
    - Executive oversight

As defined by the Merriam-Webster dictionary, governance is overseeing the control and direction of something (Merriam-Webster, 2020), the lack of which was highlighted by John Ray III when asked to elaborate on the FTX failure. Indeed, proper governance is an important aspect when it comes to blockchain regulation. John Block from DLB also highlighted the importance of governance in blockchain audit in their case study.

Respectively, John Block focused on key areas of governance (listed above). To start with, John Block highlighted the regulation of approval and endorsement by executive management and key stakeholders Adam et al., 2021). Next, he wanted to ensure that framework's mandate has been communicated across the enterprise to maintain its ongoing pertinence. Expectedly, relevant governance committees are important regulatory bodies to make sure that governance is appropriately implemented. The committees do so by overseeing the implementation and review of related materials to ensure that all changes and issues are addressed. These findings were also supported by the professor of finance at the NYU Stern School of Business, as he stated that because blockchain is gaining more popularity in the corporate world, its maintenance would raise governance concerns (David, 2016).

2. Risks Surrounding **Change Management** and Key Areas**:**

- Code management and permissions
- Policies and procedures
- Procedures related to creating, testing, and approving changes
- Interfaces
- Data migration

Scholars from Western Governors University claim that change is an inevitable part of life as it is of business and always crucial (What, 2020). Unfortunately, 70% of change initiatives fail to result in unprecedented effects, leaving many businesses shattered. To battle this, a structured and careful approach is needed to smoothly implement the changes; indeed, this is the exact definition of what change management is (What, 2020). This is especially the case when a disruptive technology such as blockchain is introduced to businesses. This was also apparent in

John Block's DBL case study. In the case study, one of the main components of blockchain's change management was code management and permission (Adam et al., 2021). More specifically, John Block points out the importance of the separation of duties during the software development lifecycle (SDLC). In other words, one person or group should not be responsible for both the development and review of source code. To supplement this procedure, it is quintessential to have all policies in place when it comes to change management including but not limited to emergency change documentation, creating, testing, and approval of modifications.

3. Risks Surrounding **IT security and Operations** and Key Areas**:**
    - Process for granting user access
    - Effectiveness of consensus mechanism
    - Efficacy of private key management
    - Scalability of the system
    - Data confidentiality

Introducing a blockchain-based solution means implementing a new IT environment. The new environment may not differ much from the traditional layout of the IT infrastructure, however, to sustain a blockchain-based solution, it requires considerable modifications. This impacts IT security and operations by introducing potential risks. Thus, John Block's priority was to protect the new system and monitor its operations. Among all potential risks for IT security and operations, John accentuates tracking user access, password requirements, private key management, and reviewing consensus mechanisms (Adam et al., 2021).

Tracking user access, essentially, has two major components that are combined under the principle of least privilege. Michael Gegick and Sean Barnum of Cybersecurity and Infrastructure Security Agency claim that the least privilege access principle ensures that users

are granted need-to-know or need-to-do based access whereby they have as much access within the system as necessary to perform their duties (Michael and Sean, 2013). The second major aspect of the principle is to remove super user access on a timely basis. John Ray III, the newly appointed CEO of FTX criticized FTX's executive management for using an unprotected root account to access confidential private keys. In other words, the usage of an unprotected root account was careless and if used should be appropriately protected by password requirements. Hence, password requirements need significant consideration.

Following, each blockchain-based environment will have its specific needs when it comes to key management depending on how it was built; in the case of Distributed Bank LLC relies on private keys since its ITF implemented asymmetric key cryptography. By means of this, private key controls ITF users' ability to control transactions. To manage private keys John underscores that key's life cycle (generation, maintenance, and disposal) and safeguarding it is of critical importance. In addition, to supplement the private key's security, John states that consensus mechanisms shall be reviewed for adding records to a distributed ledger. As described by Sandy Pundmann and Adam Regelbrugge et al., a consensus mechanism is a process used to achieve agreement among distributed processes or systems.

4. Risks Surrounding **Penetration Testing** and Key Areas**:**
    - The code review processes
    - The risk management plan
    - The adequacy of system resiliency

As defined by specialists in Cisco, penetration testing is a cyberattack simulation that is meant to test an entity's ability to withstand and respond to an actual attack should one occur (What is, 2022). And when it comes to blockchain-based solutions, they are as vulnerable as any

other system making them vulnerable to cyberattacks. Thus, John Block pinpoints that pro-active and reactive responses should be in place including code review processes, the risk management plan, and the adequacy of system resiliency. Last but not the least, it is important to learn from the penetration tests to be ready for the actual attacks. This includes properly documenting the findings and remediation of found vulnerabilities to increase the system's resiliency. According to the reports obtained by EC-Council, 70% of their study respondents indicated that penetration testing helps them identify vulnerabilities that can be used by adversaries if not addressed properly (What is Penetration, 2021); thus, not conducting or misconduct of a penetration test poses a great risk.

5. Risks Surrounding **Data Integrity** and Key Areas**:**
    - Appropriateness of data sources
    - Effectiveness & efficacy of controls
    - Effectiveness of application controls
    - Sufficiency of fraud prevention
    - Immutability of transactions

Specialists from ISACA take a careful approach while defining data integrity since the definition may vary based on its form of applicability (Data, 2011). To put it another way, data integrity in the realm of information security may not mean the same as for a database administrator. Nonetheless, in general, all definitions share some common attributes. These are completeness and wholeness of information, and an inability to push unauthorized changes (Data, 2011). Although one of the great advantages of implementing blockchain-based solutions is to ensure data integrity, it does not completely relieve its users from monitoring data integrity

as revealed by John Block's case study (Adam et al., 2021). Indeed, it requires very careful consideration.

To start with, the appropriateness of data sources incorporates confirming that only authorized entities and oracles can enter and change the data into the ecosystem. Meaning that blockchain data input should closely be monitored for any unauthorized modification. Next, the effectiveness of controls is preventative measures that are taken to cease man-in-the-middle attacks, which have grown in popularity to attack blockchain-based solutions. This sort of cyber-attack should highly be regarded due to the oracle's functionality within the ledgers – oracles serve as an input to execute smart contracts; thus, an intermediary can take advantage of the connection between oracles and smart contracts.

6. Risks Surrounding **Smart Contracts** and Key Areas**:**
    - Appropriateness of user access
    - Effectiveness of change management processes
    - Efficacy of the incident management processes
    - Network layer controls
    - Robustness of authority-delegation processes
    - Periodic review of the automation code
    - Effectiveness of contract enforcement

The ability of stock-trading platforms to automatically buy and sell stocks at certain pre-configured prices would be a great analogy to explain the concept behind smart contracts. As defined by Jennifer et al., smart contracts are codes stored within a blockchain that self-execute, and the results are recorded within the same blockchain (Burns et al., 2020). Undoubtedly, smart contracts are one of the key five elements that make the technology behind blockchain

technology. Nonetheless, blockchain smart contract still needs human supervision and regulation for them to operate effectively regardless of their formidable functionality. This is because even technology is prone to errors especially when it comes to programming, and blockchain is a product of human programming. This is why smart contracts are highlighted in John Block's case study. Kevin Werbach, a Law professor at the University of California Berkeley, also raises concerns about smart contracts. According to Werbach, vulnerabilities associated with smart contracts were the main reason for the collapse of DAO – Decentralized Autonomous Organization, which was a venture capital fund based on Ethereum (2022). Kevin Werbach explains these vulnerabilities by the complexity of the smart contractor's nature. Indeed, as the complexity increases, the overall security of a given system goes down states Mark Ciampa – an information security professional with 20 years of experience (Mark, 2019).

7. Risks Surrounding **Business Continuity (BC) and Disaster Recovery (DR) Management** & key areas**:**

    - Confirm that BC & DR are updated to include blockchain based controls
    - Confirm that input for the plans were obtained from relative sources
    - Confirm the plans were approved from upper management
    - Verify the adequacy of the plans

A key component to any successful business is to expect the unexpected and be ready to face it states John Block in his case study; that is when the business continuity and disaster recovery plans come into place. Researcher Carter Alzamora estimates that more than 50% of businesses can only handle 1 hour of downtime without a significant financial loss (2022). Specifically, John Block, emphasizes confirming that the entity has considered blockchain-relevant changes to its existing BC and DR plans or even create new ones. Moving forward,

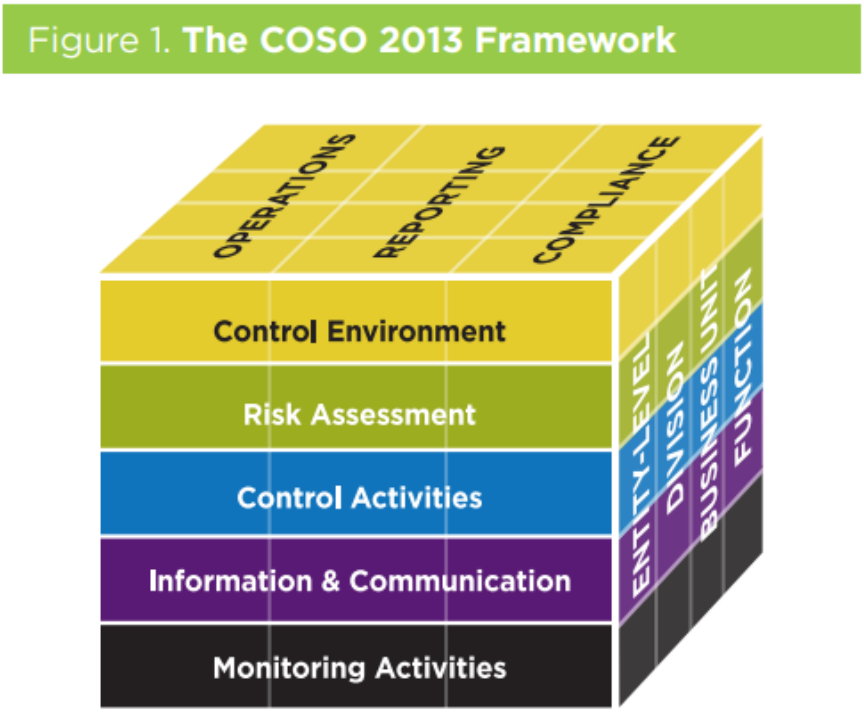
inputs of the BC and DR plans shall be thoroughly processed to ensure the validity of resources obtained from appropriate stakeholders. Last but not the least, it is principal that BC and DR plans are formally approved and reviewed annually in addition to being tested and updated based on the outcome of tests.

Findings

Background information on the 2013 COSO framework & organization

COSO did not stay behind the blockchain development and prioritized considering risks associated with it as a joint initiative. To underscore COSO's relevance to blockchain and internal audit, some background information is needed. COSO was formed in 1985 as a result of a joint initiative of the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and the Institute of Internal Auditors (IIA). The rationale behind the initiative was to provide leadership and guidance on enterprise risk management (ERP), internal control (IA), and fraud deterrence by developing frameworks. Since blockchain introduced all new sets of risks, COSO applied blockchain-specific risks by implementing them into their 2013 Internal Control-Integrated Framework. The framework is illustrated below. As seen in the illustration, the framework has five main components (which cover major blockchain risks) with a summary of key principles.

Figure 1. Illustration of the COSO 2013 Framework (Jennifer et al., 2020).

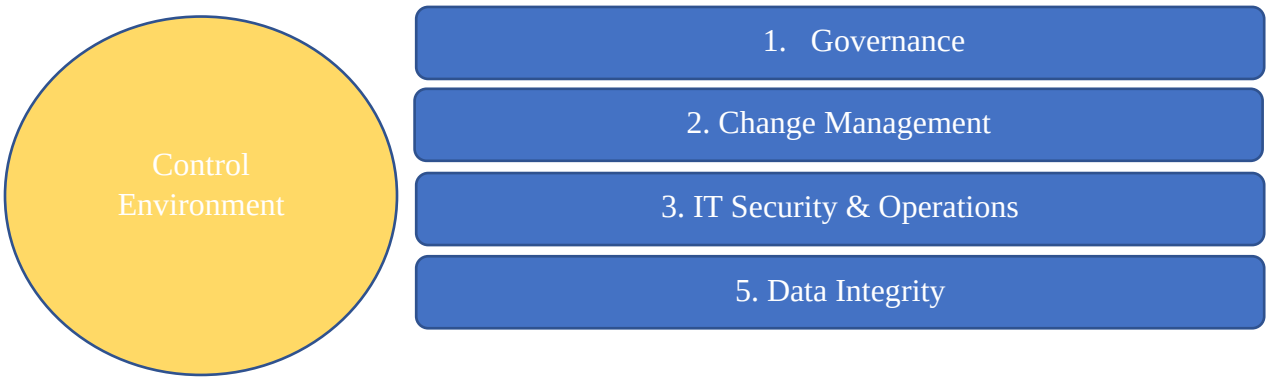


1. Control environment:
    - Demonstrates commitment to integrity and ethical values
    - Exercises oversight responsibility
    - Establishes structure, authority, and responsibility
    - Demonstrates commitment to competence
    - Enforces accountability
2. Risk assessment:
    - Specifies suitable objectives
    - Identifies and analyzes risk
    - Assesses fraud risk
    - Identifies and analyzes significant change
3. Control activities:
    - Selects and develops control activities
    - Selects and develops general controls over technology
    - Deploys control activities through policies and procedures
4. Information and communication:
    - Uses relevant, quality information
    - Communicates internally
    - Communicates externally
5. Monitoring Activities:
    - Conducts ongoing and/or separate evaluations
    - Evaluates and communicates deficiencies

Implementation of Five 2013 COSO Framework Components to Assess Major Risks:

1. Control Environment and Key Principles:
    - The organization demonstrates a commitment to integrity and ethical values
    - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
    - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
    - The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
    - The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Coverage of Major Risks:



Considering its principles, control environment is about creating an ecosystem that is aware of risks states Jennifer et al., (2020). This ecosystem consists of policies, procedures, and people that are coherently consistent with the entity's commitment to integrity and ethical values. Since blockchain does not affect human nature much, the control environment is not so drastic and only a few considerations are needed. To start with, an understanding of blockchain is paramount. People from all levels of the enterprise shall comprehend technology to sufficiently perform their

duties. This will enable the entity to take advantage of blockchain to enhance its control environment. For example, once handled properly, blockchain will aid in reducing the errors that occur due to human error while recording transactions within the ledger. Next, blockchains' functionality to automatically record and track transactions reduces human power, thus, human errors, too. Furthermore, blockchains' cryptographic immutability provides management with a certain level of trust to avoid the need for their verification due to blockchain's shared ledger that provides its users with great visibility. Indeed, when it comes to decentralized large enterprises utilizing blockchain along with advanced AI, it creates a formidable tool that can actively track and identify deviations to strengthen proactive controls. In some instances, AI might even decrease management intervention, thus, eliminating any risks deriving from management's ethical decisions and integrity.

To further face the risks, entities that use blockchain should develop a code of conduct for all its employees participating in blockchain. This will help to validate their commitment to ethics and integrity and administer employee accountability. Furthermore, even though blockchain is decentralized, all participants can come to a consensus to implement an independent third party to oversee it (depending on the type of blockchain). To not nullify the purpose of blockchain though, the third party would just function as an overseer to act upon deviations and not intervene unless necessary. Last but not the least, they should consider developing and training their employee to be better suitable for working with blockchain. Usually, this can be accomplished by assembling a cross-functional team composed of all parts of the organization whose duties include using blockchain. This will promote collaboration, effective training, and better understanding.

2. Risk Assessment and Key Principles:

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- The organization identifies and assesses changes that could significantly impact the system of internal control.

Coverage of Major Risks:

The idea behind risk assessment is a continuous process of identifying and assessing threats states Mark Ciampa (2019). Properly managing risks will enable the entity to use blockchain to its own advantage and improve risk assessment procedures. For example, blockchain provides a fast-paced environment for risk identification and mitigation since it enables real-time reporting that makes the process mainstream and fast. Moving forward, organizing ethical and legal counsel at the early stage of development will come in handy to stay

on top of risks associated with regulatory and other legal requirements. The risk assessment will also ease the potential threats behind smart contracts by assembling a dedicated team of IT experts.

3. Control Activities & Key Principles:
    - The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
    - The organization selects and develops general control activities over technology to support the achievement of objectives.
    - The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Coverage of Major Risks:

Control activities supplement risk assessment with activities that are preventive or detective in nature. In addition to all the benefits that blockchain adds to internal control mentioned earlier, there are a few advantages specific to the control environment. That is functionality such as forking; in blockchain, when one block is sufficiently written off and archived, it can no longer be

retrieved or edited unless all parties within the blockchain agree to do so by forking the block. Moreover, blockchain introduces an opportunity to significantly improve data backup and recovery. This is accomplished due to the most recent blockchains' ability to recover from nodes within themselves. To put this in other words, should one node be comprised within the network, it could be recovered with the help of nodes that are not directly attached to it yet possess the information retained within that node. As a result, traditional means of backing up data may soon become the practice of the past. While a few new controls will be added to the blockchain's way of data recovery, it will also get rid of traditional controls surrounding data recovery procedures.

Unfortunately, these opportunities will come at certain risks as well. To properly build a blockchain-based solution, control activities should be carefully structured to alleviate issues related to smart contracts, key management, consensus protocols, chain rollbacks, and forks. The combination of all these functionalities makes blockchain extremely complex and hard to manage. Moving forward, enterprise key management is another big risk. Blockchain's efficiency and security heavily rely on the entity's ability to manage private keys since blockchain by itself does not control the key nor can protect them.

Another risk comes in place due to blockchain's consensus mechanism. As strong as it may be, pre-defined conditions and rules of consensus mechanism could be susceptible to an attack called "51%". In other words, should the majority of participants of the network collaborate, they can overrule the node to manipulate it to their own advantage. Ironically, blockchain's ability to recover from such an attack, chain rollback, is another functionality that makes it vulnerable. Chain rollback could be seen as a combination of reverse engineering that serves as a backdoor to the block point in time. This poses an ethical burden on the management team who could take advantage of blockchain rollbacks to manipulate it for their own reasons. To mitigate the risks

associated with control environment, COSO has built a table that illustrates recommendations for the individual aspects of blockchain as shown below:

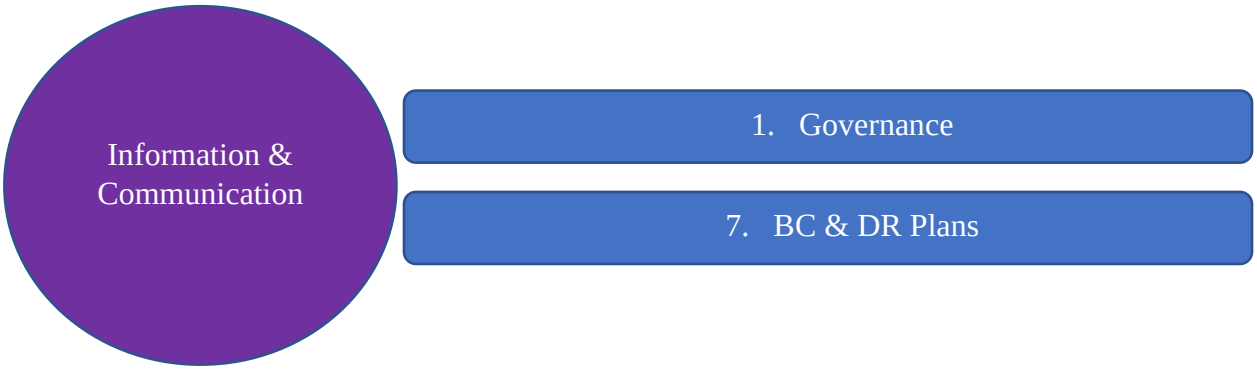
Table 5. Controls Over Key Aspects of Blockchain (Jennifer et al., 2020).

Table 5. **Controls Over Key Aspects of Blockchain**

Aspect of the Blockchain	Control Activity Considerations
Nodes	Each computer on a blockchain network is known as a "node." It will be important for companies to have established controls governing the activities of nodes that store copies of the database, perform validation of transactions, work to prepare data to be added to the chain, or perform other services. Controls may relate to the following objectives: • Making sure there are enough nodes working to minimize the opportunity for some to collaborate to attack the system. Ensuring the computational power is appropriately distributed across all nodes, such that the consensus protocol cannot be manipulated. • Testing the availability of blockchain data from different nodes in the network. • Verifying the consistency of data obtained from different nodes in the network. • Testing that nodes are performing relevant validations before agreeing to add data to the chain. • Tracking and providing incentives for correct validations and penalties for incorrect validations. (Note: An organization may not be able to perform these in relation to a public blockchain, given the large number of nodes operating on the network.)
Consensus Protocols	Consensus protocols for specific blockchains should be periodically evaluated to determine whether: • The appropriate nodes are authorized to participate in consensus. • Protocols have been appropriately designed and are operating effectively. • Incentives for complying with the protocols and penalties for not complying have been appropriately designed to mitigate fraud. The major categories of consensus include proof-of-work, proof-of-stake, or majority vote.[15]
Private Keys	Companies should take steps to manage access to their private keys. These controls will be dependent on how such keys are stored (e.g., hot **wallet** or cold wallet). In some instances, companies may engage a third-party custodian to assist in key management or to manage the assets directly. Custodians may require splitting access to the private key across multiple parties, thereby requiring approval of transactions by multiple parties (multisignature). It will also be important to ensure that the organization has considered appropriate segregation of duties to ensure that persons who approve blockchain transactions do not have the ability to record transactions within the organization's books and records.
Smart Contract	To mitigate the risks associated with smart contracts companies may: • Implement controls to validate the appropriateness of the design and implementation effectiveness of smart contracts, track changes and updates in a controlled fashion, and ensure there is proper documentation and historical record to establish accountability. • Implement controls over the inputs into smart contracts, including inputs from blockchain oracles. Controls over smart contracts should provide timely alerts and exception reports to ensure that everything is working as intended and departures and deviations are promptly reported to appropriate parties.

4. Information and Communication and Key Principles:
    - The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
    - The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
    - The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Coverage of Major Risks:

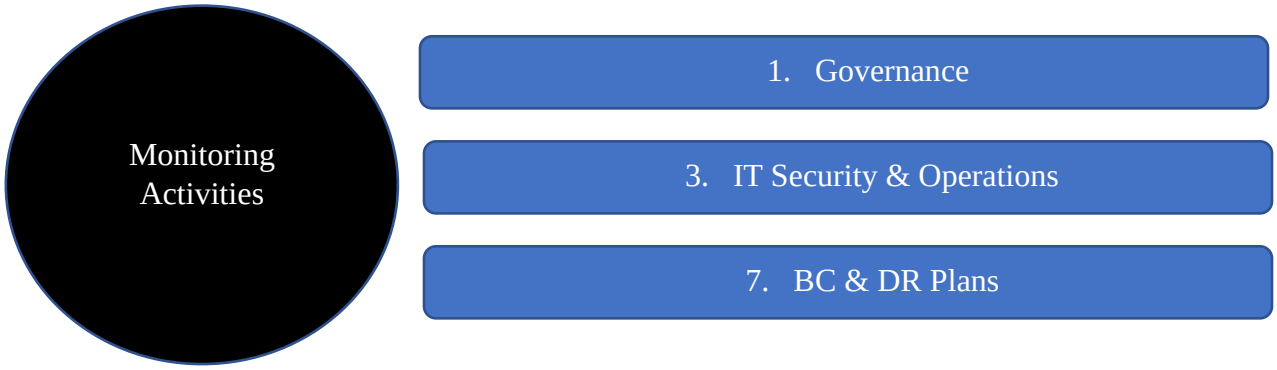


This component of the 2013 COSO Framework includes information identification, processing, and transformation. Blockchain certainly has the potential to drastically change the way how an entity will interfere with data. To start with, blockchain's transparent and ad hoc reporting capabilities are a huge benefit. Once properly implemented, blockchain will increase the availability of information within the organization. Better visibility will also lead to better data retention practices and decrease data loss likelihood. Nonetheless, entities should not completely rely on blockchain and let their guard down. It is blockchain's promising features that might delude its user into not taking blockchain's risks seriously and this is the main risk

within the information and communication control of the framework. The best way to deal with this risk is to educate key stakeholders on the blockchain. Additionally, ensuring that there is a clear and defined way of communication within the entity dedicated to blockchain would be useful. Last but not least entity should stimulate conversations with both internal and external auditors to discuss all the issues related to blockchain.

5. Monitoring Activities and Key Principles:
    - The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
    - The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Coverage of Major Risks



As the name suggests, this control is tasked with overseeing the implementation of the others. Blockchain does not affect the monitoring aspect of the framework, however, it does introduce new ways to do so. As mentioned previously, combined with powerful AI, blockchain can drastically the need for human power to interfere with data. This makes monitoring, evaluation, and auditing a lot more flexible since any data can be obtained at any time by making the audit scope flexible beyond belief. However, the risks associated with these opportunities are

the ones mentioned before related to the data amount being produced intensively. Thus, mitigating this risk is achieved by careful consideration and mitigation of risks of all the other control activities. Implementing COSO Framework into an internal audit of the blockchain-based solution is a great advantage since it enables the organization to be more prepared when assessing associated risks. As observed in Distributed Bank's case study, John Block's findings related to blockchain risks closely align with those considered by COSO and address the concerns found as a result of the survey. Since blockchain is no longer an option but is turning into a necessity, businesses should be able to trust it, and having a globally accredited framework would be a great point of reference. Moreover, once the global framework is accredited and approved, there will be third-party organizations that would be able to test against the framework and certify the testing. This could not only increase the trust towards blockchain but between businesses too.

Conclusion

Blockchain remains to be in the center of attention though it has been over a decade since its initial launch. Experts from many industries claim that adopting blockchain will be crucial to maintain their competitiveness even though they are concerned about the risks blockchain presents. Thus, it is important to de-risk blockchain to foster further investment in its growth. This study studied seven major risks associated with blockchain and supported the claim that implementation of a global regulatory framework helps to de-risk blockchain; COSO 2013 Framework was selected as the most suitable for the purposes of this study.

Appendix A – Glossary

Encryption – process of turning plaintext into ciphertext

Tokenization (token) – digital representation of an item in blockchain

Immutability – irreversibility function of blockchain

Decentralization – the concept that there is no one node with total power over blockchain

Distribution – the idea that blockchain participants can be located at different locations

Public blockchain – blockchain that is accessible to everyone

Private blockchain - blockchain that is accessible only to authorized participants

Hybrid blockchain – a mixture of public and private blockchain

Block – building units of a blockchain

Ledger – digital storage where records are stored on blockchain

Traditional network – network layer that has one central entity governing the network

Consensus mechanism – the agreement of all participants on blockchain

Node – a participant on a blockchain

Forking – idea of reversing an execution to undo blockchain

GitHub – an open-source platform where software developers collaborate

Platform as a Service – a service where entity is provided with the infrastructure and the technology to operate its business

FTX Collapse – FTX was one of the biggest crypto exchange platforms before it collapsed in 2022

Root account – account that has escalated rights (a.k.a admin right) to the entire system

Man-in-the-middle – an attack where adversary violates the integrity of connection between data input and data processor.

References

Alzamora, C. (2022). *What is a Disaster Recovery Plan and Why Is It Important?* Retrieved November 20, 2022 from https://www.recordnations.com/2018/08/what-is-disaster-recovery-plan-why-important.html

Burns et al., (2020). *Blockchain And Internal Audit: The COSO Perspective* https://www.coso.org/blockchian/blockchain-and-int-control.html

Ciampa, M. (2019) *Comptia Security+ Guide To Network Security Fundamentals.* Cengage.

Cisco (n.d). *What is Penetration Testing?* Retrieved November 20, 2022 from https://www.cisco.com/c/en/us/products/security/waht-is-pen-testing.html

Coin Insider (2021). *The Story of the DAO, and how it shaped Ethereum.* Retrieved Novmebr 20, 2022 from https://www.coininsider.com/what-happened-to-the-dao.html

Deloitte. (2019). *Deloitte's Global Blockchain Survey: Blockchain gets down to business. h*ttps://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf

Deloitte. (2021). *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets. https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf*

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal*, *72*(4), 538–562. https://www.jstor.org/stable/26414135

E-Council. (2022). *What is Penetration testing?* Retrieved November 20, 2022 from https://www.eccouncil.org/what-is-penetration-testing/

Furlonger, D. Uzureau, C. (2019) *The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age.* Harvard Business Review School.

Gegick, M. Barnum, S. (2013). *Least Privilege.* Retrieved November 20, 2022 from https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege

Goswami, R. (2022). *Never Seen Such a Complete Failure.* Retrieved November 20, 2022 from https://www.cnbc.com/2022/11/17/ftx-ceo-shreds-bankman-fried-never-seen-such-a-failure-of-controls-.html

ISACA (2011). *Data Integrity – Information Security's Poor Relation.* Retrieved November 20, 2022 from https://www.isaca.org/resources/isaca-journal/past-issues/2011/data-integrity-information-security-s-poor-relation

Kiviat, T. I. (2015). BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS. *Duke Law Journal*, *65*(3), 569–608. http://www.jstor.org/stable/24692167

Merriem-Webster.(n.d). Governance. In *Merriem-Webster.com dictionary.* Retrieved November 20, 2022 from https://www.merriem-webster.com/dictionary/governance

Srivastava, N. (2022). *What is Blockchain Technology, And How Does It Work?* Blockchain Council *https://www.blockchain-council.org/blockchain/what-is-blockchain-technology-and-how-does-it-work/*

Werbach, K. (2018). Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, *33*(2), 487–550. https://www.jstor.org/stable/26533144

WGU. (2020). *What is change management and how does it work?* Retrieved November 20, 2022 from https://www.wgu.edu/blog/what-is-change-management-how-work2005.html#openSubscriberModal

Yermack, D. (2016). *Corporate Governance and Blockchains.* Retrieved November 20, 2022 from https://corpgov.law.harvard.edu/2016/01/06/corporate-governance-and-blockchains.html