2021-04-16

Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions

Bakhshi, T

10.1007/978-3-030-75107-4_2
Springer International Publishing

Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions – Emerging Opportunities and Performance Caveats

Taimur Bakhshi, Bogdan Ghita

Abstract The recent advent of blockchain technology is anticipated to revolutionize the operational processes of several industries including banking, finance, real estate, retail and benefit governmental as well as corporate information management structures. The underlying principles of information immutability, traceability and verifiability built in blockchain transactions may lead to greater adoption of distributed crypto-ledger applications in auditing automation, compliance monitoring and guaranteeing high assurance. The present chapter discusses the contemporary applications of blockchain technology in information auditing, exploring aspects

Taimur Bakhshi 1, 2 [ORCID: 0000-0003-4750-7864] Bogdan Ghita, 2 [0000-0002-1788-547X]
1. Center for Information Management and Cyber Security, National University of Computer and Emerging Sciences, Pakistan, 2. Center for Security, Communications and Network Research, University of Plymouth, Plymouth, U.K. e-mail: [ruttbakhshi][bogdan.ghita]@plymouth.ac.uk

such as data recording, accuracy, verification, transparency, and overall value of decentralised blockchain crypto ledger for auditors. Opportunities for timeliness, completeness, and re-conciliation in appraising regulatory compliance of organizations employing blockchain-based contractual frameworks are also investigated. The chapter reviews the existing and anticipated challenges blockchain applications pose to traditional regulatory compliance models and the inherent risks for businesses and stakeholders. We highlight the impact of operational concerns such as decentralised transactions, network complexity, transaction reversals, credential management, software quality and human resources. Finally, the chapter provides perspective on assurance complexities involved in transforming from proprietary to blockchain-based framework while adhering to IT control obligations dictated by three major auditing standards Sarbanes Oxley Act (SOX), Control Objectives for Information Technologies (COBIT) and ISO/IEC 27001.

1 Introduction

Despite the disruptive potential promised by proponents of blockchain technology, in-depth studies about the impact of using decentralised crypto ledgers for information processing in auditing processes, corporate governance, and compliance remain

limited. Auditing requires guarantees of account transactions, detailed analysis, supplicated by completeness of information in the form of financial statements. To achieve these objectives, internal and external auditors should be familiar with the business, IT system controls, and specifically those system components that are related to financial transactions. To facilitate comprehensive auditing, global auditing standards, such as International Standards on Auditing (IAS), recommend financial auditors to liaise with information system (IS) auditors for collecting and processing financial data. IS auditors gather and process data from the client databases, software applications, enterprise resource planning (ERP) systems, and analyse the systems from a security control standpoint. Key requirements such as information integrity, asset safeguarding, privacy and organizational strategy are also audited. The effectiveness of an IT infrastructure against pre-defined policies, procedures and regulatory compliance is tested. The purpose of auditing is to provide service assurance guarantees to stakeholders, government, and compliance agencies as applicable. Auditing processes and compliance checks, therefore, aim to increase the confidence in published financial statements. Corporate governance, however, is often under scrutiny and inadequate flawed auditing has been observed to cause financial loss to stake holders and diminish public trust in regulatory compliance. To

rebuild confidence, newer legislation around auditing standards have been proposed, adding complexity, cost, and control policies. With the emergence of blockchain, businesses and enterprises have started to investigate ways in which the technology can benefit internal controls, information recording, and automate auditing and compliance checks. Organizations hope to reduce the workload on accounting, auditing and compliance departments while facilitating efficient access to data using decentralised crypto ledgers. Automated entry of transactional information in the blockchain and the use of pre-configured business rules to generate smart contracts effectively eliminate manual intervention. The reduction of operational costs with decreased reporting timelines and value-added auditing increased the effort of the software and financial technology industry to commoditize a range of blockchain solutions for organizations. The global auditing firms termed the Big Four (Deloitte, Ernst and Young, KPMG, and PricewaterhouseCoopers) are working on blockchain use-cases and dedicated applications to understand blockchain interoperability with existing ERP systems, economy of scale, system performance, as well as developing human resources for blockchain-enabled auditing.

Integrating blockchain technology in auditing and compliance would require a substantial redefinition of existing processes, an understanding of the multi-faceted

benefits as well as operational caveats that need to be resolved to maximize advantage. The sources of information, transaction validation, consensus among peers and the feasibility of real-time auditing should be accounted. Even though blockchain technology may offer significant advantages, several concerns ranging from integration and network complexity to taking regulatory bodies on-board for compliance need to be addressing the streamlining concerns. The present chapter reviews blockchain integration advantages in the traditional auditing process while also discussing the anticipated challenges that need to be addressed.

This chapter is organised as follows. Section 2 briefly overviews the fundamentals of blockchain technology followed by a detailed discussion on the amalgamation of blockchain applications with auditing, compliance, and service assurance procedures. Section 3 details the performance caveats and anticipated future challenges to blockchain inclusion in corporate governance. Section 4 discusses blockchain compatibility of major financial and information system auditing standards. Section 5 presents final conclusions.

2 Information Auditing, Compliance and Assurance

Information auditing, regulatory compliance and service assurance form the cornerstone of modern corporate governance. The present section overviews the fundamental working principles of blockchain technology and follows with a detailed discussion of blockchain integration in financial concerns.

2.1 Blockchain Technology

Blockchain is a relatively recent emerging technology that has found application in a wide array of avenues, including corporate record-keeping, supply chain management, energy trading, and anti-counterfeiting. The reason for quick adoption of blockchain technology in several sectors is due to the resistance to modification, and permanent verifiability of data held in a blockchain. A blockchain is a distributed crypto ledger holding data records called blocks, each block in turn containing a cryptographic hash of the previous block, along with a timestamp of transactional data. Transactions are recorded in the blockchain after validation by computing nodes hosting the distributed crypto ledger. After updating the data record, retroactive updates to the record are not possible without modification of the subsequent

blocks. Therefore, the blockchain architecture incorporates security of data by design and provides high fault-tolerance. A general schematic representing the distributed blockchain architecture and inter-party transactions is provided in Fig. 1. Blockchain networks can be implemented using public, private, hybrid and sidechain models.

In a public blockchain there are no access controls and any individual node can carry out as well as validate transactions. Participation in public blockchains is economically incentivized, and contributing nodes use popular consensus protocols such as proof of stake, proof of work, proof of authority, etc. to validate transactions. Private blockchains are access restricted and allow nodes to join by invitation. Combination of private and public blockchains result in a hybrid model and, depending on application requirements, parts of the blockchain may be controlled in a centralised or decentralised manner. The blockchain application, database and associated file system are usually managed autonomously using distributed timetamping by a peer to peer network of nodes. Record validation and authentication in the blockchain therefore, utilises collective self-interest of participating nodes offering robustness. To access data on the blockchain, as well as interact with each other, stakeholders may use smart contracts. Smart contracts are similar to automated escrows given that they can execute contractual obligations automatically.

2.2 Characteristics and Integration

The role of internal corporate auditing functions as well as the interaction of accounting processes with other aspects of the business are well-defined. Blockchain technology, therefore, may not completely transform the auditing processes but rather evolve to benefit auditing and assurance of client organizations. The role of technology in auditing and risk assessment is not new, with frequent use of artificial intelligence algorithms to accomplish future business planning.

Information auditing, however, is generally a periodic process. Auditing and complimentary processes such as risk assessment, if done in real-time using the transactional data recorded in blockchain, can continuously generate accurate infor-

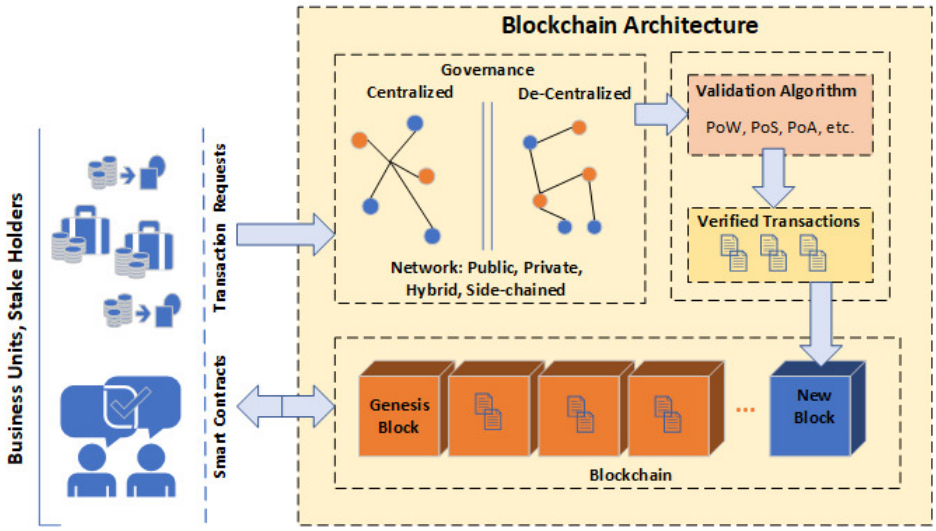

Fig. 1 Generic Blockchain Architecture

mation updates. Blockchain integration in traditional auditing framework can aid in management planning and decision making, as well as facilitate regulatory oversight bodies by sharing blockchain data between all stakeholders using smart contracts and thereby shift the auditing paradigm from a periodic concern to real-time dialogue. Blocks record the batches of transactions that have been validated and each block contains the cryptographic hash of previous block. All the blocks are therefore, linked together forming a chain, where backward iteration can confirm the integrity of previous blocks back to the first block (termed as the genesis block). Blockchain participants can, therefore, verify as well as realize the possibility of economically auditing transactions for compliance in real-time.

Some of the core characteristics of blockchain technology include decentralisation of participating nodes, the transparency of transactions, and immutability of records. These traits may improve auditing processes and information management. The definition and advantages of inherent blockchain properties are explored as follows.

Decentralisation: IT systems typically start off by centralising of resources susceptible to operational and scalability related problems. From a security standpoint, a centralised architecture allows miscreants to attack and compromise a single target. Any maintenance window of such systems may also impose service unavailability.

System failures and lack of redundancy can cause unintended and unrecoverable data loss. Moving to decentralised systems, as is the case with blockchain, allows storage of information on multiple entities. Several peer nodes in the chain can hold the same information, improving redundancy and minimizing the chances of data loss. Decentralisation also allows participating entities to directly perform transactions amongst each other, bypassing the need for a central entity such as banks. Since the record is available on blockchain, transactions can be validated. Accounting information posted on the blockchain is hence readily available for auditors who can automatically carry out their review of fulfilling obligations that are stated and implemented digitally in the form of smart contracts.

Transparency: Blockchain transparency ensures that the personal identity of the user performing the transactions is hidden, while the transactions can be publicly available and associated with the user address. For organizations, different business units can update the blockchain using their individual addresses, ensuring that information is available for auditing and compliance by the respective auditors and regulatory bodies.

Immutability: Blockchain immutability refers to the fact that once a record is added to the blockchain, it cannot be tampered or deleted. From a financial perspective this

is highly valuable, reducing embezzlement and book-keeping fraud. As discussed earlier, the blockchain is therefore a linked list containing data and a hash-pointer to a previous block resulting in a chain. The hash-pointer contains the address as well as the hashed value of the previous block ensuring that the held information cannot be changed without changing the previous block(s) and the entire chain. The result is attaining information mutability for data stored in the blockchain.

Blockchain integration in financial services spans multiple auditory, compliance and general business realms. A schematic representing blockchain framework in the organization information base is presented in Fig. 2. The primary objectives of auditing processes, including corporate governance, risk management and regulatory controls in the context of blockchain technology, are further discussed as follows.

2.2.1 Business Processes

Several business units existing within an organization define specific processes, records, and transactions. As illustrated in Fig. 2, information from each business unit can be stored in a single or multiple blockchains depending on business requirements. The choice of blockchain technology (public, private or hybrid) is dictated by the

privacy expectations, level of control over the blockchain operation and technical feasibility.

In addition to the blockchain architecture, business units can identify independent information sources on the blockchain(s) or off-chain (oracles). Business units can utilise interactions and, subject to certain predefined criteria, allow interaction and fulfilling of obligations between internal and external entities using digital smart contracts.

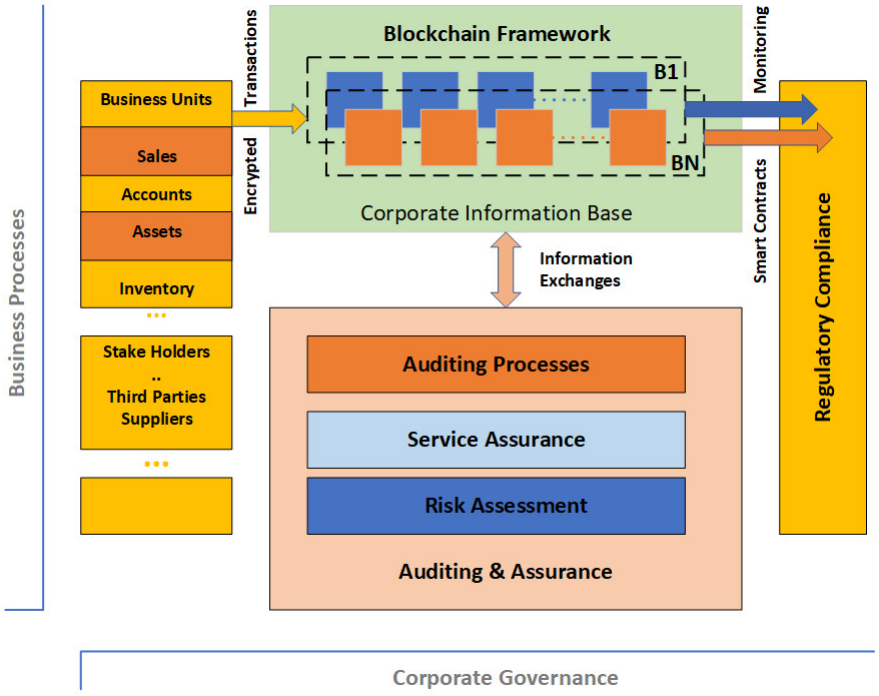

Fig. 2 Blockchain-Auditing Integration Modelling

2.2.2 Corporate Governance

Corporate governance includes the structures to manage and monitor organizational activity for the accomplishment of business objectives. The underlying governance framework relies on auditing corporate performance, earnings, expenditures, and the risks faced by businesses. With the increasing adoption of technology in the corporate workspace over the past few decades, corporate governance now also entails the development and implementation of an informational technology (control) policy.

a) Corporate Information Base The Corporate Information Base (CIB) contains the records produced by internal and external business entities stored on blockchain(s). entries added can be identified by tracking the public addresses assigned to entities. The CIB, therefore, is a single or set of encrypted decentralised crypto ledgers (B1, B2, . . . , BN) forming part of the wider blockchain framework of the organization. Using the information from CIB, corporate governance objectives of auditing, service assurance and risk management can be simplified and automated subject to relevant authorization and access control. Results of auditing reports can be fed to external and internal compliance regulatory checks, which are able to independently verify the information by having direct access to the CIB, accomplished using authentication and smart contracts.

b) Auditing and Assurance Blockchain can be applied for internal as well as external audit and service assurance activities. Financial status, asset value and company holdings can be confirmed using all or a subset of transactions available on the respective blockchain(s). Ultimately, it may change the underlying workings of the entire auditing, assurance, and risk assessment methods.

Blockchain technology, in combination with intelligent data analytics, can help making assertions about transactions, the purpose and classification of dealings. Transactions can be attributed to outflows, including a specific reason (e.g. sales and purchases, and creation of new assets). The auditors can focus more on the increasing value that can be extracted from the CIB information rather than spending extensive amount of time in gather data.

i. Auditing Processes: Blockchain can aid the accounts team in understanding the available assets and organizational obligations, making space to focus on future planning and creating value rather than basic book-keeping manoeuvres. The application of additional technology avenues, specifically machine learning in relation to blockchain can lead to automation of transactional accounting. The auditors and accountants can in turn focus on the qualitative aspects of data, instead of documenting and targeting the empirical numbers. Blockchain can help the auditing process

by providing an avenue for high-value economic interpretation, market dynamics and timely response to financial triggers. For example, information auditors can use CIB determine the debt status of a company, the possibility of bankruptcy by reconciling information from different business units, oracles and offer the same to stakeholders and regulatory bodies. Calculating the net worth of the assets in larger organizations, without having access to the relevant information sources complicates and makes the accountancy and auditing roles manually intensive. The scope of auditing work using blockchain goes beyond basic book-keeping to ascertain and corroborate meaning from transactions, the numbers and allow focus towards significant value-addition. Blockchain based record input, management, and publication via blockchain replaces traditional books and reconciliation. The focus of future blockchain-enabled accountancy and auditing would, therefore, likely see reduction of workforce in record-entry and storage and a fundamental shift to due diligence, value creation, judgmental advice and improve the processing latency involved in each avenue.

ii. Service Assurance: Service assurance guarantees can be implemented in digital resources making use of information from CIB and auditory processes. Automated contracting to furnish service assurance guarantees are in wide implementation.

Examples include, vending machines authorizing goods transfer on payment, bank credit transfers, standing orders, direct debit instructions and guarantees by brokers to provide payment on service delivery. Smart contracts in the context of blockchain imply the authorization to automatically transact on fulfilment of obligations between two parties without a central authority to validate the transfer. This is accomplished using code that can be implemented on the blockchain, between the contracting parties prior to business exchanges, giving each party transaction terms that can dynamically applied without human intervention provided the pre-defined conditions in the code are met. For example, in response to certain triggers payments can be made to entities, investments applied or liquidated, and any escrow service facilitation. In addition to reducing intermediaries, smart contracts reduce the overall risk associated with transactions for entities. In traditional settings, the breaching of contracts results in reactive civil litigation. After ascertaining the facts corrections can be enforced. Smart contracts in contrast follow a pre-emptive and preventative approach, only operating on agreed terms eliminating the scope of defaulting. The quality of code in the smart contract however, need be unambiguous and able to carry out the meaning of the agreed terms. Some of the associated challenges include moving from legal to software/IT teams for drawing up the contracts in the form of software code. Real

cost reduction would require drawing up the contracts using ready-made models and instead of investing in software firms, allowing everyday users particularly small(er) companies to automate smart contract creation from templates. Projects seeking to build programming languages to automate service assurance (legal) contracts such as Legalese can be useful in the future for integration in smart contract applications. The

legality of smart contracts, coding bugs and the repercussions/recovery from flawed transactions duly formalized by regulatory compliance would further blockchain technology in financial realm.

iii. Risk Assessment: To perform risk assessment via blockchain-enabled CIB framework accountants should ideally be adept in blockchain technical knowhow. If this is not the case then basic realization of technology fundamentals and ability make sound advisement on blockchain adoption, as well as the ability to identify

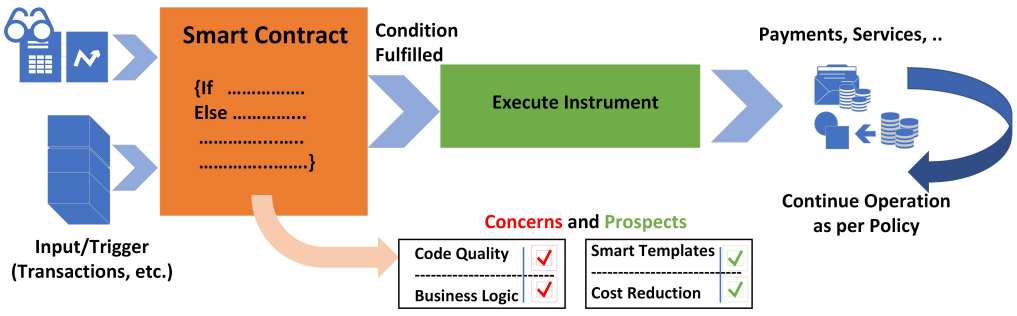

Fig. 3 Service Assurance Modelling – Smart Contracts

the potential risk and impact to business processes and clients is mandatory. Risk managers, therefore, will need to act as brokers between the technical implementors and the stakeholders. Accounts may need to brush up their skills, and in the long run professional and chartered bodies need to include in accounting curriculum. One such example is ACA qualification by ICAEW already incorporating blockchain principles in certification syllabus. Understanding the risk surrounding blockchain integration in business is again vital to future successfully traction of crypto-ledgers and smart contracts in the enterprise culture. Some of the focal areas requiring due consideration are highlighted as follows.

- Blockchain by itself is a foundational technology that may need years and even decades to mature and embed in the financial architecture. If not blockchain, at least a fundamental implementation of distributed crypto ledger is on the cards for many companies.
- Blockchain integration with legacy enterprise software should be seamless (unless used exclusively) to allow business operations to continue undeterred.
- The operating costs of the proposed blockchain solutions from a risk perspective should be comparable to and ideally lesser than traditional methods.

- Records (disputes and reconciliations) should be processed efficiently to derive value from capital information, aid decision making and managing future risks.
- Economic rewards proposed by blockchain in relation to the documented risks will ultimately decide adoption success. The benefits expected should be applicable to organizations internally as well as external regulators.
- Cyber security controls should be taken into consideration according to the broader IT control policy. Authenticating blockchain nodes, ensuring best coding practices for smart contracts, external interaction such as the selection and oversight of information provided by oracle(s) are some of the essential factors.
- Internal auditors should be able to assess the strength of block immutability, cryptography scheme, storage of private and public encryption keys.
- Regulatory compliance and legislation should recognize blockchain transactions, smart contracts, give legitimacy to underlying exchanges and thereby reduce the risk factor for organization wanting to migrate to crypto ledgers.

The capability of organizations to address the above non-exhaustive list of risk assessment avenues vary considerably. The transformation required for internal auditing, technical updates and regulatory operations may be beyond the capacity

of individual companies and exclusive use of blockchain for that matter will take considerable time.

The primitives discussed above are only a general starting point for risk mitigation and depending on organizational policy each business (unit) can tailor and extend the risk identification framework.

2.2.3 Regulatory Compliance

Regulatory compliance directs financial operations providing guidelines as well as internal/external oversight to ensure businesses are functioning as expected. Auditing at pre-defined intervals and reporting of the respective findings determines the

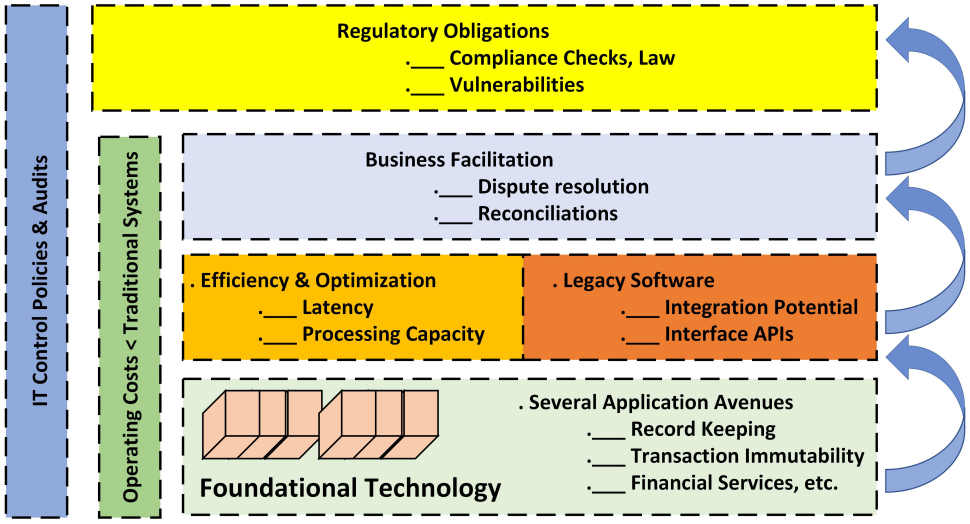

Fig. 4 Abstract Risk Assessment Modelling

efficacy of financial operations and provides businesses, regulators, and stakeholders such as clients the means to gauge financial stability. Compliance monitoring, however, is not limited to financial audit reports, corporate governance primitives such as standard processes, IT control policy, inter-departmental and external interaction fall within the scope of compliance checks. Additionally, with the inclusion of blockchain the rules for adding and removing nodes, tampering and errors in digital components, validation and verification systems discussed in relation to risk management are also applicable to compliance checks. Compliance standards also requires network management, the viability of consensus algorithm, and smart contract monitoring. Regular auditing facilitated by blockchain would have to demonstrate that system functionality is not compromised and complies with regulatory checks. Regulatory bodies should, therefore, be able to recognize blockchain as a financial technology and introduce respective compliance checks for the entirety of services falling under the crypto ledger spectrum.

In addition to regulatory compliance blockchain-based operations and contractual management would also require legislation. Operations performed and services fulfilled using smart contracts would expect recognition by courts. Blockchain transactions and smart contracting transaction breaches will still need to be enforceable

under law if there are any breaches to the contract. Redressal should be available and given due cover by law and compliance directives. Breaches could be due to issues in software or exploited in an unexpected way by the involved parties resulting in objection(s) and require redressal.

While blockchain characteristics allow for reasonably high security it does not tackle governance problems such as principal agent. Agents within different business processes have different levels of privilege in accessing and updating financial record-keeping for example, blockchain-based CIB. When the privilege level of an agent allows them actions that impact another agent/entity in that organization then the cost of the risks may impact the principal more than the initiating agent. This is quite likely when agent acts in self-interest rather than that of the principal, probably because the principal has minimal control over the agent action.

In traditional company structures signed contracts that regulate employee-organization relationship that is enforceable in courts of law. Distributed Autonomous Organizations (DAO), part of the greater blockchain spectrum allow agents to interact using open-source protocols. Performing tasks on the blockchain network is individually rewarded by tokens native to the respective blockchain network. Since, there are no bilateral agreements or legal contracts individual is only steered by net-

work incentives. Regulating the behaviour of all the network participants is solely by the protocol (or smart contract). Overriding the software code of the protocol or the contract can lead to unexpected consequences with substantial financial loss. A primary example of DAO failure was in the case of Ethereum blockchain, where the inadequacies in the code (smart contract) resulted in financial hijacking. Participants (the majority) agree to roll back the loss of funds while some maintained status quo resulting in the creation of a separate blockchain (Ethereum Classic). In the case of Ethereum, roll back was only possible as more than half of the participants agreed to it.

Regulatory intervention is therefore, required to encourage blockchain transactions with due processes to address coding related and intentional miscreation where the concerns of legitimate users in view of approved actions can be redressed.

2.3 Realization Prospects

This section summarizes a non-exhaustive list of the potential improvements to operational processes and realization of auditing and compliance efficacy allowed by blockchain technology.

1. Accounting concerns associated with transactions and transfers can be transformed and automated using blockchain and smart contracts.
2. Using CIB even minute transactions can be recorded expanding the scope of accounts and auditing functions also allowing quicker reconciliation in case of disputes.
3. Rights and obligations can be pre-defined and implemented automatically using smart contracts.
4. Access to timely information and wider data can aid comprehensive data analytics which may be further combined with machine learning and AI for decision making and increasing the efficacy of accounting.
5. Reduction in workload of accountancy and auditing due to real-time book-keeping can allow more time to understand qualitative aspects of transactional exchanges and the scope of value-addition activities such as advisory and judgement can be expanded.
6. Increasing number of records can be phased on to the blockchain, simplifying as well as increasing compliance and regulatory checks. The certainty over transaction provenance can be implemented in real-time.

7. Companies may select between the number of distributed blockchain nodes and whether the network will be public, private or follow a hybrid approach. Additionally, companies can also decide on the type of actions allowed through the execution of smart contracts between different agents internal or external to the company. Financial responsibility can hence be recognized through blockchain instruments.
8. External relationships with oracles and regulatory bodies can be maintained via permissioned relationships, where access on limited need-to-know basis is possible.
9. Companies seeking absolute control over their blockchains and using these solely for internal records or as a source of double book-keeping, a parallel ledger in tandem with traditional accountancy can use private chains within the organization. The same ledger can be shared privately with external trusted parties, e.g. suppliers. The system if successful, and subject to future regulatory approval can be rolled out to completely replace traditional financial reporting.
10. The elimination of human intervention directly and indirectly removes individual influences from corrupting the information base and lead to impartial adherence

to prescribed conditions. In the case of DAO, implementations however, coding issues and lack of legislation needs to be considered.

11. Automation can lead to increasing scalability of use, operational efficiency and remove the need for costly on-site audits and physical and paper-based inspection of inventory/records. Additionally, the speed of processing provides extended capability to accelerate settlements, payments, reduces costs and the cost of involving intermediary brokers.

The potential blockchain benefits although non-extensive, can also introduce certain performance caveats and implementation challenges which are considered in the next section.

3 Anticipated Challenges

Incorporation of blockchain technology in auditing, compliance and service assurance primitives requires a think beyond the technological expertise. Organizations must be able to verify and assess the advantages and challenges blockchain will bring to their corporate processes, whether the benefits overcome the technical and governance challenges. Proponents would need to document the advantages of a

distributed crypto ledger over existing ERP databases, improvements to the business, the economy of scale and increase in revenue. In-house auditors will need to consider a plethora of avenues. While architectural decentralisation and encryption offer substantial information security advantages, issues such as system and network latency, key management, business continuity planning and software integration with legacy processes require a (re)evaluation of blockchain technology from a usability standpoint. The extent to which existing auditing and corporate team will involve and streamline these issues depends on the acquisition of an outsourced solution from a third party, outsourcing business units or designing bespoke application(s). The present section highlights some of the concerns poised towards auditing and compliance processes influencing greater crypto-ledger inclusion in corporate governance. The primary areas of focus can be categorized in the following components.

3.1 Information Consistency

During block creation independent blocks can be produced concurrently resulting in temporary fork conditions. Tracking of hashing history using a specific blockchain algorithm can result in different scores for version history, the highest score being selected. Therefore, there orphan blocks may exist that are generated but not included

in the blockchain. One of the undesirable consequences of decentralisation is having different database versions of the hash-history at certain times. Blockchain nodes only store the highest-scoring database version and replace it if a further higher scored version is received. The existing database at the node is updated or extended and the improvements are re-transmitted to peering nodes.

Temporary forking condition results in the lack of guarantees that a particular recorded entry will remain the best available version of hashing-history forever. Furthermore, blockchains add score of new blocks on existing blocks and this operation is incentivized, rather than overwriting old blocks. As the database grows at each node the probability of a database entry becoming superseded also decreases exponentially. Temporary forking can result in misalignment leading to different versions of the blockchain. If the blockchain is being used to track commodities, business goods, and hold transactional information it can cause information volatility, and even if temporary can affect real-time auditing. The duration of such volatility may hamper business operations and bias decision making. Continued service assurance and regulatory compliance can, therefore, be difficult to achieve and require an assessment of the type of business records that can be moved to blockchain-based ap-

plications. Blockchain-held records should preferably be able to sustain information volatility around forking events.

An extended version of temporary fork is in the form of a hard fork. Hard forks arise as a result of change in the algorithmic rules so that the validation process considers blocks produced as per new rules as being invalid. All blockchain nodes need to upgrade the algorithmic rules to avoid hard forking. Unless all nodes are updated to the new software (rules) a permanent misalignment termed a split can occur leading to new and legacy blockchains. Popular blockchain application Ethereum was subjected to a hard fork to overcome the exploitation of code vulnerability that resulted in two active chains the new Ethereum and classic Ethereum. Hard fork proposals to circumvent theft and coding bugs may lead to unintended chain creations. Rolling back blockchain records is hence seldom possible and can result in a permanent split, taking considerable time to revert to old rules or never.

As with temporary forks, auditing processes using blockchain-held information need to carefully consider the implications of hard folk. Pre-emptive policy planning including organizational decisions to follow information based on majority consensus can be useful. Determining which entity has majority consensus can be left to the organization provided it follows (any) regulatory assurance provided for the

same. Following a hard-fork auditing manager may also consider moving account transactions to the newer crypto-ledger with sufficient asset adjustments to comply with regulatory discretions. Notifying and making agreements with the involved parties including clients, third-party suppliers and regulatory bodies and integrating their respective stakes in the new chain can again be quite challenging and prone to delays.

Auditors and compliance managers need to closely monitor hard forking announcements by their respective blockchain application and understand the affects these may have on their accounts. Margin requirements for any errors and overlaps need to be determined. In case of any unreliability in information or extended volatility, businesses need to be able to move to legacy systems formally notifying all concerned.

3.2 Network Complexity

Blockchain architecture presents a distributed set of nodes inter-connected via a network, the Internet. The average time it takes to generate an additional block is termed as block time. Depending on the blockchain application being used the block time (block creation frequency) can vary between a few seconds to a few minute(s).

Once the new block is created it becomes verifiable, low latency and high frequency block creation leads to quicker transactions. Latency is an important contributing factor in real-time auditing as high block time can lead to slower transactions and take longer time to verify transactions.

To improve block time the available bandwidth needs to be sufficient allowing the transactions to traverse the blockchain network before verification by the respective consensus algorithm. Increasing number of users also increases the transaction workload requiring better network connectivity and improved bandwidth. Effectively recording transactions also needs sufficient storage capacity, energy consumption and can be costly. Auditing whether internal or external should cater for the scalability of the blockchain solution, specifically the throughput of the system in transmitting, receiving, and validating transactions. Public blockchains can be difficult to manage and scale to organizational requirements, the number of transactions and validation latency. However, the network can be relatively simpler to manage for private blockchains and fine-tuned to handle the required number of transactions.

3.3 Credential Management

Blockchain data storage over a distributed network reduces the risks of data being held in one central location and allows information (storage) redundancy. Compromise of data over a single peer does not alter the integrity of information due to decentralisation. Peer-to-peer network reduces the vulnerability of data that crackers can exploit; however, peering requires data encryption during transmission. Blockchain security mechanisms prevalently use public-key cryptography. The public key is an address on the blockchain, tied to the tokens traversing the peer-to-peer blockchain network are recorded against this address. The corresponding private key is the password used to allow client access to digital assets and perform (available) interactive operations with the blockchain application.

Key encryption is vital to the decentralised operation and broadcasting of transactions on the blockchain network. While the transactional messages are delivered on a best effort basis, provisions need to be made regarding the storage and management of private keys. Public key infrastructure (PKI) and addresses can be embedded in the respective blockchain application and the distribution of private keys can still rely on the same PKI. The key management and exchange mechanism may require regulatory oversight to increase client confidence and minimize asset theft. Transac-

tion recording through time-stamping schemes needs to be employed in tandem to allow consensus algorithms validation and serialization of recorded changes.

Growth in the size of the blockchain can inevitably lead to a centralisation is risk since increasing computing resources are needed at the peers (blockchain nodes) to process data and as a consequence also requires securely storing the encryption keys. Compromised credentials coupled with coding bugs can lead to financial losses, requiring change in business rules and algorithmic implementations resulting in hard forking. A primary example of programming errors and information comprise is the case of Decentralised Autonomous Organization (DAO) which cost millions of dollars and resulted in a hard fork of Ethereum. The same is true for bitcoin forks and vulnerabilities leading to errors earlier on. Comprise of credentials and software susceptibilities are not limited to crypto-ledger transactions alone, other blockchain and stand-alone complimentary instruments such as smart contracts are also vulnerable to errors. From an auditing and compliance perspective credential storage and access needs realistic testing prior to production (live) implementation.

Table 1 Anticipated Challenges and Remedies

Anticipated Challenge	Description	Remedies
Information consistency	Inconsistent and contradicting information.	Auditing of validation sources, consensus protocols.
Network complexity	Bandwidth and throughput issues.	Evaluation of bandwidth requirements, node capacity, and available resources prior to implementation.
Credential management	Storage of private and public credentials.	Formalization of access control models, adoption in blockchain credential management.
Software interoperability	Software bugs, coding issues and overlapping or contradicting logic.	Formal software development and quality control approach.
Regulator oversight	Inadequate or incompatible regulatory checks.	(Re)definition of legislative and regulatory scope to encompass blockchain technology.
Human resourcess	Untrained accountancy and auditing teams.	Incorporation of blockchain technology in professional training syllabus.

3.4 Software Interoperability

Software interoperability generally characterizes and defines an IT system whose interfaces are understood and can be integrated with complimentary products and systems, in present and future without restrictions. At present several blockchain projects and applications have been developed and can be considered as well established in the public and private domain, e.g. Ethereum, Bitcoin, etc. Despite increasing adoption there are interoperability issues of blockchain infrastructures

amongst each other as well as with legacy enterprise systems. Typical ERP systems have multiple functional modules defined by business requirements, including internal and external auditing and accounting mechanisms, third-party and supplier logistics, control and management, production, and quality control. These system components are widely used having vendor support and are present in all industries. Blockchain being relatively nascent, requires participants to join forces in creating an interoperable platform from a technical as well as corporate governance perspective. Blockchains systems being used by an organization need to be compatible with the existing ERP systems to maximize advantage and remove duplication. The degree to which legacy systems can be integrated with blockchain applications, and decisions pertaining whether the blockchain will be embedded into the legacy system requires technical evaluation and support from existing software vendors and blockchain infrastructure designers. Furthermore, the rules for interaction between the legacy frameworks and blockchain infrastructure need to be agreed keeping in view the scalability of the proposed solution(s). Increasing participants, larger data volume (ledger size), network resources and corresponding changes in underlying transactional latency in relation to present processing and payment systems are all indicators for auditors to consider before leveraging blockchain applications.

While interoperability remains a primary concern, at the more fundamental level code issues in blockchain systems also present a risk avenue that hampers blockchain adoption in auditing. Using recognized software development techniques and formal verification of code operation, the risks arising due to flawed logic and purposeful malicious interactions can be minimized. Smart contracts for example, are frequently used in combination with blockchain applications. Using automated logic to carry out per-agreed terms the smart contracts eliminate the need for human intervention in fulfilling interactional requirements. As the underlying logic of the contracts increases in complexity, addition of participants and policy milestones, so does the probability of flaws in the implementation. Coding bugs in the conditional logic of smart contracts may result in flawed transactions that might be impossible to roll back. Of particular interest is the interaction of the blockchain with components that are not part of the architecture – oracles considered to be the sources of integral information. In the auditing framework, the oracles might be external entities such as vendors, suppliers, clients, insurance agents, etc. providing information that needs to be cross validated by others (oracles) prior to being recorded in the blockchain. The risks associated with performance of these independent validators – oracles, can in turn compromise the authenticity of transactional blockchain information.

Erroneous information may contaminate the entire blockchain. The identification of oracle-installed information can be difficult to identify, quantify and adjust in auditing as well as future risk management.

3.5 Regulatory Oversight

While several technical challenges impede the implementation of blockchain-based auditory processing, one of the greater non-technical challenges arises from serious lack of regulatory oversight and planning. Regulatory uncertainty poses a barrier to the wider adoption of blockchain technology in public entities and private companies. Across the globe several national and international regulatory bodies, financial organizations and governments have started to study and discuss the prevailing technical and compliance checking challenges posed by blockchain-based auditing. However, the regulatory oversight is acutely short of being settled. There are insufficient standards and regulatory controls in place to ensure functional auditing, compliance and service assurance provisions using blockchain. In the European Union (EU) it is unclear how blockchain-based corporate information record-keeping can ensure compliance with the General Data Protection and Regulation standards (GDPR) dictating high privacy. GDPR allows E.U. citizens to be able to understand the way

companies collect data on them and to seek their explicit consent before using the information their information. GDPR also allows for data modification and deletion (as necessary or) requested by individuals. Blockchain however, allows for immutable and undeletable transaction history from the (first) genesis block thereby contradicting crypto-ledger principle. There is no real equivalent of the GDPR in the US and a range of state and federal rules exist for the same privacy issues. The closest complimentary is the Federal Trade Commission having very limited powers to implement privacy policies over businesses. Therefore, the inclusion blockchain in EU as well as the US markets necessitates regulatory oversight and compliance defining personal data, information control mechanisms, deletion of data, and accountability in case of breaches. Regulatory compliance may also allow certain information to be kept on the blockchain while off-chaining remaining records. Furthermore, the rules pertaining anti-money laundering legislation also require access to auditing and accounts, dealing with such technicalities needs to be detailed at length by regulatory bodies.

Overall, the impact of blockchaining on auditing and the regulatory oversight required remains a greatly under-researched area. While the technology itself is

promising, it has the potential to disrupt existing regulatory oversight and newer relevant legislation and control frameworks are needed.

3.6 Human Resources

Auditing functionaries are expected to adjust their human and organizational capital to seamlessly continue with mandated responsibilities in a blockchain-enabled corporate information system. While qualified accountants, auditors and legal counsels are nonetheless an integral part of the corporate workforce, individual organizations need to expand their human resources by taking cyber security experts and blockchain gurus onboard. Lack of available human resources in the technical and corporate domains may lead to unnecessary delays in implementation where blockchain may be of immediate benefit. Well-trained individuals may not only help in the actual adoption of blockchain but also research and improve blockchain integration. Where such resources are not available internally, outsourcing can be a viable option to meet the workforce demands, contracting individuals and companies having sufficient experience with emerging blockchain and complimenting technologies. Future auditing professionals, academia and analysts would likely benefit by inclusion of blockchain operations in their respective training. Specialized training by organi-

zations to bring their auditors up to speed with blockchain technology can also be useful. Auditing organizations, chartered bodies, IT certification streams and governmental agencies in general also needs to incorporate blockchain training in core auditing and accounting courses and start certification programs for the same. Some chartered organizations such as the Institute of Chartered Accountants in England and Wales have already incorporated blockchain syllabus in their ACA (association of chartered accountants) qualification. Blockchain-tailored programs are also available for Chartered Public Accounts (CPA) members in North America. Although several individual courses are also available for practitioners, the quality, practicality of use and applicability to the auditing and accounting profession again requires regulatory oversight and standardized evaluation mechanisms.

4 Standards and Transformations

This section highlights the compatibility between decentralised crypto ledgers and the prevalent legislative and auditing relating to financial and technology controls including SOX, COBIT, ISA and ISO27001.

4.1 Standards and Legislative Requirements

Businesses implementing blockchain will need to evaluate the standard regulatory and legislative controls related to the platform, transactions, operations, and auditing requirements. Experts generally tend to agree that blockchain provides targeted solutions to fraud prevention and still requires adequate maturity to replace the entire fintech ecosystem. Proponents, however, argue that blockchain can be used for record-keeping as well as fact (reality) checking by intelligently designing the control logic and authenticating inputs to the blockchain application. Trust models defining the scope and interaction of external sources such as Oracles and in-house legacy IT systems with the blockchain applications are therefore, needed. Additionally, financial and IT industry has several prominent controls, assurance, legislative and standardization frameworks applicable that the blockchain platform should satisfy if companies are to increase stakeholder, client, and regulatory confidence in the technology.

The present section explores the scope of prevalent IT control and reporting standards including the Sarbanes Oxley Act (SOX), Control Objectives for Information Technologies (COBIT), and ISO/IEC 27001 in the context of blockchain applications. The important highlights of the regulatory acts and standards, a mapping of

the respective requirements and detriments in relation to blockchain technology are discussed as follows.

4.1.1 Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX legislation was passed by the U.S. Congress in 2002 to deal with rising financial crimes and to protect investor interests from accounting fraud as well as organizational bankruptcies. SOX at its core enacts formal guidelines for auditors, credit rating companies, investment funds and governmental agencies to identify responsibility and accountability in all matters financial. SOX compliance (internal) audit take place once a year by an independent SOX auditor. Prior to the audit, specifics such as conflict of interest, time required for the audit, areas of focus, expectations and the findings being reported to all relevant stake holders needs to be agreed. SOX compliance seeks to improve investor confidence, lower costs, and introduce stronger internal controls.

Some of the key features pertaining financial auditing from different sections of the act include the following:

- **Section 302 – Financial Accuracy:** SOX mandates and assigns financial accuracy in corporate reporting on the executives, personally.

SOX requires the recording of financial information for each business category independently and not be attributed to assets that might artificially inflate income and share price. Using blockchain decentralisation, auditors can be certain the financial information being recorded is available in several nodes and cannot be tampered with later.

- **Section 401 – Off-sheet Reporting:** All off-balance sheets and transactions to be officially reported.

  Reporting off-loaded balance sheets and debts is mandatory under SOX. Different blockchains can be used to track balances of different nature, the information when inter-linked providing a coherent view of all available financial data to the auditor. Furthermore, financial reporting before and after any mergers and acquisitions, is also a key SOX requirement. Immutability of blockchain records ensures that once the information has been recorded it cannot be deleted or artificially under/over-reported and therefore, presents the accurate figures of assets before and after any mergers, profit declarations and acquisitions.

- **Section 802 – Altering Documents, Mergers and Acquisitions:** Realistic pro forma evaluations as opposed to hypothetical and inflated figures before mergers and acquisitions.

Similarly, overestimating of assets, and manipulation is not possible due to the transparency involved where several parties on or off-chain (oracles) can verify the blockchain transactions through a realistic validation of asset values.

- **Section 409, 906 - Executive Privilege and Disclosure:** Prohibition of personal loans to executives. Executives to disclose ownership of (any) equity security. The main drawbacks associated with SOX are the high operational cost associated with hiring of external auditors, legal fee and overall loss in productivity while trying to satisfy all SOX Act requirements. While a fundamental concern, transparency is costly to track and implement in the corporate structure. Multi-faceted financial information needs to be continuously checked, updated, and stored. Any updates also should be immediately available for perusal by stakeholders. Such requirements are difficult to implement in traditional accounting departments, often under-invested and under-resourced. Blockchain technology can be used to incentivize greater transparency, information sharing and automation. Using smart contracts providing controlled access to records blockchains may reduce the operational impact of SOX minimizing the cost associated with SOX adoption. SOX, therefore, aligns with the fundamental principle of blockchain operation offering greater transparency and automated auditing of distributed immutable

records. Information can be made available to the relevant stake holders and create more business opportunities while complying with SOX legislation. As the block technology becomes more mature accounting departments will need the human resources to manage and interact with blockchain-enabled applications to fulfil SOX requirements. The vulnerabilities inherent in blockchain architecture at present may affect the operational SOX mandate. For example, vulnerabilities arising due to inappropriate credential management can result in executive signing off on flawed reports. Information consistency between off-chain oracles used to validate records would still be prone to errors originating externally (via oracles) either intentionally or un-intentionally. Errors in financial reporting once posted due to immutability cannot be deleted or revoked. The same is true for sensitive information that should be outside the public domain and once added to a transaction cannot be removed.

- **Section 404 – IT Security Controls:** While a prominent aspect of the SOX audit is financials, the act also provides guidelines on the IT security controls and respective assessment of IT infrastructure. Evaluation of internal controls includes computer systems, networking devices and any electronic components involved in data transmission. Blockchain applications if incorporated in the organizations'

financials, may therefore, be the subject to the same scrutiny. A typical IT audit will review the following controls.

i. Access Control: Access control encompasses the cyber and physical controls preventing unauthorized access to sensitive financial information. In conventional systems access controls require keeping servers in secure data-centers, effective password management, and providing least privilege (POLP). Inclusion of blockchain technology requires the distribution of information across a decentralised peer to peer infrastructure, which if public means records being in the public domain. Private chains can be used to limit access as well as strong encryption and hashing to allow information to be recorded on public crypto ledger, however, only be accessible to users with the respective credentials. Unmanaged passwords, weak storage of private keys, inadequate encryption, plain-text transmissions over the Internet may lead to quick compromise of information and result in organization facing SOX penalties.

ii. Security Policy: Broader IT security policy entails the placement of controls across the organization mitigating breaches and recovering from security incidents. Traditional access control, network firewalling, database redundancy is recommended however, the distributed nature of blockchain crypto ledger, time complexity concerns and software coding updates may lead to issues such as temporary forking

creating multiple copies of contradicting records. Hard forking to correct consistency problems can result in permanent split of records. Regardless, of the type of forking, rolling back and erasing information is not possible due to transaction immutability. Security policy, therefore, can benefit from carefully selecting information, validation sources and consensus protocol to deter incorrect information propagation and compliance with SOX.

iii. Change management: Change management involves updating IT process and systems to allow additional users, update devices, workstations, and the configuration items in an IT assets database. SOX requires record keeping of such events, making it easier for auditor and internal IT administrators to keep track of all changes and resolve (any) problems. The blockchain infrastructure can be used to hold vital IT asset information. While facilitating the financial and IT record-keeping, blockchain itself would also be subject to change management policies. Adding and removal of users to the blockchain application, generation of passwords, key encryption mechanisms and updates to hashing algorithms as well as consensus protocols would all be subject to change management policies adhering to SOX requirements.

iv. Backup and Redundancy: The security policy should also entail adequate backup and redundancy to protect sensitive data, and data-centers or third-party sites

holding data are subject to the same SOX compliance directives. Using blockchain offers data redundancy and back up by default, less temporary and hard forks where contradicting information streams may exist. Additionally, all nodes participating in the blockchain peer network should comply with the security policy. While centralised governance of distributed blockchain peers is not practical in public blockchains, version control and compliance can be relatively better managed in private and hybrid blockchain models.

The fundamentals to consider while complying with SOX Act in the IT domain is to understand and determine an acceptable blockchain operation. The framework can be further evaluated under complimentary auditing standards such as COBIT and ITGI or a combination of the same. Creating, modifying and maintain accounts on the blockchain and handling of information should be guarded to offer greater consistency and erroneous data inclusion. Prior testing of proposed policies in a controlled blockchain environment, monitoring, logging may help auditors as well as the organization in achieving greater reliance on automated blockchain record management and SOX compliance. Despite some of the present shortcomings in blockchain applications, the often-costly maintenance and creation of extensive internal auditory

controls and financial reporting associated with SOX can be significantly decreased using blockchain based auditing systems.

4.1.2 Control Objectives for Information Technology (COBIT)

The control objectives for information technology (COBIT) is management framework for IT systems developed by the Information Systems Audit and Control Association (ISACA) to assist organizations in creating and implementing accurate governance policies.

COBIT started in 1996 and over the decades has seen application in finance and auditing community to better understand and control organizational IT ecosystem. Several versions have been released over the years with the latest being COBIT 2019. The latest versions according to ISACA, is designed to deal with frequent update requirements to IT. COBIT provides strategies that provide a for a highly flexible, and detailed framework to deal with changing technology requirements. COBIT also sets other industry standards defining high level internal controls and assurance such as COSO (Committee of Sponsoring Organizations) into action. COBIT and ISACA directives have focused on the emerging trends and security needs with particular emphasis on emerging incorporation of blockchain in the financial technology sector.

Additionally, the framework also integrates with complimentary IT management frameworks (e.g., ITIL). In relation to blockchain technology, COBIT focuses on the following considerations.

i. IT Controls: Helps management to assess the controls placed around blockchain controls are sufficient and operationally adequate.

ii. Risk Management: Identification of blockchain based risks that may impact the organization and stakeholders financially as well as cause reputational damage.

iii. Governance: Providing and overall governance perspective on the use of blockchain technology according to technical and non-technical considerations.

ISACA provides a holistic approach to the incorporation of blockchain technology, advising on six auditing aspects that need to be considered throughout the operational lifecycle of blockchain applications.

1. Pre-implementation Preparations: Prior to implementation, considerations regarding the type of data, the acquisition and storage need to be made. Blockchain is usually used to track quantities (of digital assets, balance, etc), however, the real-time or value fluctuation of the asset is not maintained in the chain. The valuation of the data held inside the blockchain is therefore, of concern especially when the

determination is not possible due to inaccessible market data or significant value variations in the same.

2. Governance Primitives: The existence of digital assets for governance primitives is usually possible by extracting asset information from the blockchain. While blockchain by default is resistant to record tampering and transactions, it does not mean that the information (data) is fully accurate. The authenticity of data is reliant upon the technology controls in place, the external oracle(s) and the choice of blockchain (e.g., bespoke in-house, public, private, consortium, outsourced, etc.). Auditing of the blockchain system is additionally required to test the sufficiency of controls, thereby, validating the provenance of accurate data.

3. Development Lifecycle: While there are no written agreements in place to dictate the association of assets with internal and external obligations, procedures including digital signatures, private key integrity, and authentication rights need to be included during the blockchain application development cycle. Furthermore, additional procedures may be required, specifically controls implemented during software development to ensure that credentials are managed according to business policies and can be continuously tested to ascertain their operational effectiveness. Coding bugs (if any) should be identified through formal software development checks.

Table 2 Standards and Legislation

Blockchain Feature	Compatibility	SOX	COBIT	ISO/IEC 27001
Financial Accuracy		f	p	p
Off-chain Handling		f	n	n
Record Updating		f	x	x
Executive privilege		f	f	f
Access Control		f	f	f
Security Policy		f	f	f
Change Management		f	p	n
Backup and redundancy		p	f	f
Pre-implementation preparation		n	f	p
Development Life-cycle		n	f	f
Consensus Protocols		n	f	f
Personnel Security		n	f	f
Asset Management		f	f	f
Environment		n	p	f
Incident Management		n	p	f

Compatibility Key:- Full: f, Partial: p, Non-existent: n, Contradictory: x

4. Security Controls: Security around blockchain technology is paramount to reduce unwanted financial consequences. Access to private keys, storage, use of escrows need to be considered. Keys can even be split across multiple parties to ensure approval of transactions is subject to multi-signature. The use of traditional security control models (Bell-Lapadula, Biba, Clark-Wilson, etc.), can be implemented to address unwarranted collusion and conflict of interest. Similarly, for smart contracts, the design and code of contracts can be validated to check appropriateness and effectiveness. The input to contracts can also be monitored to ensure that these are working, and any anomalies are highlighted to the relevant users.

5. Transactions and Management: Information stored and retrieved from the blockchain may not guarantee the any assertions. The reliability of information stored in the transactions is fundamental to the success of blockchain implementations. Although, blockchain ensures privacy by anonymizing individual users through public addresses, the pseudo-anonymized transactions however, allow miscreants to create flawed and fictitious transactions that have no real value. Inflation of assets, revenues, and misappropriation of facts can lead to execution of contracts that are unwarranted. Therefore, it is necessary to ensure the legitimacy of transactions and this requires further preparation of policies and logic from organizations.

6. Consensus Protocols: Organizations implementing blockchain and entirely removing any other type of transactional record need to understand that the completeness of information stored is reliant on the reliability of stored information. As witnessed, in earlier concerns, appropriate and controlled and information input to blockchain transactions ensure that complete and accurate information is captured. Controls requiring consensus should, therefore, ensure that all on-chain and off-chain activity is available and recorded for auditing. Furthermore, the records should be time-stamped and written to the blockchain to monitor the consensus operation, the respective time constraints, and matching of any off-chain data against

the recorded transactions. Although, the above list is non-exhaustive, COBIT framework nonetheless allows a relatively more comprehensive plan for the adoption of blockchain technology. Guidelines are provided for organizations wanting to implement blockchain in a holistic or phased replacement for exiting record-management and auditing. COBIT also complements legislative requirements including the SOX Act and wider service assurance control frameworks such as COSO, by providing low-level detailed implementational guidelines that to a certain extent fulfil the necessities of these relatively high-level abstract standards.

4.1.3 ISO/IEC 27001

ISO 27001 is an international standard for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System. The ISO 27001 is a well-known standard in the ISO 27000 series that providing the fundamentals for an information security management system (ISMS). The ISO 27000 standard is a joint concern of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), therefore, ISO 27001 is also sometimes referred by IEC 27001.

The standard stared in 1995 and defines the fundamentals of establishment, implementation, maintenance, and continuous improvement an information security management framework. ISO 27001 solely focuses on IT or IS security and is applicable to all organizations of any size. The implementation and assessment results in organizational certification. The latest version of the standard came in 2013 (ISO 27001:2013). Organizations that follow the ISO/IEC 27001 recommendations can achieve certification, assuring stakeholders and clients that reasonable IT controls have been put in place around their information.

As discussed in earlier text, the blockchain implementation would still seek the IT controls within an organization and ISO 27001 being an information and data security standard will, therefore, continue to apply. Companies wanting ISO 27001 on their blockchain-enabled infrastructure would require fulfilment of the rules laid out by the standard. The key aspects of the standard applicable in the scope of blockchain technology are listed and discussed as follows.

1. Information and Security Policy: Access to data, as realized in SOX and COBIT will need to be categorized and stored as according to prevailing sensitivity requirements. Data retention requirement of ISO 27001 and destruction will require

re-visiting as the deletion of data on blockchain due to immutability will be of concern.

2. Personnel Security: Access to the blockchain application should be on role requirements within each business unit as well as externally. Expiration of contracts with third-parties, employee role changes and termination would require the relevant access privileges to be revoked or adjusted.

3. Asset Management: Controls introduced to account the ownership of assets, the respective platforms and guidance around storage of hardware and software keys, software certificates and their value requires categorization and auditing.

4. Access Management: Controls around the access to blockchain, the restrictions in place and the procedures that are following in relation to the creation, reading, updating, consensus-approvals as well as the procedures needed de-activate off-chain data would be defined.

5. Environment: Environment refers to the security of the hardware or physical equipment forming the basis of the IT infrastructure – the blockchain nodes, the hardware modules, off-chain storage mechanisms. The monitoring of the environment

using CCTV security, physical access controls and the alarm generation mechanisms in the physical space need to be considered.

6. Operations Security and Incident Management: Operations security in the case of blockchain may deal with the maintenance and automated checking of software updates to off-chain data storage, oracle(s). Prevalent security vulnerabilities advertised globally by security auditing firms and their applicability to the blockchain infrastructure will also require due diligence. Any VPNs used for managing distributed ledger nodes (one or more servers) would still be subject to the same security controls that are dictated by ISO 27001 is operational setting. This may also involve strong cryptographic keys, their management, possession, and storage definitions. Finally, a dedicated security operations team with the adequate training in blockchain-enabled infrastructure should be available to deal with security incidents, notifications and troubleshooting with internal and external technical teams.

ISO/IEC 27001 standards fulfilment to achieve the respective certification, allowing companies to advertise the viability of their blockchain ecosystem would require due consideration for several features discussed above.

4.2 Perspectives on Blockchain Transformation

According to the existing legislative and standardization primitives the specific data controls requiring development for future blockchain certification include some of the following.

Inputs and Interactions: Simply including data in the blockchain for the purpose of recording is not enough. Internal and external audit needs to review a number of factors including the type and volume of data to record, the transaction latency and authentication of data. Similarly, the privacy and extent of anonymization of data, the legislative requirements with regards to traceability of information should be realized in blockchain applications. Controls and definitions of blockchain interaction with off-chain business entities need to be incorporated in respective standards. Additionally, the scope of consensus algorithms and their validity of use as per the underlying principles of the respective business also need appraisal and inclusion in the legislative and standardization primitives.

Storage and Retrieval: Inevitably the amount of data stored in a blockchain can vary depending on the technology being used. Therefore, the variable requirements require appropriate controls. Whether complimentary technologies such as on-site or

off-site cloud storage, encrypted file systems and dedicated filers are employed, these should be subject to the same controls as traditional IT infrastructure and to a certain degree have already been defined in the standards discussed earlier. Nevertheless, the risks around storage need to be eliminated and for this purpose the certification requirements and auditory compliance checks need to be further elaborated. One further concern, is for data specifically stored on cloud-based systems, the applicability and recognition of regulatory framework across national and geographic boundaries to aid in legal and regulatory investigations as needed.

Access Controls: Access controls although have been defined in all legislative primitives, are still a critical privacy and integrity concern for organizations. The degree and importance of these concerns vary with the type of blockchain to be used, e.g. private, public, permissioned, etc. and the limits of administration to allow or limit access. Credential management and the means to secure the integrity of transactions, the relevant private and public keys, respective storage mechanism should be subject to adequate access control. Formal definition of roles of users, business units and external parties need to be defined using standard access control models and incorporated specifically in relevant regulatory frameworks according to blockchain requirements.

While legislation such as SOX Act are comprehensive in abstracting the auditory and control requirements to be implemented in a wide-range of scenarios, the applicability of the act in regions outside the U.S. or suitable derivates needs further exploration. Similarly, the lower-level frameworks that seek to simplify the relevant IT controls need re-defining on issues such as data deletion and the weightage of public-private information in blockchain recorded data to satisfy legal requirements. Overall, the relevant legislation and certification standards provide a suitable starting point for phased implementation of blockchain, requiring updates as dictated by real-world scenarios and availability of wider variety of use-cases.

5 Conclusion

The inception and development in blockchain technology over the past few years have increased its realm beyond cryptocurrencies to financial auditing services. Proponents of the technology believe that it might remove the requirement for manually intensive financial audits and automate the accounting process to the extent that real-time validation on all transactions can be performed. The underlying concerns that have arisen due to inherent blockchain vulnerabilities and the scope of their implications in the auditing world have raised concerns about the technological, as

well as legislative, regulatory compliance and certification checks that the technology needs to undergo prior to widespread adoption in fintech services. Blockchain technology by itself promises the elimination of redundancy and duplication of efforts in the auditing and regulatory realms. However, since the technology is not completely innate in addressing software issues, security concerns and miscreant abuse, a complimentary approach is encouraged where auditory and accounting teams utilise blockchains and wider the scope of their operational capability is quite likely. While employing blockchain applications, auditory frameworks will also need to develop the policies and processes to validate all blockchain related platform functionalities. Existing legislative and IT control standardization frameworks such as SOX Act cater to the needs of blockchain applications to significant level. Further work in improving abstract directives and guidelines laid out in similar certifications (e.g. CORBIT, ISO/IEC 27001, etc.) is nonetheless needed to expand and embrace blockchain in auditing and compliance and add value to businesses.

References

1. CPA Canada, AICPA. Blockchain technology and its potential impact on the audit and assurance profession. Deloitte Development LLC. (2017)

http://https://www.cpacanada.ca/en/ Cited 10 Oct 2020

2. Mahbod, R., and Hinton, C. D. : Blockchain: The future of the auditing and assurance profession. Armed Forces Comptroller. **64(1)**, 23-–27. (2019)
3. Ortman, J. C.: Blockchain and the future of the audit., CMC Senior Theses. 1987. Claremont (2018)
4. Sadu, I. Auditing blockchain. Internal Auditor, 75(6), pp. 17-19. (2018)
5. K Salah, MHU Rehman, N Nizamuddin, A Al-Fuqaha. Blockchain for AI: Review and open research challenges. IEEE Access, 2019/1/1(7), pp. 10127-10149. (2019)
6. Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu.A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 53, 3, Article 67, 43 pages. (2020)
7. Smith, S. Blockchain augmented audit – Benefits and challenges for accounting professionals. . Journal of Theoretical Accounting Research, 14(1), pp. 117–137. (2018)
8. Turker I., Bicer A.A. How to Use Blockchain Effectively in Auditing and Assurance Services. In: Hacioglu U. (eds) Digital Business Strategies in Blockchain Ecosystems. Contributions to Management Science. Springer, Cham. (2020)
9. Behl, Ramesh; O'Brien, James A.; Marakas, George M. (2019) Management Information Systems. McGraw-Hill Education. ISBN 978-93-5316-466-9.
10. Haes, S.D.; Grembergen, W.V. Chapter 5: COBIT as a Framework for Enterprise Governance of IT. Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.). Springer. pp. 103–128. ISBN 9783319145471. (2015)

11. COBIT 2019 Framework: Introduction and Methodology from ISACA. (2019)

https://www.isaca.org/resources/cobit Cited 29 Sep 2020

12. ISO/IEC 27001:2013. Iternational Standards Organization (2013)

https://www.iso.org/standard/54534.html Cited 6 Oct 2020