IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 8, 2021, accepted October 10, 2021, date of publication October 25, 2021, date of current version November 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3122518

An Architecture to Facilitate Security Assurance and Legal Compliance for Call Auditing in the Wholesale Electricity Market

AKLILU DANIEL TESFAMICAEL, VICKY LIU, MATTHEW MCKAGUE, AND WILLIAM CAELLI
School of Computer Science, Queensland University of Technology, Brisbane, QLD 4000, Australia
Corresponding author: Aklilu Daniel Tesfamicael (aki.tesfamicael@hdr.qut.edu.au)

ABSTRACT The auditability of telephone call records plays an essential governance role in the electricity industry in Australia as non-compliance with the Australian National Electricity Rules can lead to financial charges and result in developing a poor reputation. The existing telephone call recording processes using manual logbook entries or a recording system without verification and auditing capabilities are labour-intensive and prone to human error. This study is motivated to address this real-world problem by designing a system that streamlines telephone call audit processes. This can be verified with digital technologies to meet security requirements as well as legal requirements stipulated by the Australian National Electricity Rules. In meeting security and legal compliance requirements of the Australian National Electricity Rules, this study develops a novel approach using the Clark-Wilson Integrity Model and blockchain technology for an automatic telephone call audit system with security provisions to prevent unauthorized access to and manipulation of telephone call records nationally. Although the application of blockchain has generated great interest in other areas, few studies have been conducted on its application to auditing. This study uses the Clark-Wilson Integrity Model to verify metadata records' integrity at the systems where metadata are generated. The proposed architectural design not only enhances data integrity and confidentiality but also enables the automatic execution of telephone call audit processes for auditors. The auditing system we propose presents a higher level of security compared to the existing system.

INDEX TERMS Audit, blockchain, compliance, security.

I. INTRODUCTION

In Australia, under the National Electricity Rules, generators and energy market operators trading in energy markets must record each telephone conversation as soon as possible after making or receiving all communications in the form of a manual logbook entry or by another auditable method which will provide a permanent record [1]. A digital Call Recording system may be used as an alternative to manual logbook entry. Australian National Electricity Rules govern the operation of the National Electricity Market [1]. The Rules have the force of law and are made under the National Electricity Law.

The current telephone call recording information is provided to auditors in a variety of electronic and paper-based formats that require auditors to invest significant time when conducting telephone call recording auditing. This is a legal compliance requirement for electricity generators when they trade electricity in the national wholesale electricity market.

The Australian Energy Market Operator (AEMO) is responsible for monitoring generators for compliance and enforcement under legislation governing Australia's wholesale energy markets. Generators are therefore motivated to comply with the National Electricity Rules. As such, both hire auditors to operate continuous auditing models and perform audit data analyses.

Energy market traders experience high volumes of telephone calls during the trading period. The traditional process for delivering paper confirmation is inefficient, time-consuming and prone to human error, relying on manual processes and other insecure telephone call recording technologies. This also makes the process vulnerable to activities that, intentionally or unintentionally, may breach the confidentiality or integrity of recorded market-related telephone conversations. Ultimately, this may lead to non-compliance

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Shen.

with the National Electricity Rules. To address this problem, we propose an automated mechanism to enhance overall trust and security so that authorized users are unable to manipulate metadata arbitrarily and only in an appropriate manner that preserves the integrity of the telephone call metadata and recordings. At the same time, the audit procedures are automated to meet compliance requirements. By making telephone call recordings verifiable and auditable using digital technologies, telephone call audits can be streamlined to meet legal requirements stipulated by the Australian National Electricity Rules.

A breach of telephone conversation data confidentiality and integrity in the electricity industry could have national security implications. Financial charges and a poor reputation are potential consequences of regulatory non-compliance. This study is motivated to address this real-world problem by designing a system that streamlines telephone call audit processes. This can be verified with digital technologies to meet security requirements as well as legal requirements stipulated by the Australian National Electricity Rules.

This research defines higher benchmarking for security and business requirements than the legal requirements stipulated by the Australian National Energy Rules.

A. SCOPE OF RESEARCH PROJECT

This research focuses on the automation of the auditing of telephone call recordings with security provisions to prevent authorized/unauthorized data manipulation. This project assumes that the Telephone Exchange and Call Recording (TECR) systems are already in place. From this section onward, the term ''TECR systems'' refers to the Telephone Exchange and Call Recording systems. It also assumes that all trading telephones used for energy trading purposes include an authentication function to identify the operator. Only authenticated and authorized entities are allowed to access them.

This research focuses on the provision of integrity and authenticity for the design of auditing systems in terms of recognition of:

- the role that reliable data input from authorized users plays as a pivotal role to prevent garbage in, garbage out (GIGO) issues.
- the fact that separation of duties is critical to effective internal control as it reduces the risk of erroneous and inappropriate action.
- the need for provision of a metadata reconciliation to eliminate data discrepancy
- a requirement for audit automation so that auditors and the regulator can be more confident in the data given to them by the generators.

To achieve the required result, we use the blockchain Hyperledger Fabric framework with digital certificates to manage user roles and permissions in the system. The blockchain is used to ensure that the telephone call metadata and telephone call records are not deleted or altered without detection. The automation of the audit process, confidentiality and integrity are achieved through this method. We designed the system according to a Clark-Wilson Integrity Model to ensure that best practices are followed to protect the integrity of the metadata generation to enhance overall trust and security in the National Electricity Market.

The proposed system treats any telephone call made by authorized users as a telephone call record (transaction). Each time a telephone call is made, it is automatically recorded. The metadata and hash of the telephone call recordings are stored in the blockchain. The actual telephone call recordings are stored in a separate data store for efficiency. In the blockchain, the metadata transaction consists of the telephone call recordings information and the hash which is used to verify its integrity.

B. RESEARCH QUESTIONS AND CONTRIBUTION

The research questions investigated and reported upon in this paper are as follows:

1) How do we design an auditing system to meet legal compliance by ensuring the integrity and authenticity of the auditing metadata and telephone recordings that are verifiable using digital technologies?
2) How do we ensure the source data input to the proposed system is reliable to prevent GIGO issues?
3) Can we provision additional security capabilities to prevent authorized and unauthorized users from inappropriately manipulating data?

The contribution made by this paper is based upon proposals for:

1) Blockchain-based structure as a technologically verifiable mechanism for the telephone call auditing system. Using a blockchain allows the regulator and generator to agree on an auditable log without burdening the regulator with data storage or denying generators ownership of their own data.
2) Use of the Clark-Wilson Integrity Model to prevent authorized and unauthorized users from inappropriately manipulating data.
3) Blockchain and Clark-Wilson Integrity Model adaptation to enhance overall trust and security in a real-world business case capable of making an impact.

The anticipated outcomes of this proposed project include:

1) From the perspective of generators, they can meet legal compliance requirements so that the regulator does not apply penalties to them.
2) From the regulator and auditor's perspective, they can validate data submitted by generators using the proposed system.
3) Generators can benefit from streamlining the telephone call audit procedure by automating the manual process.

The target audience for this research includes academic researchers in the area as well as electricity generation enterprises and regulatory bodies.

C. PAPER STRUCTURE

The remaining sections of the paper are organized as follows. Section II presents the security and legal compliance requirements of telephone call recording, whilst Section III discusses relevant background matters, including related work, an overview of current call recording methods and proposed system components. Section IV looks at the proposed system design and architecture, followed by Section V, which discusses system design analysis. A conclusion and future work are outlined in Section VI.

II. SECURITY AND LEGAL COMPLIANCE REQUIREMENTS

Under the National Electricity Rules [1], each generator must record all telephone conversations related to power trading with timestamping, and the records should be stored for data retention obligations. The legal requirements listed from LC1 to LC4 can be easily achieved. The key legal compliance (LC) rules are summarized as follows:

- LC1 (telephone call must be recorded) - all telephone conversations must be recorded in the form of manual logbook entries or by a system capable of recording actual telephone calls.
- LC2 (telephone call recording information) - all recordings must include the date, time and content of each conversation.
- LC3 (audit report) - audit reports of telephone conversation records must be available on request for auditing purposes.
- LC4 (data retention) – retention of all telephone conversation records for a minimum of seven years.

This research sets security (SR1-SR3) and business (BR1 and BR2) benchmarking higher than the legal requirements (LC1 – LC4). We define the following key security requirements (SR) and business requirements (BR) that must be satisfied to achieve compliance and desirable levels of integrity and confidentiality for the interest of generators. It is advantageous to have availability and visibility of the auditing of telephone call recordings for the regulator.

- SR1 (integrity) - records of telephone conversations must not be tampered with while telephone call records are being recorded and stored in the system. This should be achieved by preventing users from arbitrarily manipulating data to preserve data integrity (reliable data from the authorized user), separation of duties to prevent fraud by one person acting alone and the provision of a metadata reconciliation method to flag for any data discrepancy
- SR2 (authentication and authorization) - systems used to record and store telephone conversations must only limit communications to authorized participants.
- SR3 (confidentiality) - all records of telephone conversations must be protected from unauthorized access.
- BR1 (call audit automation and availability) - audit processes need to be automated to provide constant availability and visibility of the auditing of telephone call recordings for the regulator.
- BR2 (ownership) – each generator must maintain control of its telephone call recordings.

There are two ways to buy and sell electricity in the national wholesale electricity market (NEM): through the spot market and the contract market. In the physical (spot) trading market, traders sell electricity on a day-to-day short-term basis as part of a process regulated by the Australia Energy Market Operator (AEMO). Whereas in the contract trading market, traders supply or procure electricity on a longer-term basis at a more stable price and to secure certain levels of energy volumes. The National Electricity Rules apply to physical trading as they participate in the national wholesale electricity market regulated by AEMO.

III. BACKGROUND

This section discusses related work, the current telephone call recording system and system components required to design the proposed system.

A. RELATED WORK

This section discusses previous work using blockchain for auditing purposes, particularly in the accounting, auditing and telecommunications fields. The scope of this review is limited to the use of decentralized blockchains to address issues of auditing and security, particularly in meeting legal compliance and security requirements.

At a high level, a blockchain is an append-only ledger such that contents can be added but not removed or changed. Further, the order of entries is preserved.

There are two types of blockchain: public and private blockchains. A public blockchain is permissionless, whereby anyone can participate (i.e. add new entries to the ledger). However, a private blockchain is permissioned where only permitted blockchain participants can participate [2].

Numerous existing studies [3]–[28] have explored blockchain applications in various areas, particularly in finance and accounting. However, most of these studies are in the early concept stage and require more work to advance to the execution phase. Practical implementation in a real-world scenario is also lacking.

Numerous existing studies [29], [30] claim that blockchain brings an opportunity to assist accounting by providing an alternative to auditing and accounting services. However, ''blockchain modes'' in normal applications of cryptography have long been used. What has become clear is that auditing should be performed in a more efficient and effective way by reducing time spent on manual audit activities. Using blockchain with smart contracting enables the elimination of a third party in the auditing tasks and can improve efficiency by reducing manual errors [7] and [31].

The opportunities and challenges of blockchain and smart contracts for accounting and auditing are still under investigation in academia. Numerous studies [21], [30] and [33] discuss the use of blockchain in accounting, focusing on how this technology could enable verifiable and transparent accounting practices. However, our research focus is from security and audit quality perspectives.

Consulting entities Deloitte and KPMG also conduct some existing commercial implementation. Deloitte developed a blockchain platform named "Rubix". It was developed to target four main applications, financial reconciliation, audits, land registry and loyalty points [34]. In 2017, Deloitte claimed that it had successfully performed a blockchain-based auditing application. KPMG, in partnership with Microsoft, created their blockchain platform addressing the implementation challenges in the financial, healthcare and public sectors [35].

There is a lack of studies that examine the security and auditing aspects in telephone call auditing, especially on the application of blockchain for the auditing of telephone call recordings. A related work proposed by Kozloski *et al.* [36] implemented an event tracking method using a blockchain application. This is for a device to detect an event and transmit transactions to the blockchain network. Using this method, they can track and maintain records of telecommunication device events using a blockchain application. This work demonstrated the use of blockchain in the telecommunications area for tracking data generated by a particular mobile device. Our research is different from Kozloski *et al.* [36]. We apply blockchain and the Clark-Wilson Integrity Model as an integrated solution to provide overall security and trust to meet security and legal compliance requirements for the National Electricity Rules. The data security provisions in our proposed system are applied in the systems where data are generated and once those data are transmitted to the blockchain-based auditing system.

Numerous industry-based projects adopt blockchain models to facilitate some level of legal compliance requirements and audit activities. This study focuses on designing and developing a framework for automating telephone call recording audit systems to meet legal and security requirements.

B. CURRENT TELEPHONE CALL RECORDING SYSTEMS AND LIMITATIONS

Organizations record telephone call conversations for various reasons, including for the purposes of legal compliance, training, customer service experience and/or to prevent potential disputes. Each jurisdiction has its own legislation to allow the recording of telephone call conversations.

AEMO and generators must comply with legal compliance requirements for telephone call conversation records as described in Section II.

With the current telephone call conversation recording system in the Australian energy industry, there is a lack of use of technology-based solutions to monitor and audit records of telephone call conversations in a secure manner. When a caller makes or receives a telephone call, details of the telephone call conversation are recorded manually, which is a time-consuming and error-prone process. The other method uses a recording system that does not provide confidentiality and integrity for the telephone call recording data. There is a need to have an auditing system to enable telephone call auditing in an effective, efficient and secure way. The existing telephone call recordings are also not stored securely. Although the confidentiality of telephone call recordings is not required, this research defines such security requirements for confidentiality and integrity. Telephone call recording data at rest and in transit must be protected to provide confidentiality and integrity.

Fig. 1 illustrates the overall process used by the current Telephone Call Recording system. For example, anyone can make and receive a telephone call without any authentication (1). Once a telephone call is placed, a telephone call is established in the Telephone Exchange system (3). Meanwhile, the telephone call is logged in the recording system (2a). For those who use a manual log book method, telephone call information is logged in a manual logbook entry (2b). An auditor conducts auditing either by reviewing telephone call recordings from the system (4a) or the manual logbook entries (4b).

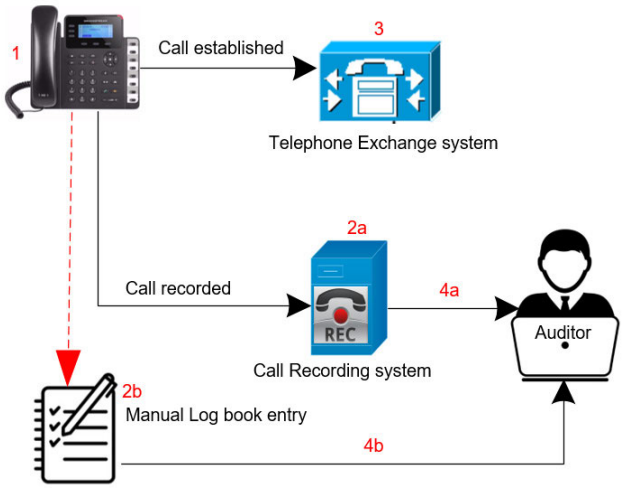


FIGURE 1. Current telephone call recording system.

Based on a review of the current Telephone Call Recording system, there are three limitations identified;

Case 1: If AEMO requests telephone call records from the generator, then the generator presents the telephone call records without integrity assurance. The presented telephone call recordings may be manipulated inappropriately by the generator.

Case 2: If the generator is required to send all telephone call recordings to AEMO, then the generator has no control over the confidentiality of the telephone call recordings. AEMO also will be overwhelmed with the submitted telephone call recordings. The generator is also not assured that AEMO does not alter the submitted telephone call recordings.

Case 3: If the telephone call recordings are manipulated by a disgruntled generator employee, then the telephone call recordings presented to AEMO are compromised.

Case 4: If the Telephone Call Recording system fails to record without notice, this will result in financial penalties for the generator.

The proposed system uses the Clark-Wilson Integrity Model and a blockchain mechanism to address the limitations of the existing telephone call recordings scheme as listed in Cases 1-4. This allows generators and AEMO to trust telephone call recordings with the assurance of both integrity and confidentiality.

C. SYSTEM COMPONENTS

This section details the components required in our proposed system (described in Section IV).

1) BLOCKCHAIN

Blockchain is a decentralized, shared and immutable ledger for recording transactions in a verifiable way. Blockchain can be divided into three types: public blockchain, private blockchain, and consortium blockchain [39], [40]. Public and private blockchains differ in many ways that can affect the level of security they provide. The main difference is that anyone can join the blockchain network in the public blockchain at any time, whereas the private blockchain is based on preselected membership. In a private permissioned blockchain, only authorized users can add entries into the blockchain system. Trusted parties are preselected to allow access to the system. A consensus mechanism must verify any transaction input to the system. In the case of a consortium blockchain, it is controlled by a group of members. It has a pre-defined set of nodes. Users may have read and/or write access.

We use the Hyperledger Fabric framework [33], which is a type of consortium blockchain. Hyperledger Fabric blockchain consists of a network of nodes and peers. Nodes store blockchain data while peers hold copies of ledgers.

The Hyperledger Fabric components include member services, certificate authority, nodes and peers.

1) Membership services: provide identification and authentication to the system with digital certification.
2) Hyperledger Fabric Certification Authority (CA) issues or revokes digital certificates for participants of the blockchain system. A digital certificate is a mechanism for binding public keys to an owner. The Hyperledger Fabric CA validates the identity and public key of the owner. A digital certificate is signed by the private key of the Hyperledger Fabric CA to attest authenticity.
3) Nodes. Not all nodes in a consortium blockchain are equal. In Hyperledger Fabric, there are different nodes: client node, peer node (endorsing and committing peer), and ordering node.
    a) Client Nodes submit an actual transaction invocation to the endorsers and broadcasts transaction proposals to the ordering service.
    b) Endorsing peers endorse/provide the approval to a transaction when the client node proposes it.
    c) Committing peer validates/commits a transaction after endorsement from the endorsing peer.
    d) Ordering Node places the transactions from multiple peers in order and then sends them to each peer as a block to get updated in the ledger.

In the Hyperledger Fabric blockchain, each node maintains a copy of the ledger by applying transactions that have been validated with the consensus protocol. A client sends a transaction proposal to endorsers in order to submit a transaction. All endorsers have to reach a consensus upon the proposed transaction. If the transaction is approved, it is sent to ordering nodes that reach a consensus to arrange submitted transactions and package them into blocks. Subsequently, the transaction is forwarded to committing peers for transaction validation.

2) CONSENSUS MECHANISMS

A consensus algorithm is a process used in the blockchain system to achieve agreement on a single data value. The Practical Byzantine Fault Tolerant (PBFT) consensus algorithm is one of the most popular consensus algorithms used in the permissioned blockchain. It is efficient [41]. With PBFT, each blockchain node needs to be authenticated and authorized to participate in the consensus process of the blockchain. Consensus in the PBFT can be reached when malicious nodes are less than one-third of the total number of nodes [41].

The security properties supported by the permissioned-based blockchain include:

1) Data authentication: Participants in the blockchain network have their own two keys that are assigned to them. Transaction proposals are digitally signed using an owner's private key, which also includes a public key in the transaction payload sent to peers and orderers. Peers and orderers then verify the signature using the owner's public key.
2) Hash chained data storage: The hash is for the previous block so that all data in all blocks are connected together in a chain from the initial block to the most recent block. Any attempt to delete or change a block will break the chain of hashes and be detectable.
3) Consensus: The consensus mechanism ensures that all the nodes agree on what transactions are on the chain and the order of transactions. Transactions recorded on the blockchain are immutable because they cannot be deleted or changed.
4) Authorization: Only authorized parties are allowed to submit and/or access transactions in the blockchain system. If data are sent from an unauthorized user, the signature of that user will not be matched, and data do not appear on the chain.

D. CLARK-WILSON INTEGRITY MODEL

Several information security models have been developed to enforce security policies, including the Bell-LaPadula, Biba, Brewer and Nash, and Clark-Wilson Integrity models [37]. Bell-LaPadula model addressed data confidentiality and controlled access to classified information. The Biba model focuses on integrity to prevent information flow from low-level to high-level security. Both Bell-LaPadula and Biba

models are designed for the military and government systems to protect confidentiality and integrity of information. The Brewer and Nash (Chinese Wall) model is an information model to provide controls and mitigate ''conflict of interest'' in commercial organizations. This study uses the Clark-Wilson Integrity Model [38], which is designed for businesses to protect data integrity. This model is suitable for addressing commercial data quality before entering the proposed blockchain system.

The Clark-Wilson Integrity Model classifies data into two sets: Constrained Data Items (CDI) and Unconstrained Data Items (UDI). The CDIs are objects that the integrity model is applied to, and UDIs are objects that are not covered by the integrity policy. An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state. UDIs are objects that are not governed by the integrity policy of the Clark-Wilson Integrity Model, while CDIs are.

This model uses the three-part relationships of subject/program/object, known as a triple, to access objects through programs. This model is encoded as a set of triples:

$$< \text{UserID, TP, \{CDI1, CDI2, \ldots CDIn\}}$$

where,

- UserID: user identification that has permission to execute *tp* on *CDIs*.
- TP: a transformation procedure (such as an approved program).
- CDI: data objects that a TP may reference on behalf of the user.

The Clark-Wilson Integrity Model uses two categories of mechanisms to realize integrity: well-formed transactions and separation of duty.

Well-formed transactions ensure only authorized actions can be executed, which preserve data integrity. They are used to prevent users from arbitrarily manipulating data through a series of operations that transform a system from one valid state to another. These are five certification rules (C1-C5) to enforce the integrity policy.

C1: To ensure all CDIs are in a valid state when any IVP is executed.

C2: To perform and ensure those CDIs are transformed from a valid state into a valid state through TPs.

C3: To enforce the principle of separation of duty.

C4: Audit log in TP operations.

C5: To execute UDIs to CDIs through TPs.

The principle of separation of duty requires more than one person to complete a task in order to prevent fraud by one person acting alone. There are four enforcement rules (E1-E4) to reinforce the separation of duties.

E1: To ensure the CDIs are only changed by certified TP.

E2: To ensure the authorized user accesses particular CDIs through a TP.

E3: To ensure users are authenticated to execute a TP.

E4: To ensure only an authorized security officer can change the list of users associated with that TP.

IV. PROPOSED SYSTEM ARCHITECTURE DESIGN

Section III states the core components of a blockchain system and the Clark-Wilson Integrity Model that are used in our system design. This section outlines the proposed architecture, defines the functionality of the nodes and the members' roles, and describes the process of members identification and authorization and the communication processes.

A. OVERVIEW OF THE PROPOSED DESIGN ARCHITECTURE

This section presents a broad overview on how the proposed system operates. Fig. 2 illustrates how call recordings are created from the generator's end and then transmitted to the blockchain system.

1) An authenticated caller places a telephone call.
2) The telephone call is established via the Telephone Exchange system.
3) The telephone call is logged in the telephone call recording system.
4) The metadata records generated from the TECR systems must be matched for data consistencies before transmitting the metadata records to the blockchain system.
5) Both the TECR systems digitally sign their own metadata transaction proposal independently and send it to the blockchain system.
6) A peer node verifies the identity of the TECR systems and their authorization to submit metadata transactions. Upon successful verification, the peer node endorses the transaction and sends an acknowledgement back to both systems.
7) The TECR systems receive the acknowledgement from the peer node.
8) The TECR systems submit metadata records with the endorsed transaction proposal to peer node.
9) A consensus is reached on the order and confirming the correctness of the set of transactions that constitute a block.
10) If it is a valid metadata transaction, a peer node orders the received metadata transaction and generates a new block.
11) The peer node broadcasts the generated block to the system.
12) The peer node adds the validated metadata transaction to the ledger.
13) Automated audit reports are sent to the regulator, generators and auditors.

Metadata is related information about the actual telephone call conversation recording data. Metadata records are generated from both the TECR systems. If these two records are matched, then the metadata records are ready to transmit to the blockchain system. Otherwise, they are flagged for further investigation on why the metadata records are mismatched. This is to ensure that data consistency and reliability is maintained. This is called a metadata reconciliation process. This process is crucial to the generators to take appropriate action to address the issue of mismatched metadata records

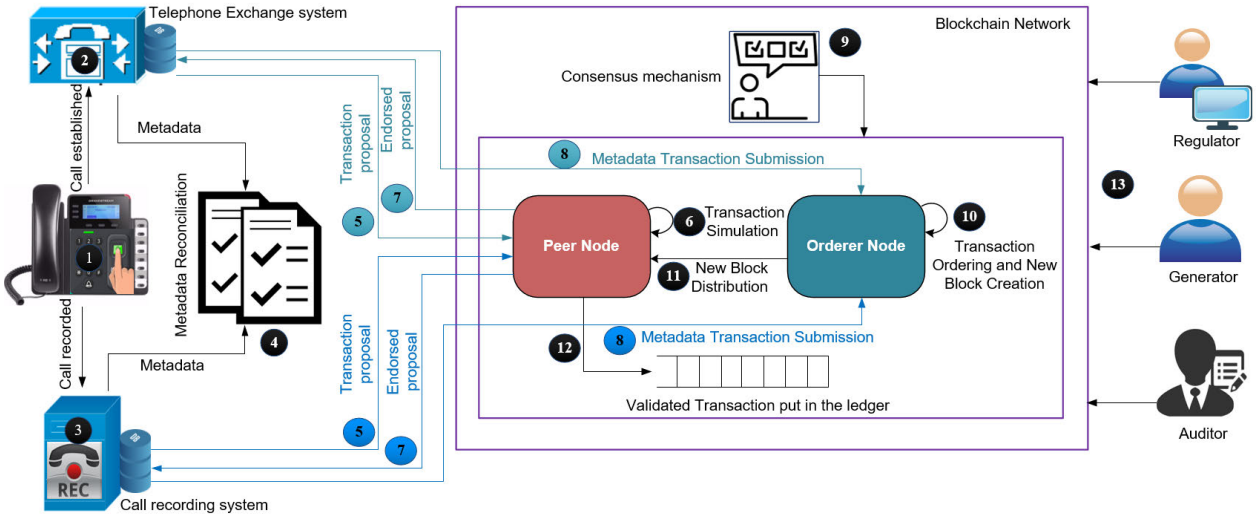


FIGURE 2. Proposed architecture for a secure and automated telephone conversation data auditing.

so that the legal compliance requirement (LC1) is satisfied, as stated in Section II. In the current system, a failure of the Telephone Call Recording system can occur by failing to record a telephone conversation without notice. This has occurred to generators on a number of occasions resulting in financial penalties.

From performance and confidentiality perspectives, the telephone call recordings are not transmitted to the blockchain system. Only metadata records are transmitted. The telephone call recordings remain at the generator's system. From the perspective of integrity, the generator cannot manipulate the telephone call recordings once metadata records are committed to the blockchain system. A hash of the recording is also sent to the blockchain so that the integrity of the recordings can be validated.

The nodes in the proposed blockchain-based auditing system have different roles: peers and orderers nodes. Peers propose a new transaction that is shared and committed to the ledger. When a peer node proposes a transaction and the transaction is committed, the orderer node helps ensure that transactions are ordered correctly, and such ordered transactions are being shared with the rest of the peers.

B. FUNCTIONS OF NODES IN THE PROPOSED BLOCKCHAIN SYSTEM

The proposed blockchain system consists of client, endorse, commit and order nodes. A client node acts on behalf of a generator to send metadata records from the TECR systems to the blockchain system. A peer node endorses and commits metadata transactions submitted by the client node. The order node orders the submitted metadata transactions from the committing node and writes them to the ledger.

The three stages of transaction processing in the proposed system are: proposing a metadata transaction, ordering and packaging metadata transaction(s) into blocks, and validating the transaction(s) and combining with other verified transactions into the ledger. During the stage of proposing a metadata transaction, the client node generates and signs a metadata transaction proposal and sends it to the endorsing node. The endorsing node validates the received signed proposal. At the second stage, the metadata transaction is packaged by the ordering node and is then ready for distribution to the peers. The final stage of the metadata transaction involves the distribution and validation of blocks, where they are committed to the ledger.

C. MEMBER ROLES OF THE PROPOSED SYSTEM

Blockchain network members are the users of the blockchain system. Members of our proposed system are generators, the regulator and auditors. These members have roles and capabilities in the system that allow them to interact with the blockchain system through their peer nodes by creating transactions.

In the proposed system, ''domain'' refers to the entire blockchain system. A domain consists of a number of ''subdomains''. Each generator is assigned to a ''subdomain'' for its call recording auditing system.

The regulator is the owner of the entire blockchain domain. Users, such as generators and auditors, are invited by the regulator to join the blockchain system. As a domain super user, the regulator has full access control permission to the entire ledger set across the blockchain network. Each generator is assigned as a ''subdomain super user'' with full access control over their own ledger in the blockchain system.

A generator can employ an auditor to conduct auditing on the telephone call recordings in order to facilitate meeting legal compliance requirements. A regulator employs an auditor to conduct auditing on all generators call recordings in order to ensure generators meet legal compliance requirements.

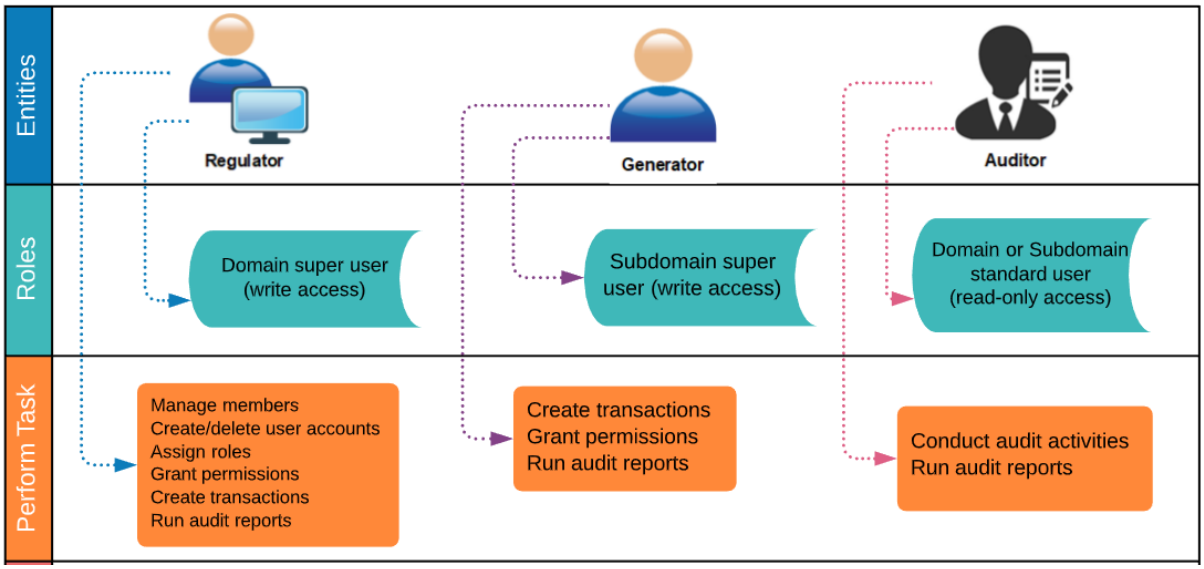


FIGURE 3. Members roles and capabilities of our proposed blockchain network.

There are two types of roles that can be assigned to auditors: ''domain standard user'' or ''subdomain standard user''. Auditors that a regulator hires are assigned a ''domain standard user'' role, which allows them read-only access to all ledgers in the blockchain system. If a generator employs an auditor, they are assigned a ''subdomain standard user'' role, which allows him/her read-only access to the generator's ledger.

The TECR systems are assigned with a ''standard user'' role with read/write access to submit metadata records to the proposed blockchain system.

Each member of the blockchain system, such as generators, auditors, and a regulator have at least one peer node associated with their membership account. Multiple generators cannot own a single peer node, i.e. it is only owned by a single organization and is therefore associated with a single member of the blockchain. The regulator and generators use their peer nodes to agree on the validity state of a metadata transaction to be written to the ledger. Auditors are participants in a blockchain network who do not participate in the consensus.

The roles of the blockchain users and their tasks in the system are shown in Fig. 3 above.

In the proposed system, we adopt a role-based access control mechanism to enable access to metadata transactions in the blockchain system. Access to metadata transactions can be limited to specific tasks such as the ability to submit, view, audit and/or modify metadata transactions. When the TECR systems send metadata records to the blockchain system, they become immediately accessible to the regulator and authorized auditors. The regulator automatically has read access to all metadata records nationally, while each generator only has read access to their own ledger. Table 1 summarizes the role-based access privileges assigned to each type of user in the proposed blockchain system.

D. MEMBERS IDENTITY VERIFICATION AND AUTHORIZATION PROCESS

In our proposed system, each member possesses a key pair, cryptography private and public key. A private key is used for metadata transaction signing and endorsing. The CA attests the associated public key and is made available for anyone to validate signed and endorsed transactions.

Fig. 4 shows a flow diagram of the new member registration and authentication process in the blockchain network.

The regulator as a ''domain super user'' delegates each generator to have read/write access to their own ledger and to manage their own subdomain. Each generator can employ its own auditor to audit their own ledger with read-only access. The regulator can also employ auditors to audit all generators ledgers with read-only access.

E. METADATA COLLECTION, STORAGE AND RETRIEVAL PROCESSES

This section describes how the metadata records are collected and submitted from generators and how metadata records are stored and retrieved for auditing purposes.

1) METADATA GENERATION PROCESS

Metadata generator systems refer to the TECR systems. Fig. 5 illustrates how these systems interact with each other to provide metadata records. Each record contains a number of fields listed in Table 2. Metadata records that are matched are sent to the proposed blockchain system. Metadata records that are not matched are flagged for further investigation to ensure data consistency.

Telephone conversations can also be converted into text-based or XML (Extendable Markup Language) format with data mining technique to abstract to a summary as part of the

TABLE 1. Role-based access privileges in the blockchain system.

Entity	Role	Access to metadata
Regulator	Domain super user	Real-only access to all metadata transactions.
		Read/write access to metadata transactions after consensus has been reached.
		Grant/revoke user permissions on the blockchain domain.
Generator	Subdomain super user	Read/write access to create/submit metadata transactions.
		Read-only access to their own metadata transactions.
		Read/write access to their metadata transaction after consensus has been reached.
		Grant/revoke permissions within its own subdomain.
Auditor	Domain standard user	Authorization is granted by the regulator with real-only access to metadata transactions.
		No read/write access to metadata transactions.
Auditor	Subdomain standard user	Authorization is granted by the generator with read-only access to the generators metadata transactions
		No read/write access to metadata transactions.
Recording system	Standard user	Read/write access to submit metadata transactions.
Telephone Exchange system	Standard user	Read/write access to submit metadata transactions.

metadata records to be sent to the proposed blockchain-based system.

2) METADATA TRANSACTION PROCESS

Each generator has a client node and a peer node on the blockchain system. A peer node refers to the endorser, committer and orderer nodes. A client node proposes a metadata transaction to the endorser node through which they send their metadata transactions and interact with the ledger. Each member of the blockchain system has their own peer nodes to represent them.

As shown in Fig. 6, the TECR systems, through their client nodes, send a transaction proposal to the endorser peer node in the blockchain system (1). An endorser node validates the metadata transaction proposal. Upon successful transaction validation, the endorser peer accepts the transaction proposal and returns a signed proposal to the client node (2). The client node then packages the metadata transaction, including the endorsement record and sends it to the orderer node (3). The orderer node validates the transaction received from the client node and creates a new block. The newly created block then broadcasts to all peer nodes and commits to the ledger as a valid block (4).

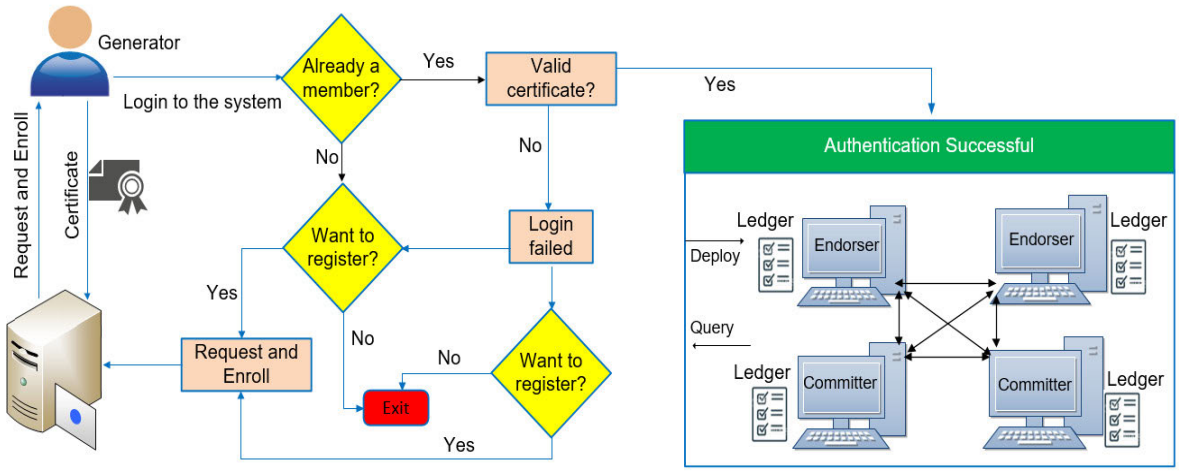


FIGURE 4. Member registration and authentication process in the blockchain network.

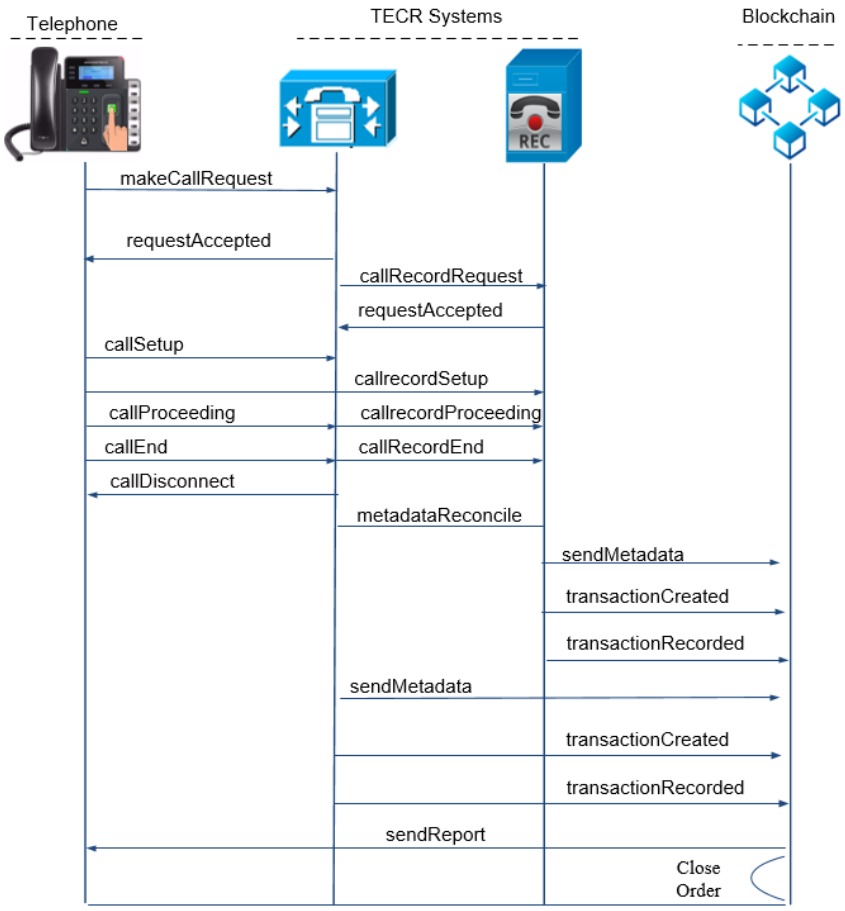


FIGURE 5. Interaction diagram between telephones, TECR and blockchain systems.

TABLE 2. Metadata record fields.

Field	Description
dateTimeOrigination	The date and time when a call is established.
callingPartyNumber	The telephone number of the phone making a telephone call.
calledPartyNumber	The telephone number of the phone receiving a telephone call.
dateTimeConnect	The date and time when a call is connected.
dateTimeDisconnect	The date and time when a call is terminated

3) METADATA AUDITING PROCESS

From the generator's perspective, the auditor is employed by the generator to facilitate the meeting of legal compliance. From the regulator perspective, the regulator employs the auditor to ensure generators meet legal compliance requirements.

The proposed auditing system streamlines the auditing process by making the metadata of call recordings verifiable to replace the paper-based auditing, which is costly and time-consuming. This system enables auditors to complete auditing in a timely manner by making call recording records readily available and verifiable. Through this system, generators and the regulator can also create automated auditing routines that auditors usually perform manually. For example, auditing can be scheduled to run at a specific date and time to meet a specific requirement. This is beneficial when generators and the regulator want assurance that compliance is met without involving auditors. A Transaction query representation is given in Fig. 7.

F. PRESERVING INTEGRITY OF METADATA RECORDS USING THE CLARK-WILSON INTEGRITY MODEL

To enhance overall trust and security, the integrity and authenticity of the metadata records at the source (before metadata are transmitted to the proposed blockchain-based auditing system) are of great importance in order to maintain reliable metadata records. Having reliable and controllable metadata records improves data quality and achieves greater data accuracy.

This research uses the Clark-Wilson Integrity Model to build a system to provide integrity services for the metadata records at the source. The Clark-Wilson Integrity Model uses two categories of mechanisms to realize integrity:

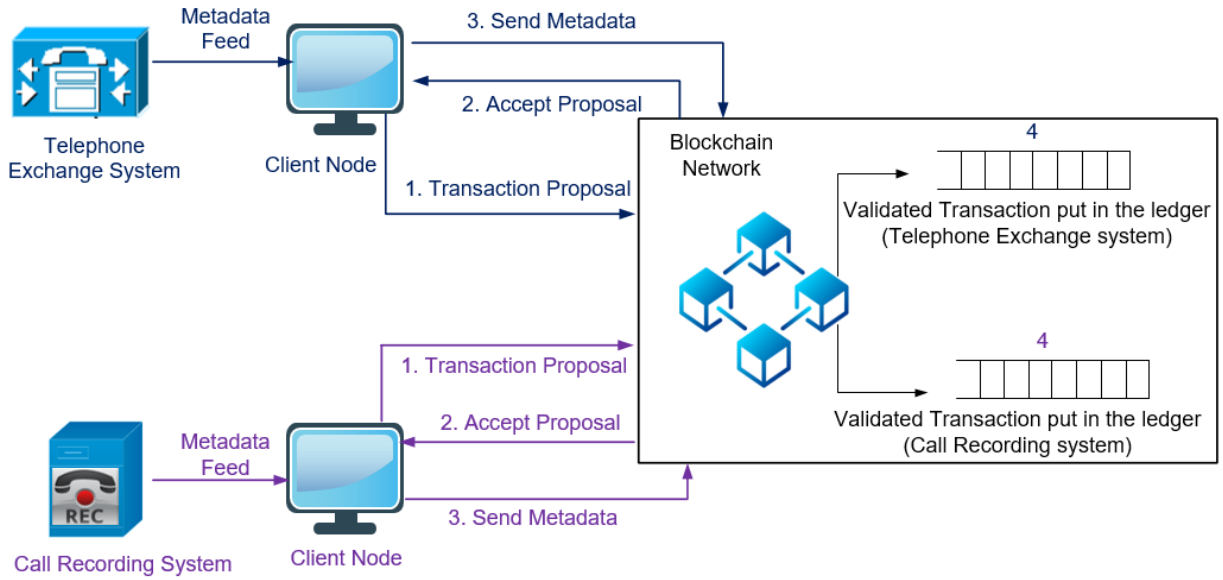


FIGURE 6. The metadata transaction process in our proposed system.

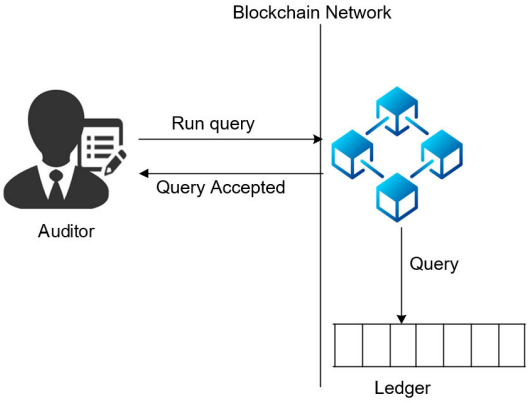


FIGURE 7. Metadata transaction query from the ledger.

well-formed transactions and separation of duty. Below we discuss how our design implements these two categories using the concepts in the Clark-Wilson Integrity Model.

1) WELL-FORMED TRANSACTION

The principle of a well-formed transaction is referred to as a transaction where the user is unable to manipulate data directly, but only in ways that preserve or ensure the integrity of the data. Clark-Wilson Integrity Model classifies data into Constrained Data Items (CDI), where integrity is enforced, and Unconstrained Data Items (UDI), where integrity is not enforced. In our case, the metadata information generated from the TECR systems are considered CDIs. For instance, a trader cannot view the metadata record arbitrarily without completing a verification process. The integrity of the audio-level telephone conversation recordings is not assured so that the telephone conversation data are considered UDIs.

TPs and IVPs are processes that maintain integrity in different ways. For instance, if a user invokes a view, writes or deletes a request for a metadata record, it is considered a TP.

IVPs (through the metadata reconciliation) are performed by comparing the metadata information from the Telephone Exchange system to the metadata information generated from the Call Recording system. IVPs verify that the metadata records are matched from both systems to ensure data consistency. If the metadata records from the two systems are unmatched or unreconciled, that will be flagged for further investigation. Data inconsistency can result in high costs to the organization, including financial and reputational penalties.

Following are two cases where we demonstrate how the Clark-Wilson Integrity Model is applied in our research.

Case 1: the integrity of metadata generation:

1) A caller is *authenticated* and *authorized* to make a telephone call - TP
2) *Metadata* is generated from the TECR systems after a telephone call is completed - CDI
3) *Reconciliation* of metadata records is performed between the metadata received from the TECR systems – IVP

Case 1 above presents in terms of CDIs, which TP processes. The caller, in this case, is the user. The TP refers to the authentication program that authenticates the caller. The metadata is generated through the TP, referred to as the CDIs. IVPs perform the reconciliation of the metadata records.

Case 2: the integrity of access to the metadata records:

TPs are also applied on the metadata records stored in the system so that authorized users are unable to manipulate metadata arbitrarily but only in an appropriate manner that preserves the integrity of the metadata. Below is a Clark-Wilson Integrity Model application scenario whereby a user requests access to metadata records from the system.

1) User logs in (i.e. authenticates). TP is aware of who the user is.

2) The user requests access to metadata records.
3) TP checks to see if the user has the authorization to access metadata followed by an approval process as per Table 3 below.
4) An authorized user is allowed to access metadata records after approval is granted.
5) TP denies access to an unauthorized user or an authorized user that has no right or approval to access metadata.
6) TP writes logs to the audit trail so that IVP (reconciliation) can verify data consistency.

2) SEPARATION OF DUTY

According to the Clark-Wilson Integrity Model, no single user should perform the task from start to end in order to maintain the integrity of the data. The task should be divided among two or more people or entities [38]. In the proposed system, users who have access to the metadata records are set up with their own login access and have a user profile configured with associated rights/roles. No single person can perform actions from start to end. For instance, a trading manager can request access to metadata records through the access request mechanism. The request goes through the approval process, and the security manager must approve the trading manager to have read-only access to metadata records as per the trading manager role, as specified in Table 3. If any change is required to the metadata records, the security manager should raise the change, and the change manager must approve this. All actions must be logged for further integrity verification purposes through the IVR (reconciliation) method. This strict process is followed to ensure that no authorized user can manipulate the metadata records and consistency is preserved. Table 3 below describes the user profiles (entities) and their roles in the system.

Fig. 8 below is an overview of the proposed architecture that shows how integrity is preserved using the Clark-Wilson Integrity Model. This architecture integrates with the proposed blockchain-based auditing system to provide necessary overall trust and security so that required security and legal compliance are both met.

V. FEASIBILITY ANALYSIS OF THE PROPOSED SYSTEM DESIGN

This section evaluates how the proposed system meets the security and legal compliance requirements stated in Section II.

A. MEETING SECURITY, BUSINESS AND LEGAL REQUIREMENTS

This section contends that the proposed scheme meets the five security requirements (SR) mentioned previously in Section II.

TABLE 3. Entities and roles in the TECR systems.

Entity	Roles
Physical Trader	Authorized to make and receive telephone calls.
	No access to metadata records.
Physical Trading Team Leader	Authorized to make and receive telephone calls.
	Read-only access to metadata records (approval required through TP).
	Retrieval of metadata must be authorized by the trading manager and security manager.
	Cannot delete or modify metadata records.
Physical Trading Manager	Authorized to make and receive telephone calls.
	Read-only access to metadata records (approval required through TP)
	Retrieval of metadata must be authorized by the security manager.
	Cannot delete or modify metadata records.
Assurance Manager	Not authorized to make and receive calls.
	Read-only access to metadata records (approval required through TP).
	Retrieval of metadata records must be authorized by trading manager and security manager.
Auditor (employed by a generator)	Not authorized to make and receive telephone calls.
	Read-only access to metadata records (approval required through TP).
	Write access to logs.
Security manager	Not authorized to make and receive telephone calls.
	Write access to metadata (create and add new entries), but cannot modify or delete the original metadata records.
	Can retrieve recoding data.
	Write access to logs.
	Can change system configuration (change approval required by change manager).
	Administration and supervision of the system.
Change manager	Review and approve/reject changes

1) SR1: INTEGRITY

The proposed system uses the Clark-Wilson Integrity Model and the blockchain to reinforce integrity.

The proposed system adopts and adapts the Clark-Wilson Integrity Model by using certification and enforcement rules to ensure the data integrity of metadata records generated from the generator's TECR systems. The certification and enforcement rules are categorized as follows:

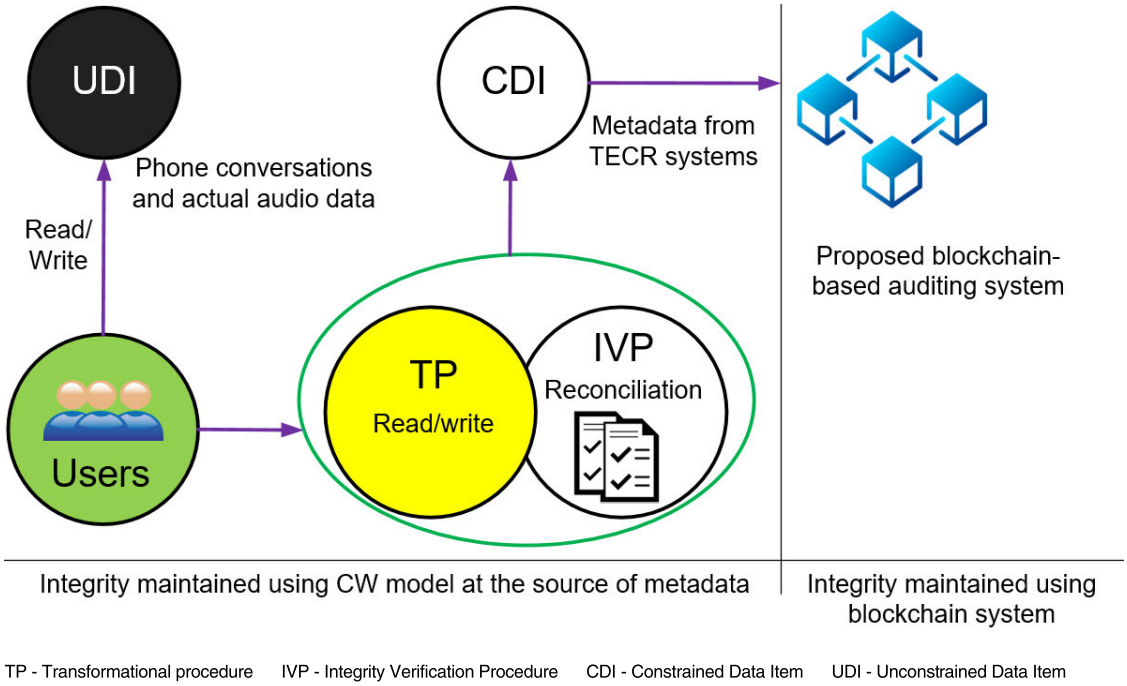


FIGURE 8. Application of the Clark-Wilson integrity model to preserve the integrity of metadata records at the source.

1) C1, C2 and E1 rules provide the basic framework to ensure internal consistency of the CDIs.

In our proposed system, the metadata reconciliation process is referred as an IVP, which is used to verify the consistency of the CDIs. This is achieved by reconciling the metadata records to check consistency between the TECR systems. Any change to metadata records (CDI) is through a TP.

2) E2 and C3 rules reinforce the principle of separation of duty to prevent one individual from acting alone to subvert CDIs.

In our proposed system, a strict separation of duties is maintained between different users to access the TECR systems such that duties are not performed by one individual.

3) E3 rule enforces the requirements that only authenticated users can execute a TP.

The proposed system uses a multi-factor authentication mechanism to authenticate users to access the TECR systems. The system log audits successful/unsuccessful login attempts.

4) C4 rule imposes the requirement that all events must be logged.

In the proposed system, each record generated from the TECR systems is logged and audited. Any data transactions submitted to the blockchain system are also logged and audited to monitor possible security breaches or system abuse/manipulation.

5) C5 rule requires any TP to take a UDI as input and perform only valid transformations. The transformation either rejects the UDI or transforms it into a CDI.
6) E4 rule ensures that only an authorized security officer can change the list of users associated with that TP.

In the proposed system, a security officer has the role of user administration and supervision. Access permissions can only be modified by a security officer, which makes the integrity enforcement mechanism mandatory.

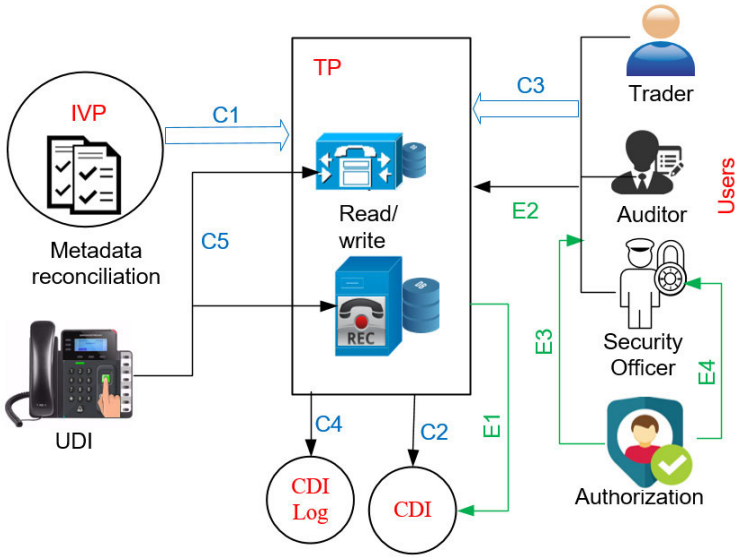
Fig. 9 shows how the certification and enforcement rules of a Clark-Wilson Integrity Model concept are applied in our design to meet the integrity requirements of the metadata records generated from the generator's TECR systems.

In our proposed blockchain-based auditing system, we use role-based access control mechanisms to delegate who is allowed to read and/or write to the ledger. When a metadata transaction is submitted, the blockchain system validates the submitted transaction, and each peer needs to reach a consensus before the submitted transaction is stored in the ledger. If a metadata transaction has been stored in a ledger, it cannot be modified or deleted. The unique hash value generated for each metadata transaction in the ledger is used to verify the integrity of the metadata.

2) SR2: AUTHENTICATION AND AUTHORIZATION

From the perspective of the metadata generator systems (TECR), a multi-factor authentication mechanism is used to authenticate users to access the systems. Once the user is authenticated, the TECR systems check a user's profile to determine if the user can access metadata records, as stated in Table 3.

From the perspective of the blockchain-based auditing system, each member possesses a key pair, a private and public key. A private key is used for metadata transaction signing and endorsing. The CA attests the associated public key and is made available for anyone to validate signed and



C1: Ensure all CDIs are in a valid state when any IVP is executed
C2: Perform and ensure those CDIs are transformed from a valid state into a valid state through TPs
C3: Enforce the principle of separation of duty
C4: Audit log on TP operations
C5: To execute UDIs to CDIs through TPs
E1: Ensure the CDIs are only changed by certified TP
E2: Ensure the authorized user access a particular CDI through a TP
E3: Ensure users are authenticated to execute a TP
E4: Ensure only authorized security officer can change the list of users associated with that TP

FIGURE 9. Application of Clark-Wilson integrity model rules to our design architecture.

endorsed transactions. Each member (generator, auditor and regulator) of the system requires specific access to read and/or write transactions to the system, as stated in Table 1.

3) SR3: CONFIDENTIALITY

From the perspective of the TECR systems, all call recordings are encrypted and stored in the Call Recording system. Each metadata transaction transferred to the blockchain-based auditing system is also encrypted before transmission to maintain confidentiality.

From the perspective of the blockchain-based auditing system, all metadata records stored in the ledger are encrypted for confidentiality purposes.

4) BR1: AUDIT AUTOMATION AND AVAILABILITY

The current telephone call recordings and reconciliation information are provided to the auditor in either electronic and/or manual format that requires the auditor to spend significant time to conduct auditing against each telephone call recording. In the proposed system, the auditing process has been streamlined to replace manual labour-intensive auditing tasks.

From the generator's perspective, the metadata reconciliation mechanism is in place to automatically flag any unmatched metadata records between the Telephone Exchange and Call Recording systems. For example, if the Call Recording system fails to record a telephone conversation, then this is flagged as a missing record. The current system lacks this curial function that can lead to financial penalties.

From the regulator's perspective, the proposed blockchain-based auditing system provides constant availability and visibility of the auditing of telephone call recordings to the regulator. When the TECR systems transmit metadata transactions to the blockchain-based auditing system, metadata records are readily available for regulators for auditing purposes. However, in the current system, a regulator has to request a generator to provide telephone call recordings when required.

This is beneficial to the regulator or generator to ensure meeting the compliance requirement, with or without needing to involve the auditor.

5) BR2: OWNERSHIP

In our proposed system, each generator maintains control of their own telephone call recordings. They have their own telephone call recording storage and have access to it. What is transmitted to the proposed blockchain-based system is the metadata records from the TECR systems. This allows generators to demonstrate to the regulator or auditors that they have not deleted or changed any telephone call recordings.

6) LEGAL COMPLIANCE (LC1-LC4)

This study contends that the proposed system meets the defined security and business requirements, which satisfies the legal requirements (LC1 – LC4) mentioned in Section II.

TABLE 4. Average number of telephone calls and call recordings.

	Per trading day
The average number of telephone calls made and/or received	7,800
Average telephone call recording data generated	982 megabytes
Average metadata generated	0.45 megabytes

B. PERFORMANCE FEASIBILITY OF OUR PROPOSED DESIGN AND ARCHITECTURE

In assessing the practical feasibility of the proposed design, we estimated the average telephone call volume in the National Electricity Market per trading day and the size of the telephone call recordings with the associated metadata records. The wholesale electricity market trading day is a 24-hour period that begins at 4:00 am each day [3].

Based on a real case of the telephone call recordings from an actual power generator, approximately 7800 records are generated per trading day. There are around 100 generators in the national electricity market in Australia [32]. Thus, as summarized in Table 4, approximately 982 megabytes of telephone call recordings and 0.45 megabytes of metadata records are generated nationally.

This research defines scalability as the ability for a system to be able to process associated volumes of metadata transactions. The proposed blockchain-based auditing system only contains the metadata records rather than actual telephone call recordings. Metadata records are more lightweight than actual telephone call recordings. The proposed blockchain system only carries a light load of metadata transactions; therefore, the performance issue is less of a concern. Furthermore, our design has no real-time requirement as auditing is usually required after the trading period is complete.

Our design is based on the permissioned blockchain. Performance on the permissioned blockchain, such as the Hyperledger fabric, is different from the permissionless blockchain. Pongnumkul *et al.* [44] and Thakkar *et al.* [45] also attested to better performance of the permissioned blockchain based on the Hyperledger fabric than the permissionless blockchain. Gorenflo *et al.* [43] argued that the Hyperledger fabric can increase transaction throughput from 3,000 to nearly 20,000 transactions per second.

To validate the performance feasibility of the proposed design, this research estimated the blockchain ledger storage requirements of the electricity market. Calculations are based on the average daily telephone call transaction volume for the auditing system and the daily telephone calls made/received. The following assumptions are made:

- All Hyperledger Fabric blocks are 1 megabyte (MB) in size and have 1000 transactions per block.
- Only hash, digital signature and trading transactional data are stored in the blockchain ledger (in the case of the trading system).
- Only hash, digital signature and call recording metadata are stored in the blockchain ledger (in the case of the auditing system).
- Australia's wholesale electricity market operates 24 hours a day, 7 days a week.

Based on the above assumptions, the amount of storage required for the proposed auditing system per transaction per year is 32.29 gigabytes (GB). Using the most conservative estimate of 1000 transactions per block, 2.91 GB of storage per year is required based on a 0.09 transaction per second (TPS) (derived from 7,800 telephone calls made/received per 24 hours trading day) level of blockchain activity. These calculations are based on data supplied by an actual power generator and then extrapolated to derive the maximum volume of transactions applicable to the electricity market nationally. The ledger storage requirements for the proposed architecture design is shown to be feasible to implement using a commonly available commercial grade of cloud-based platforms.

The calculations of the storage required is as follows:

(0.09 TPS/1000 transaction per block) x (1024 KB/block) x (3600 second/hour) x (24 hour/day trading) x (365 days/year trading) = 2,906,358 KB or 2.91 GB of storage per year.

C. COMPARISON BETWEEN CURRENT AND PROPOSED SYSTEMS

This section provides a comparison between the current and proposed systems in terms of protection of the confidentiality, integrity, availability and quality control of the metadata records.

1) CONFIDENTIALITY AND INTEGRITY

The current system lacks the use of an automated solution to monitor and audit records of telephone call conversations in a secure manner. It does not provide for the confidentiality and integrity of the telephone call recording data. There are also no existing authentication or authorization methods.

The proposed system adopts and adapts the Clark-Wilson Integrity Model by using certification and enforcement rules to ensure the integrity of metadata records generated from the generator's TECR systems is maintained. Each metadata transaction stored in the ledger generates a unique hash value for the metadata's content, which is particularly important for improved data integrity. Access is also restricted to authorized member participants, and transactions are encrypted to preserve confidentiality. Further, the proposed system uses a multi-factor authentication mechanism to authenticate users access to the TECR systems. Each member possesses a key pair, a private and public key. A private key is used for metadata transaction signing and endorsing. Members of the proposed system also require specific authorization to read and/or write transactions to the system.

2) AUDITING CAPABILITIES AND VISIBILITY

The auditing process in the current system is a time consuming manual process which lacks visibility. In the proposed system, audit procedures are automated to meet legal compliance requirements. The auditing process and reviews are streamlined for the generator, regulator and auditor.

3) DATA QUALITY CONTROL

In the current system, no data quality control mechanism exists. In the proposed system, metadata consistency is achieved by a metadata reconciliation mechanism to flag any metadata discrepancy. The proposed design also has the ability to eliminate GIGO issues that are not provided by the blockchain system alone.

VI. CONCLUSION AND FUTURE WORK

This research addressed the telephone call auditing process to meet security and business requirements, as well as legal requirements stipulated by the Australian National Electricity Rules. A Clark-Wilson Integrity Model and a blockchain-based system are proposed to preserve the integrity and confidentiality of associated telephone call recordings and to automate the auditing process. This project defined security and business requirements, which exceed the legal requirement benchmark stipulated by the Australian National Electricity Rules. The proposed system can not only enhance data quality and security but also has the capability to provide constant availability and visibility of telephone call auditing.

Our proposed design is a framework that can be adopted and/or adapted by any commercial blockchain-based application that needs to consider data quality control. The blockchain system only controls integrity when data transactions are processed and stored in the chains, not data quality and integrity when data enter the blockchain system. Our proposed design addresses overall security from the data generating process to the blockchain system. With the support of a state-owned power generator, our future work is to develop a complete prototype to demonstrate the feasibility of the proposed architecture. Moreover, this research forms the foundation for the creation of a prototype for appropriate auditing automation processes. This will form the basis of future requests for research funding. The proposed architecture will be developed as a complete proof-of-concept which may be used in conjunction with our previous work [42] when tendering for supply and installation. It is suggested that government should issue requests for the development and testing of this proposal. Upon successful bidder testing, this proposal suggests that government would issue tenders for the production and installation of the proposed system in a running environment. This proposal is based on successful experience in the energy sector, particularly the successful structure and deployment of energy-related networks and systems over many years.

ACKNOWLEDGMENT

The authors would like to thank Dr. Bob Maczkowiack for taking the time to review the manuscript. They sincerely appreciate his invaluable comments and editing work on this study.

REFERENCES

[1] National Electricity Rules. *Australian Energy Market Commission*. Accessed: Jul. 20, 2020. [Online]. Available: https://www.aemc.gov.au/sites/default/files/2021-03/NER%20v161%20full_0.pdf
[2] G. Perboli, M. Stefano, and R. Mariangela, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.
[3] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Oct. 2017, pp. 1–5.
[4] J. Schmitz and G. Leoni, "Accounting and auditing at the time of Blockchain technology: A research agenda," *Austral. Accounting Rev.*, vol. 29, no. 2, pp. 331–342, Jun. 2019.
[5] X. Zhu and D. Wang, "Application of blockchain in document certification, asset trading and payment reconciliation," in *Proc. J. Phys., Conf.*, vol. 1187, 2019, Art. no. 052080.
[6] C. Ingle, A. Samudre, P. Bhavsar, and P. S. Vidap, "Audit and compliance in service management using blockchain," in *Proc. IEEE 16th India Council Int. Conf. (INDICON)*, Rajkot, India, Dec. 2019, pp. 1–4.
[7] A. M. Rozario and M. A. Vasarhelyi, "Auditing with smart contracts," *Int. J. Digit. Accounting Res.*, vol. 18, pp. 1–27, Jan. 2018.
[8] E. Bonson and M. Bednarova, "Blockchain and its implications for accounting and auditing," *Meditari Accountancy Res.*, vol. 27, pp. 725–740, 2019. [Online]. Available: https://www.emeraldgrouppublishing.com/journal/medar?_ga=2.132316422.903189292.1635133745-985869193.1635133745
[9] S. Suzuki and J. Murai, "Blockchain as an audit-able communication channel," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Turin, Italy, Jul. 2017, pp. 516–522.
[10] V. Lemieux, D. Hofman, D. Batista, and A. Joo. (2019). *Blockchain Technology & Recordkeeping*. ARMA Educational Foundation, Canada. [Online]. Available: https://www.researchgate.net/publication/333659272
[11] P. W. Abreu, M. Aparicio, and C. J. Costa, "Blockchain technology in the auditing environment," in *Proc. 13th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2018, pp. 1–6.
[12] T. Rechtman, "Blockchain: The making of a simple, secure recording concept," *CPA J.*, vol. 87, no. 6, pp. 15–17, 2017.
[13] W. Zhang, Y. Yuan, Y. Hu, K. Nandakumar, A. Chopra, and A. D. Caro, "Bockchain-based distributed compliance in multinational corporations' cross-border intercompany transactions," in *Proc. Future Inf. Commun. Conf. (FICC)*, Singapore, 2018, pp. 508–517.
[14] X. Chu, T. Jiang, X. Li, and X. Ding, "Bye audit! A novel blockchain-based automated data processing scheme for bank audit confirmation," in *Proc. China Blockchain Conf. (CBCC)*, Singapore, 2019, pp. 68–82.
[15] B. Carpenter, "Can blockchain help the department of defence achieve a clean audit?" *J. Government Financial Manage.*, vol. 67, pp. 48–53, Mar. 2018.
[16] S. Wohlgemuth, K. Umezawa, Y. Mishina, and K. Takaragi, "Competitive compliance with blockchain," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Kyoto, Japan, Mar. 2019, pp. 967–972.
[17] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.
[18] A. M. Rozario and C. Thomas, "Reengineering the audit with blockchain and smart contracts," *J. Emerg. Technol. Accounting*, vol. 16, no. 1, pp. 21–35, Mar. 2019.
[19] J. H. Raphael, "Rethinking the audit: Innovation is transforming how audits are conducted—And even what it means to be an auditor," *J. Accountancy*, vol. 223, pp. 28–32, 2017.
[20] J. A. Jaoude and R. G. Saade, "Blockchain applications–usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.
[21] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *J. Inf. Syst.*, vol. 31, no. 3, pp. 5–21, Jun. 2017.
[22] H. Nguyen, C. Ignat, and O. Perrin, "Trusternity: Auditing transparent log server with blockchain," in *Proc. Web Conf.*, Lyon, France, 2018, pp. 79–80.
[23] T. Antipova, "Using blockchain technology for government auditing," in *Proc. 13th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Caceres, Spain, Jun. 2018, pp. 1–6.

[24] J. Dai, N. He, and H. Yu, "Utilizing blockchain and smart contracts to enable audit 4.0: From the perspective of accountability audit of air pollution control in China," *J. Emerg. Technol. Accounting*, vol. 16, no. 2, pp. 23–41, Sep. 2019.
[25] S. Smith, "Blockchain augmented audit–benefits and challenges for accounting professionals," *J. Theor. Accounting Res.*, vol. 14, no. 1, pp. 117–137, 2018.
[26] A. Sutton and R. Samavi, "Blockchain enabled privacy audit logs," in *The Semantic Web (ISWC)*. Cham, Switzerland: Springer, 2017, pp. 645–660.
[27] *The National Blockchain Roadmap: Progressing Towards a Blockchain-Empowered Future, Australia Department of Industry, Science, Energy and Resources*. Accessed: Aug. 10, 2020. [Online]. Available: https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf
[28] N. Brender, M. Gauthier, J. Morin, and A. Salihi, "The potential impact of blockchain technology on audit practice," *J. Strategic Innov. Sustainability*, vol. 14, pp. 35–59, Feb. 2019.
[29] A. Kwilinski, "Implementation of blockchain technology in accounting sphere," *Acad. Accounting Financial Stud. J.*, vol. 23, pp. 1–6, Feb. 2019.
[30] Y. Zhang, F. Xiong, Y. Xie, X. Fan, and H. Gu, "The impact of artificial intelligence and blockchain on the accounting profession," *IEEE Access*, vol. 8, pp. 110461–110477, 2020.
[31] J. Xue, C. Xu, Y. Zhang, and L. Bai, "DStore: A distributed cloud storage system based on smart contracts and blockchain," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.*, Guangzhou, China, 2018, pp. 385–401.
[32] Spot and Contract Market. *Australia Energy Market Commission (AEMC)*. Accessed: Aug. 10, 2020. [Online]. Available: https://www.aemc.gov.au/energy-system/electricity/electricity-market/spot-and-contract-market
[33] *A Blockchain Platform for the Enterprise, Hyperledger*. Accessed: Aug. 15, 2020. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/v2.2.1/
[34] *Rubix—Deloitte Enterprise Blockchain Government Solutions?*. Bitcoin Exchange Guide. Accessed: Sep. 16, 2020. [Online]. Available: https://bitcoinexchangeguide.com/rubix/
[35] KPMG and Microsoft Announce New. *Blockchain Nodes*. PMG. Accessed: Jul. 25, 2020. [Online]. Available: https://home.kpmg/sg/en/home/media/press-releases/2017/02/kpmgand-microsoft-announce-new-blockchain-nodes.html
[36] J. R. Kozloski, C. A. Pickover, and K.Weldemariam, "Blockchain-enhanced mobile telecommunication device," U.S. Patent 10 693 954 B2. Sep. 16, 2018. [Online]. Available: https://patentimages.storage.googleapis.com/75/d1/0f/e01e4a0ce3d0b3/US10693954.pdf
[37] M. Bishop, E. Sullivan, and M. Ruppel, *Computer Security: Art and science*. 2nd ed. Reading, MA, USA: Addison-Wesley, 2019.
[38] D. D. Clark and D. R. Wilson, "A comparison of commercial and military computer security policies," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, Apr. 1987, p. 184.
[39] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
[40] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[41] L. Zhang and Q. Li, "Research on consensus efficiency based on practical Byzantine fault tolerance," in *Proc. 10th Int. Conf. Model., Identificat. Control (ICMIC)*, Guiyang, China, Jul. 2018.
[42] A. D. Tesfamicael, V. Liu, M. Mckague, W. Caelli, and E. Foo, "A design for a secure energy market trading system in a national wholesale electricity market," *IEEE Access*, vol. 8, pp. 132424–132445, 2020.
[43] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "FastFabric: Scaling hyperledger fabric to 20 000 transactions per second," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, Seoul, South Korea, Sep. 2019, pp. 455–463.
[44] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, Jul. 2017, pp. 1–6.
[45] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *Proc. IEEE 26th Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst. (MASCOTS)*, Milwaukee, WI, USA, Sep. 2018, pp. 264–276.

AKLILU DANIEL TESFAMICAEL received the B.S. degree in mathematics from the University of Asmara, Asmara, Eritrea, in 1997, and the M.S. degree in information technology from the University of South Australia, Adelaide, Australia, in 2003. He is currently pursuing the Ph.D. degree in information security with the Queensland University of Technology (QUT), Brisbane, Australia.

He is working as a Technical Architect at CS Energy, Queensland Energy Company, that generates and sells electricity in the National Electricity Market. He has previously worked in energy sectors and government departments for over 16 years, attaining the position of a Solutions Architect and a Senior Network Engineer. His research interest includes network and security architectures for critical infrastructure.

VICKY LIU received the Ph.D. degree in information security from the Queensland University of Technology, Australia. Her Ph.D. dissertation proposed an information system architecture to facilitate the enforcement of privacy and security. She is currently a Lecturer with the Science and Engineering Faculty, Queensland University of Technology. Her research interests include network and security, in particular focusing on the Internet of Things (IoT) technologies and security aspects as well as network performance optimization. Recently, she actively involves in a number of government-funded research projects in addressing solutions for designing appropriate IoT architectures and balancing performance and security for IoT ecosystems.

MATTHEW MCKAGUE received the B.Sc. degree (Hons.) in mathematics from the University of Regina, Regina, Canada, in 2004, and the M.Math. and Ph.D. degrees in combinatorics and optimization from the University of Waterloo, Waterloo, Canada, in 2005 and 2010, respectively.

He is currently a Lecturer in cryptography at the Queensland University of Technology, Brisbane, Australia. Previously, he worked as a Research Fellow at the Centre for Quantum Technologies, Singapore, and a Lecturer with the Computer Science Department, University of Otago, Dunedin, New Zealand.

WILLIAM CAELLI received the B.Sc. degree (Hons.) from The University of Newcastle, Newcastle, Australia, in 1966, and the Ph.D. degree in nuclear physics from The Australian National University (ANU), Canberra, Australia, in 1972.

He is currently an Emeritus Professor and an Officer in the Order of Australia (AO). He was a Co-Founder of ERACOM Pty Ltd. (originally Electronics Research Australia Pty Ltd.), in 1979, the Foundation Director of the Information Security Research Centre (ISRC), QIT/QUT, in 1988, and later the Founding Head of the School of Data Communications. He was the Director/Founder of International Information Security Consultants Pty Ltd. (IISEC). He is an Emeritus Professor with the Queensland University of Technology, an Adjunct Professor at Griffith University, and an Honorary Fellow in cybersecurity at TAFE, Queensland. He has 50 years of involvement, experience, teaching, and research/publication in all aspects of information/cyber security, including public policy and related matters, having first investigation experience of a cyber-attack in late-1968. He has over 55 years professional experience in ICT overall.

Prof. Caelli is a member of the National Cybersecurity Committee and the Cyber Resilience Task Force of the Australian Computer Society (ACS). This has included some eight years as a member of the Board of the USA's Colloquium for Information Systems Security Education (CISSE).