BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem

Awuson - David, K., Al-Hadhrami, T., Alazab, M. A., Shah, N. & Shalaginov, A.

Original citation & hyperlink:
Awuson - David, K, Al-Hadhrami, T, Alazab, MA, Shah, N & Shalaginov, A 2021, 'BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem', Future Generation Computer Systems, vol. 122, pp. 1-13.
https://dx.doi.org/10.1016/j.future.2021.03.001

DOI 10.1016/j.future.2021.03.001
ISSN 0167-739X

Publisher: Elsevier

BCFL Logging: An Approach to Acquire and Preserve Admissible Digital Forensics Evidence in Cloud Ecosystem

Kenny Awuson-David[a,], Tawfik Al-Hadhrami[b,*], Mamoun Alazab[c], Nazaraf Shah[d], Andrii Shalaginov[e]

[a]*Institute for Future Transport and Cities, Coventry University, Priory Street, Coventry, CV1 5FB*
[b]*School of Science and Technology, Nottingham Trent University, Nottingham, NG11 8NS, United Kingdom*
[c]*College of Engineering, IT and Environment, Charles Darwin University, Australia*
[d]*Institute for Future Transport and Cities, Coventry University, Priory Street, Coventry, CV1 5FB*
[e]*Norwegian University of Science and Technology Gjovik, Norway*

Abstract

Log files are the primary source of recording users, applications and protocols, activities in the cloud ecosystem. Cloud forensic investigators can use log evidence to ascertain when, why and how a cyber adversary or an insider compromised a system by establishing the crime scene and reconstructing how the incident occurred. However, digital evidence acquisition in a cloud ecosystem is complicated and proven difficult, even with modern forensic acquisition toolkit. The multi-tenancy, Geo-location and Service-Level Agreement have added another layer of complexity in acquiring digital log evidence from a cloud ecosystem. In order to mitigate these complexities of evidence acquisition in the cloud ecosystem, we need a framework that can forensically maintain the trustworthiness and integrity of log evidence. In this paper, we design and implement a Blockchain Cloud Forensic Logging (BCFL) framework, using a Design Science Research Methodological (DSRM) approach. BCFL operates primarily in four stages: (1) Process transaction logs using Blockchain distributed ledger technology (DLT). (2) Use a Blockchain smart contract to maintain the integrity of logs and establish a clear chain of custody. (3) Validate all transaction logs. (4) Maintain transaction log immutability. BCFL will also enhance and strengthen compliance with the European Union (EU) General Data Protection Regulation (GDPR). The results from our single case study will demonstrate that BCFL will mitigate the challenges and complexities faced by digital forensics investigators in acquiring admissible digital evidence from the cloud ecosystem. Furthermore, an instantaneous performance monitoring of the proposed Blockchain cloud forensic logging framework was evaluated. BCFL will ensure trustworthiness, integrity, authenticity and non-repudiation of the log evidence in the cloud.

Keywords: Blockchain, DSRM, GDPR, Digital log evidence, Trustworthiness, Admissibility

*Kenny Awuson-David
Email addresses: davidk2@coventry.ac.uk (Kenny Awuson-David), Tawfik.al-hadhrami@ntu.ac.uk (Tawfik Al-Hadhrami), alazab.m@ieee.org (Mamoun Alazab), aa0699@coventry.ac.uk (Nazaraf Shah), andrii.shalaginov@ntnu.no (Andrii Shalaginov)

[1]Since 2021.

1. Introduction

The affordability and straightforward approach to quickly deploy a network in a way that has never been realised before have attracted cybercriminals [1, 2]. The challenges faced by cloud forensic investigators in acquiring digital evidence from a cloud platform such as Infrastructure as a service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) have been acknowledged by [3, 4]. The Multi-tenancy, geo-location, political and legal issues have added to this [5, 3]. However, with Hyperledger Fabric Blockchain, an investigator can easily verify the logs' validity as Blockchain transactions are encrypted and hashed with a timestamp, and there is traceability of all transactions. Forensic examiners need to acquire evidence from a cloud ecosystem that is tamperproof, free from contamination and admissible before a court of law, as acquired cloud evidence can prove quite challenging due to its dynamic nature [6]. The landscape of cloud computing not only raises doubt over where data are situated, but it also gives rise to confidentiality and regulatory compliance problems. For instance, the EU GDPR introduced on 25th May 2018 requires that businesses comply in protecting personal data. However, such compliance issues have added another layer of complexity in investigating and acquiring digital evidence from the cloud ecosystem, [7]. Blockchain technology provides auditable transaction logs, making legal disputes less likely and simpler to settle. In an increasingly cloud-oriented society, the ability to identify, obtain, preserve, and analyse potential digital evidence is increasingly essential, [8].

The first measure in the deployment of the experiment for this paper was the creation of a cloud ecosystem in a virtual environment using Docker containerisation instead of virtual machines (VMs). Docker containerisation technology is more efficient compared to VM's due to its capacity for lightweight bandwidth usage [9]. Docker containers have revolutionised the software supply-chain in small and big enterprises. Some authors have observed that no new technology has ever before infiltrated the top 500 enterprises worldwide so swiftly, [10].

This virtual environment will enable Blockchain Cloud Forensic Logging (BCFL) framework to explore and verify how artefacts are preserved and secured in a Blockchain cloud ecosystem, both in transit and storage [11]. The resulting findings will evaluate the need for using Blockchain to maintain and preserve log evidence integrity in a cloud environment. The key features of Blockchain, such as the distributed ledger, smart contracts, encryption, hashing and immutability of data, are aimed to ensure trustworthiness and log evidence integrity in the cloud ecosystem. Blockchain uses its immutability mechanisms to preserve log entries even when the VM instance is deleted or re-booted in a cloud ecosystem.

The drive of this paper is to accomplish the following objectives:

- To investigate how Blockchain technology can be integrated into the cloud ecosystem and its security mechanisms used to maintain trustworthiness and transparency in the cloud by establishing a secure and resilient communication channel between all cloud stakeholders.
- To evaluate related work and the use of Blockchain consensus, data immutability and smart contract mechanisms to preserve the acquired cloud logs' integrity.

The purpose of the experiments undertaken for this research was to provide information on how cloud log evidence can be acquired, preserved and stored securely without being compromised or tampered with. It will follow a Design Science Methodology, then the designed architecture and framework. Secondly, a supply-chain scenario set up to investigate and answer all the above questions using our hybrid visualised test environment. Elasticsearch, Kibana and Logstash (ELK) were used to capture real-time application and system performance metrics [12], [13]. Docker containerised nodes were evaluated to ascertain how they would handle transaction logs in a Hyperledger Fabric Blockchain environment.

The contribution of this paper are summarised as follows:

- Using permissioned Blockchain to maintain tamper-proof log evidence in the cloud ecosystem.
- Integrating permissioned Blockchain in the cloud ecosystem that enables evidence acquisition that enhance GDPR compliance and maintain a secured chain of custody.
- Strengthening Blockchain Distributed Ledger Technology (DLT) and data immutability to maintain acquired log evidence admissibility in the cloud.
- Using a BCFL framework to acquire digital evidence in the cloud ecosystem that establishes a transparent chain of custody and maintains evidence integrity without impacting business operations.

Motivation

Cloud service providers (CSPs) use their own log formats, and without a unified standard or structure, there is a possibility of contamination of log evidence both in transit and in storage [14, 15, 16, 17]. CSPs have continued to look for a solution that can mitigate the ever-increasing threats by implementing a logging mechanism that can maintain digital evidence admissibility. With a resilient, secure and trusted cloud ecosystem design with Blockchain forensic logging capability, it is believed that enables admissible digital evidence.

2. Related Work

Few studies have attempted to apply Blockchain cloud forensic methods to mitigate digital forensic evidence acquisition complexities in the cloud ecosystem. This section introduces related works from four different features: cloud forensic logging, cloud digital evidence integrity, Blockchain cloud forensic, and Blockchain distributed ledger technology logging mechanism.

2.1. Cloud forensic logging

[18] proposed a Forensic Monitoring Plane model designed to solve the challenges in investigating the cloud ecosystem. A centralised server-based architecture that identifies and collects evidence from a suspected malicious activity in the cloud ecosystem. However, according to ENISA 2011, "multi-tenant outsourced services typically cannot give access to the raw log data as it contains records of multiple users and thus would compromise the privacy of other customers [19]. In addition, [20] proposed detailed guidance that demonstrates cloud logging architecture with a set of analytical guidelines adapted to suit all cloud platform services, enabling forensic investigators and operational teams to be more efficient in cloud logging.

2.2. Cloud digital evidence integrity

[16] proposed a Secure-Logging-as-a-Service (SecLaaS) to enhance forensic investigation in the cloud ecosystem that enables the acquisition of admissible log evidence in the cloud. The solution is based on OpenStack that enables cloud forensic investigators to verify the integrity of the acquired log evidence using proof of past log (PPL) and Log Chain (LC). Furthermore, [21] proposed to enhance the Blockchain-as-a-service (BaaS) with more components to support cloud stakeholders. BaaS cloud is designed to leverage Blockchain cloud solutions to secure digital cloud assets and enable businesses to adopt cloud Blockchain. The BaaS concept is similar to the cloud Platform-as-a-Service (PaaS) model but with more enhanced features.

2.3. Blockchain cloud forensic

Block4forensic is a framework based on vehicle-related digital evidence acquisition in post-accident scenarios. The acquired evidence is used to reconstruct what happened during an accident and identify who is at fault and evidence used to support the investigation. Block4forensic integrates a vehicular public key infrastructure (VPKI). It uses a Blockchain distributed ledger mechanism to enable the storage of hashed data. At the same time, transaction details are stored in distributed ledgers as non-hashed data. [22]. Moreover, [23] proposed a Blockchain Interplanetary File System (BlockIPFS) approach that facilitates traceability and improves data trustworthiness. It also enables a secure distributed file-sharing mechanism using Blockchain and maintains data integrity, including preserving the secure ownership of file transactions. [24] presents Forensic-Chain framework that

uses permissioned Blockchain to maintain digital forensics evidence chain of custody. Forensic-Chain concept aims to maintain digital evidence integrity and secure the acquisition process.

2.4. Blockchain distributed ledger technology logging mechanism

ProvChain mechanism, a framework that has the capability to collect, validate cloud data origin through embedding the source data into a Blockchain transaction. Provchain concept aims to extend Blockchain mechanisms to different use cases and verify data records. It can also be used for cloud auditing and generating a Blockchain receipt for each data transaction. As Provchain is designed to collect provenance data from a cloud, it also requires data mining, [25]. In addition, Block-DEF is a digital forensic Blockchain-based framework used to store and preserve digital evidence information in Blockchain. However, in this framework, Byzantine fault tolerance consensus mechanisms are adopted. Therefore, only evidence information is stored on Blockchain, while the remaining evidence is stored in a trusted platform. Furthermore, [26] build and deployed a permissioned Blockchain-based log auditing infrastructure on-premise that maintains log evidence integrity. [27] proposed a Block-DEF, a Blockchain model designed to facilitate scalable Blockchain module. Block-DEF concept aims to maintain tamper-proof evidence through a Blockchain name-based PBFT while ensuring maintenance of privacy, traceability and evidence integrity is achieved.

Cloud forensics investigation is viewed differently from traditional computer forensics as it involves several administrative domains, extensive data replication, multi-tenancy and often operates across various jurisdictions and lack of trust among cloud stakeholders [28, 29, 30]. In many court cases, cloud adversaries go free as evidence presented before the court is not admissible [31, 32].

The BCFL framework mitigates the high level of evidence contamination pathways (multi-tenancy, geo-location, and cloud service-level agreement) in the cloud. In addition, it acts as a bridge that enables evidence acquisition that accomplishes the GDPR compliance. In contrast to the other related work, Provchain is based on permissionless Blockchain and required Blockchain miners to be paid for the validation of block authenticity. While BCFL is based on permissioned Blockchain and does not require mining to facilitate its function of ensuring log evidence acquired is admissible.

2.5. Comparison Table

Table 1 compared literature in cloud forensics, Blockchain cloud integration and how to improve digital evidence acquisition in the cloud ecosystem. The comparison table highlights a clear view of the research gap in the area of secure cloud forensic logging.

Table 1: Comparison of Using Blockchain to Secure Forensic Evidence in the Cloud Ecosystem

Contribution	Cloud Artifact Identification	Cloud Permissioned Blockchain	Securing Data Integrity with Blockchain	Blockchain Cloud Trustworthiness	Tamperproof Digital Evidence	GDPR Cloud Forensic Challenges	Cloud Log Evidence Immutability	Year
[25]	✓	-	✓	✓	✓	-	-	2017
[24]	✓	✓	✓	✓	✓	-	-	2019
[22]	✓	✓	✓	✓	✓	-	-	2018
[27]	-	✓	✓	✓	✓	-	-	2019
[26]	-	✓	✓	✓	✓	-	-	2018
[33]	-	-	-	-	✓	-	-	2020
[21]	-	✓	✓	✓	✓	-	✓	2019
[23]	-	✓	✓	✓	✓	-	-	2019
BCFL	✓	✓	✓	✓	✓	✓	✓	2021

2.6. Traditional and Cloud Forensic

Traditional digital forensic techniques may not be possible to capture and preserve evidence as the same in a cloud landscape [34]. According to [35] Blockchain transaction is stored with high integrity, resiliency and trustworthiness that is tamperproof. Table 2 highlights the challenges in traditional and cloud forensics processes. An experienced traditional forensic investigator may find it challenging to carry out a forensic investigation in the cloud as the physical location of evidence could be in a different country that does not have a standard legal electronic investigative framework. In an increased cloud-oriented society, the ability to identify, obtain, preserve, and analyse potential digital evidence is valuable for business continuity and security. Distributed consensus, data consistency, and immutability of processed transactions solve the challenges of cloud evidence admissibility. Besides, these features can make it nearly impossible to alter learning records on the network [36, 37].

Table 2: Traditional and Cloud Forensics Comparison

Traditional Forensics	Cloud Forensics
The electronic crime scene can be easily identified.	The electronic crime scene is difficult to access as it is fragmented in different geo-locations.
An organisation owns the network infrastructure and all its digital assets, including managing system logs.	Digital assets, including logs, are primarily owned by cloud service providers (CSP).
Network devices retain their logs and can be accessed by system administrators.	Due to the on-demand nature of the cloud, log evidence is lost when the virtual machine is deleted [38].
There are standard tools used for digital forensic acquisition.	There are no clearly defined standard tools used for digital forensic acquisition in the cloud.

2.7. Cloud Computing

Cloud computing is defined by the US National Institute of Science and Technology (NIST) as "a model for enabling Businesses to share resources, on-demand network as access to a shared pool of configurable computing resources, for instances networking components such as servers, storage, applications, and services that can be swiftly deployed and connected with slight management input or service provider interaction [39]". In addition, to cloud deployment, NIST defines three cloud service models, known as the SPI model infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), respectively. Cloud technology separates application and information resources from the fundamental infrastructure and the mechanisms used to deliver them, enabling collaboration, agility, scaling, and potential cost reduction. A vital element of cloud computing is its "multi-tenancy" capability, which is described as a "shared pool of resources" in the NIST definition [40], as will be further explained in section 2.8.

In the presence of an untrusted host, some threats could compromise data security. An adversary or insider can compromise a cloud network using payloads such as man-in-the-middle or a distributed denial-of-service attack (DDoS) and malicious malware [41, 42, 43]. A log tamperproof evidence approach is needed to mitigate the challenges faced by cloud forensics investigator. Acquiring log evidence from the cloud ecosystem can be an uphill task for a digital forensic investigator as the nature of the cloud ecosystem could prove challenging to preserve the acquired log evidence's

integrity. It is clear that the current digital forensics acquisition process in the cloud is not working as a comprehensive new approach is required.

2.8. Cloud Multi-tenancy

As mentioned above, a key component of cloud computing is its "multi-tenancy" capability. Multi-tenancy can be defined as a cloud service that supports on-demand resources or applications by multiple users[44]. This means that services cannot usually give access to raw log data as it contains records of multiple users on the same shared server. If log acquisition access is given, it could breach other customers' privacy rights, [45]. Therefore, features inherent to clouds computing (storage) services such as multi-tenancy, data security, file encryption, and communications encryption also need to be addressed as part of a digital forensics investigation.

2.9. Blockchain

In 2009, a whitepaper called Bitcoin: Satoshi Nakamoto published a Peer-to-Peer Electronic Cash System to resolve the current challenges faced in the monetary market, with the main aim of developing a technology that can allow electronic transactions from one party to another without going through financial institutions. One of the significant challenges addressed was the double method, which is used to avoid double-spending (a unique problem with digital currency is the risk of reproducing the same amount, even after spending). The idea of Bitcoin is to provide a digital currency that made it easier to solve the problem of double-spending, and the technology that facilitates it is known as Blockchain [46, 28, 47].

Blockchain structure can be described as an organisational structure where each department (which are the blocks) has a defined project to work on, with start and end dates (the transaction). The department then allocates these projects to individuals that work in a consensual manner where every effort is made to improve the performance of the organisation. Similarly, in a Blockchain ecosystem, each block consists of a transaction that has a header, timestamp for forensic and digital hashing that secure transaction. It also includes a reference that contains the information from the previous block. Blockchain security mechanisms such as cryptographic, smart contract, hashing and data immutability are building block of Blockchain structure in preserving the integrity of data both in transit and storage. This technology proved itself during the introduction of the Bitcoin cryptocurrency as a permissionless Blockchain. It establishes trustworthiness between two strangers to carry out a safe transaction without a central entity such as banks. The distributed ledger technology, where specifically transactions, are linked to each other, mainly through the Merkle tree, as shown in Fig. 1.

In a Blockchain technology design structure, the genesis block is the first block of the chain and does not have any pointer to any other block in the chain as highlighted in Fig. 2. However, the

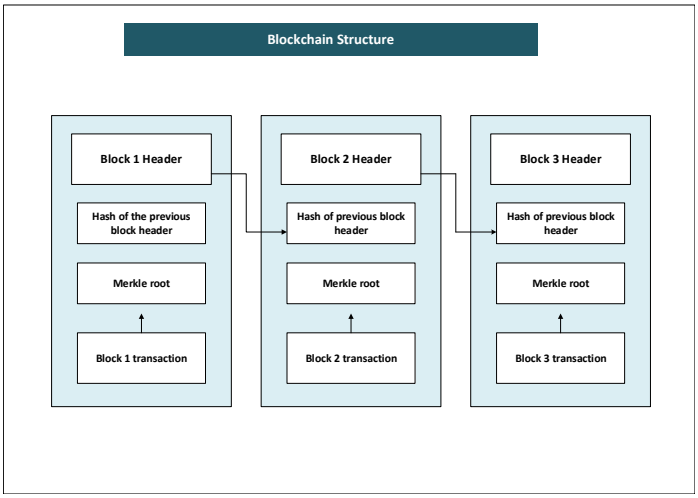

Fig. 1: The Block Structure of Blockchain Technology

Blockchain block structure depends on the type of Blockchain and the data stored in the block. For example, Permissioned and Permissionless Blockchain data storage in the block differ.

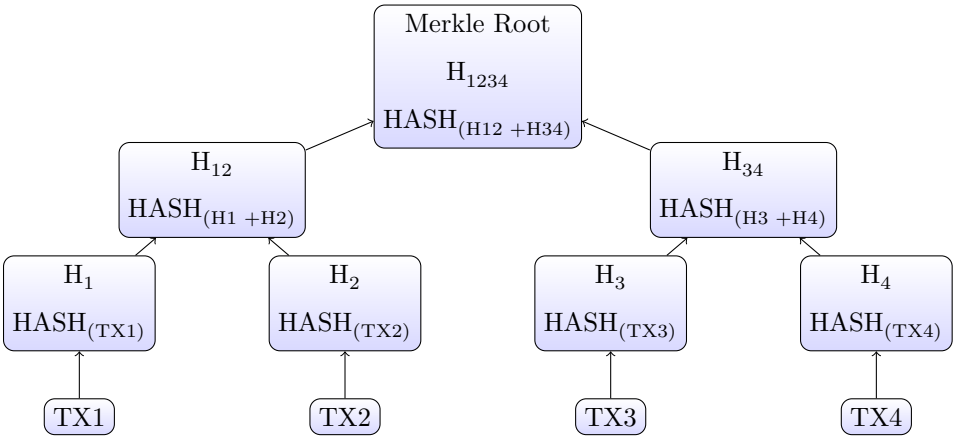

Fig. 2: Blockchain Merkle tree

Blockchain is designed to ensure data immutability and secure transactions in mind and the capability to distribute data through a consensus mechanism. To achieve this, it uses the Merkle tree, which is a cryptographic hashing tree mechanism used by Blockchain to ensure that the data block of every leaf node is hashed and verified [25, 48]. 2 captures the high-level structure of the Blockchain Merkle tree, which uses a hashing function such as MD5, SHA-3, SHA-256 and mathematical algorithm which take an input and provide unique output.

Each non-leaf node in the hierarchical structure is categorised with a hash and digital signature of the child node as its input. The cryptography hash function is designed to take any input data and produces an output built on the algorithm in use that has changed fixed length. The output hash function is always a string value that is programmed in Java, Python or Go language.

For instance, the SHA256 hash is a 256-bit 32byte string of the input data. The Merkle tree structure enables Blockchain to maintain the integrity and confidentiality of all the data processes and transaction between nodes in the ecosystem. It permits Blockchain participants to remove a leaf that is considered private but maintains the hash algorithm, thus preserving the integrity of the tree.

The European agency for network and information security (ENISA) has highlighted possible vulnerabilities in a permissionless Blockchain that might compromise data integrity during storage. They advise organisations within the European Union to consider data confidentiality and integrity in a permissionless Blockchain. One of the most complex challenges in applying the GDPR regarding the digital forensic acquisition in the cloud ecosystem is the underlying IT systems abide by the concept of the principle of privacy by Design(Art.25 GDPR) [49]. This stipulates that privacy should be promoted as a default setting for all IT hardware and software. This adds another layer of complexity in acquiring admissible tamperproof evidence from any digital device that maintains a healthy evidence chain of custody throughout the investigation process. Blockchain Cloud Forensic Logging (BCFL) will preserve the integrity of acquired log evidence in the cloud ecosystem and mitigate the GDPR challenges faced by cloud forensic investigators within the European Union.

3. DESIGN SCIENCE RESEARCH METHODOLOGY (DSRM)

In our approach to the research problem, we adopted the Design Science Research Methodology (DSRM) of [50] and adapted it to suit a Blockchain cloud forensic logging environment that enables admissible evidence acquisition in the cloud ecosystem, as shown Fig.3. The DSRM is a model developed by [51] is a research design methodology that aims to produce original new and real knowledge [52]. It consists of the output of an artefact, which in computer science research could be output in the form of an adaptation, invention, improvement, or routine design [53]. For the investigative activity, it is vital to be familiar with the design science research methodology (DSRM) knowledge context which contributes to the novelty of this paper. In the DSRM adoption, an initial phase is to set up a test environment that integrates Blockchain into the cloud ecosystem to simulate an experiment in a VMware virtualised environment. VMware workstation 15.0 was used to simulate a cloud environment that hosts a guest Linux Ubuntu 20.04 operating system. It was considered that running an experiment on a VMware application instead of any cloud platform would enable us to get the accurate final experimental result. It is challenging to request log information from the cloud ISP's.

Next, the decentralised ledger provides auditable transaction logs that maintain a high level of evidence, integrity and immutability. The investigators can inspect all log transaction in the BCFL network terminal, which list the connections to the chaincode on the peer with timestamps. In the social context of the DSRM, the Hyperledger Fabric Blockchain is used to secure logs evidence

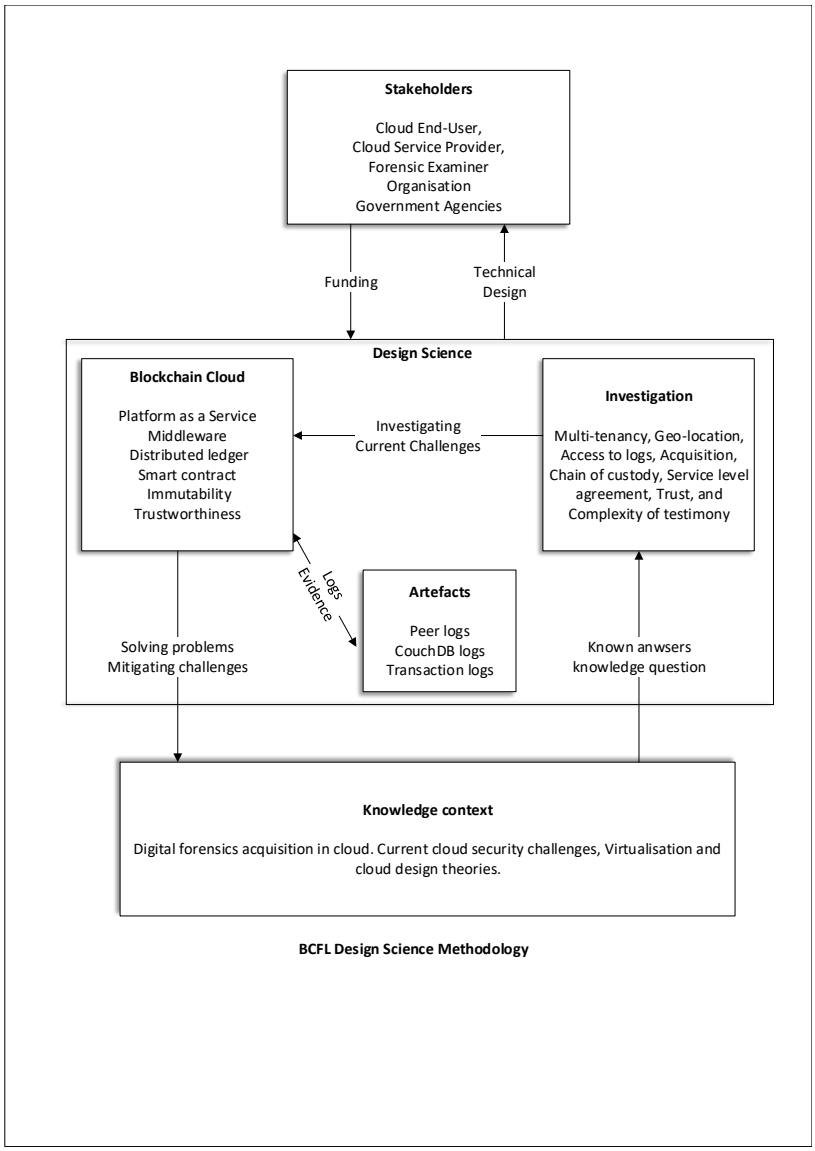

Fig. 3: BCFL Design Science Methodology

that is tamperproof and admissible in the court of law, which represents the stakeholders' goals. The method preserves log evidence integrity, trust and availability in the cloud ecosystem. It also secures the evidence throughout the investigation life circle. The stakeholder provides funding to achieve the goal of the investigation. The investigative box of the methodology captures all the challenges faced by cloud forensics investigators in acquiring admissible log evidence in the cloud ecosystem. The knowledge context section is the paper's main contribution, where we propose a Blockchain cloud Forensics Logging framework to solve the challenges of acquiring admissible log evidence in the cloud. In addition, the BCFL section is the proposed framework that uses Blockchain mechanisms to answer and solve the cloud digital forensic acquisition challenges. The difficulties in acquiring admissible evidence in the cloud ecosystem are immensely challenging apart from multi-tenancy factors; however, geopolitics add to this complexity as well. The main advantage of DSRM is that it can correct defects during the design and testing phase of our framework. The Artefacts section are where all the admissible logs can be accessible by the forensic investigator, cloud service providers and customer with user rights. Finally, the stakeholder's section addresses the design goals and budgetary issues.

Methodology Comparison

Table 3 compares different methodologies with the DSRM that enables cloud forensic investigators to acquire admissible log evidence from the cloud ecosystem. In addition to this, it is problematic to maintain an evidence chain of custody in the cloud due to lack of trustworthiness among cloud actors and the designed nature of the cloud, as highlighted by the NIST Cloud Computing Forensic Science Working Group (NCC FSWG). Furthermore, the cloud hypervisors nature has made it complicated for log evidence to be admissible in the cloud that stakeholder will rely on. The BCFL framework provides log transparency, trustworthiness among the cloud actors. This was achieved by using the distributed ledger mechanisms of Blockchain, the immutability of its logs and smart contract to preserve log evidence integrity and maintain chain of custody throughout the investigation process. In the current cloud ecosystem, the forensic investigator depends upon the cloud service providers (CSP) for access to logs. There are no approved standards of approach that can validate logs provided by the CSP's which unfortunately calls into question the integrity of the logs, even when the provided logs have valuable information, it should be admissible [16].

Table 3: Mitigating Digital Evidence Challenges in the Cloud Methodology Comparison

Contributions	Methods	**B**lockchain-Based Cloud Logging	**T**ransparency and Trustworthiness	**R**ecovering Evidence Deleted from the Cloud	**C**hain of Custody	**T**imestamp Synchronisation	**M**ulti-Tenancy and Geo-locations	Year
[25]	Provchain:A Blockchain-based data provenance architecture	✓	✓	✓	-	✓	-	2017
[54]	Semantic-based methodology for digital forensics analysis.	-	✓	-	✓	-	-	2020
[55]	Blockchain-based lawful evidence management	✓	✓	-	-	✓	-	2020
[16]	Forensics enabled cloud through secure logging-as-a-service	-	✓	-	-	✓	✓	2015
BCFL	A DSRM Blockchain Cloud Forensic Logging Method	✓	✓	✓	✓	✓	✓	2020

DSRM Activity Theory Design and Development Stages

Fig. 4 shows the design and development stage of the simulation of the Blockchain cloud ecosystem. The first stage enables trustworthiness and transaction log integrity through the application of Blockchain distributed ledger technology. The fabric provides channel mechanisms that support and facilitate a more secure cloud ecosystem. The second stage is creating a smart contract or chaincode that enables only authorised members with the contract to have access to application or logs. The third stage is the deployment of the supply chain smart contract to all peers, and each peer then maintains a copy of the distributed ledger. This enables a more balanced agreement between cloud service providers and cloud customers. The fourth stage sees the initialisation of the smart contract

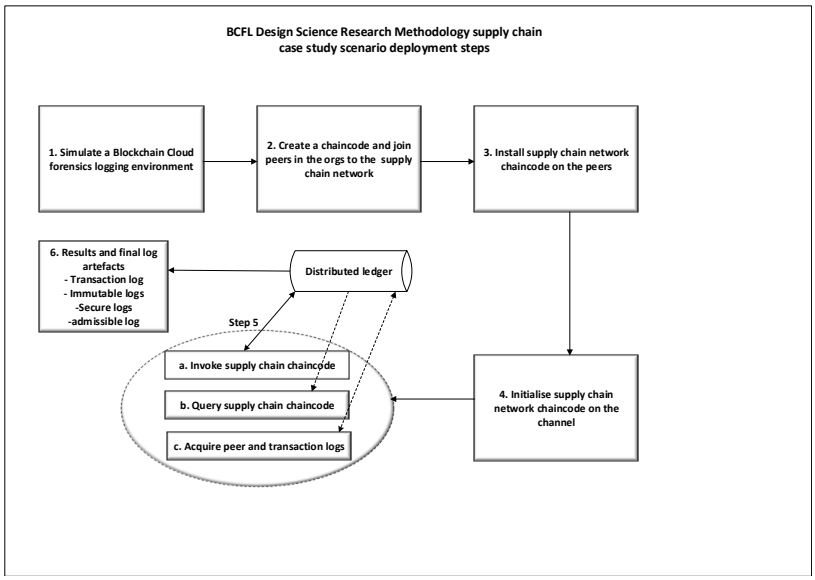

Fig. 4: Design and Development Phase For Simulated BCFL DSRM

on the channel mechanisms that enable and maintain transaction log integrity and its immutability. The distributed ledger in the fifth stage is used to invoke and query the chaincode. It uses its chain of blocks to provide another layer of security through consensus mechanisms that facilitate transparency and trustworthiness. The final stage is where the transaction is sent to the smart contract to update the ledger, which is an invocation. It also reads the current state of the ledger, known as the query, as this will support and facilitate the acquisition of admissible log evidence in the cloud ecosystem.

3.1. Log Evidence Investigation Processes

System logs are an essential source of digital evidence which are accessible by digital forensic investigators in traditional networks. However, accessing these is more challenging in the cloud ecosystem due to lack of ownership or full user right between the Cloud Service Providers (CSP), and cloud customers, which has led to a lack of transparency, trust in and integrity of log evidence [17], [56]. The different types of log evidence, from application logs to system security logs and audit logs, play a crucial role as evidence sources. For example, the system security logs can help the investigator reconstruct the crime scene and identify the particular suspect who took action on a precise system with timestamps. Application logs record activity created by the applications along with errors, warnings and other functional faults of the applications. Another complexity in acquiring digital evidence from a cloud ecosystem could arise from the cloud's architectural design.

For instance, the investigators need ascertained imaging and chain of custody of evidence from the hypervisor or virtual machine layer. To acquire more information on service errors, one can easily browse log files for clues involving the specific request ID. However, If the VM is ever shut down, then the entire system, including logs, can also be destroyed and never recovered [57]. Forensic investigators use a process to acquire digital evidence from a network by securing the crime scene, such as compromised computers or network devices. They then make copies of logs, disks, other digital artefacts and access logs as needed to support or refute the supposed criminal activity. They finally provide authenticated copies of full logs to the requesting attorneys or law enforcement agencies as required. Furthermore, in the UK, digital forensic investigators must adhere to the four principles of the Association of Chief Police Officer (ACPO) [58] digital forensic investigation guide. As explained above, the different cloud technology architecture poses challenges to these processes, but Blockchain has emerged as a technology to mitigate these challenges. The immutability and integrity of data in which a record of transactions made in the Blockchain ecosystem are maintained across several distributed nodes linked in a peer-to-peer network, [59]. Fig. 5 demonstrates how BCFL logging can be adapted in the current cloud forensic evidence acquisition process to solve the challenges faced by cloud forensics investigators. This is accomplished by using Blockchain distribution ledger technology to eliminate the geo-location, multi-tenancy, and political challenges that add layers of complexity in acquiring digital evidence in the cloud ecosystem.

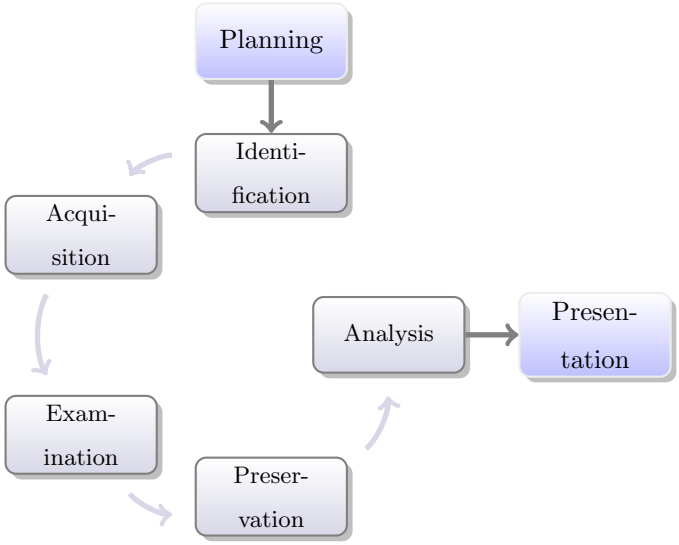

Fig. 5: Blockchain Cloud Forensics Log Investigation Process

4. Hyperledger Fabric

Hyperledger Fabric is a Permissioned Blockchain that was designed around some essential elements and use-cases that were seen as vital for organisational users. As highlighted in Table 4, the centre of the design is the ledger, which holds sets of transaction blocks. A transaction can be defined as the fundamental mechanisms that update the current status of the Blockchain. In turn, the transaction mechanism is facilitated by smart contract program codes installed on the Blockchain known as Chaincode [60]. It is vital to understand how the blocks and transactions are formed. Each block is arranged in a sequence and made up of established transactions that enable secure transactions and trust in the formation. The transactions are then stored in a precise, controlled series.This is in contrast to Permissionless Blockchain, where the creation of the transaction and the sequence is given and not primarily done at the same time or on the same computer. This is because the ordering and the execution of transactions are separated. One of the essential points to note in the permissioned Blockchain technology is the formation of its transaction block mechanisms. Blockchain blocks are sequentially organised in a way such that each of the blocks has the transaction details of the block before it and also to enable systematic storage of all transactions. In Hyperledger Fabric, the computers being used to operate the Blockchain can run in three different modes (node types):

Client: The primary function of the client application in the Hyperledger Fabric ecosystem is to ensure and maintain the notification mechanisms of all the blocks that are added to the Blockchain ledger. It also ensures all the peers and participants in the ecosystem systematically have this information.

Peer: The peer's primary function is to indicate the communication status of the Blockchain ledger and facilitate all transactions and manage the chaincode algorithm. Most importantly, it maintains the communication status of all the participants and peers in the Blockchain ecosystem.

The peer can frequently act as a committer, execute a transaction or even verify the endorsement and authenticate the transaction. Thus, the peer is a fundamental mode of the Hyperledger Fabric as it manages all events and presents these events to all participants in the Blockchain ecosystem.

Orderer: The ordering service's primary function is to ensure all transactions reach the peers by arranging all Blockchain transactions into the block and shipping them to peers. One can say it is the backbone of the Blockchain network as it manages transactions for the peers and application and sets up authentication policies for the reader, writers, and admin to ensure a secure communication pathway. Again, one of its most important functions is the management of the pluggable trust engine, for example, the Byzantine fault-tolerant (BFT), as it facilitates their transactions.

Table 4: Hyperledger Fabric Business Blockchain Components

Blockchain Component	Core Functions and Responsibilities
Shared Ledger	A Permissionless Blockchain such as that used in Bitcoin enables transaction visibility by replicating a shared copy of the transaction to all participants.
Smart Contract	In a Blockchain ecosystem, the smart contract or chaincode is a programmed business agreement embedded with the transaction record and executed with the rule defined by the business.
Privacy	Cryptography is used to maintain a secure transaction in the Blockchain ecosystem. It facilitates secure authentication and verification of all transactions. To maintain data privacy and security in the Blockchain, immutability, endpoint visibility and tamper-proof logging mechanisms are incorporated.
Trust	Blockchain establishes a trust mechanism by adding the ledger with appropriate confidentiality and ensures that all participants, transactions and assets are verifiable. It also maintains an immutable transaction audit trail of all events as trust is essential in any Blockchain ecosystem.

Fabric Certificate Authority (CA): The authority is vital to facilitate Public Key Infrastructure (PKI-based) certificates to Hyperledger Fabric network participants and supports the Lightweight Directory Access Protocol (LDAP) secure authentication and Hardware Security Module (HSM). It uses the root CA to provide a secure enrolment mechanism for all participants in the

permissioned Blockchain ecosystem.

4.1. Blockchain Cloud Forensic Logging Framework

The Hyperledger Fabric supports the concept of a channel, which is a separate Blockchain that enables a secret transaction. For example, the channel mechanisms in Hyperledger Fabric Blockchain will mitigate the problem of multi-tenancy in the current cloud ecosystem. Each Fabric client can be deployed to utilise a different communication channel, as demonstrated in the framework shown in Fig. 6.

The distributed ledger technology plays an indispensable role in resolving the current challenges faced by forensic investigators in acquiring digital evidence in the cloud environment. This is because of the use of peers, each of whom stores an immutable copy of the ledger, which enhances transaction data integrity, immutability and trustworthiness at all times throughout the transaction circle. Another essential component of Hyperledger Fabric architecture is the chaincode.

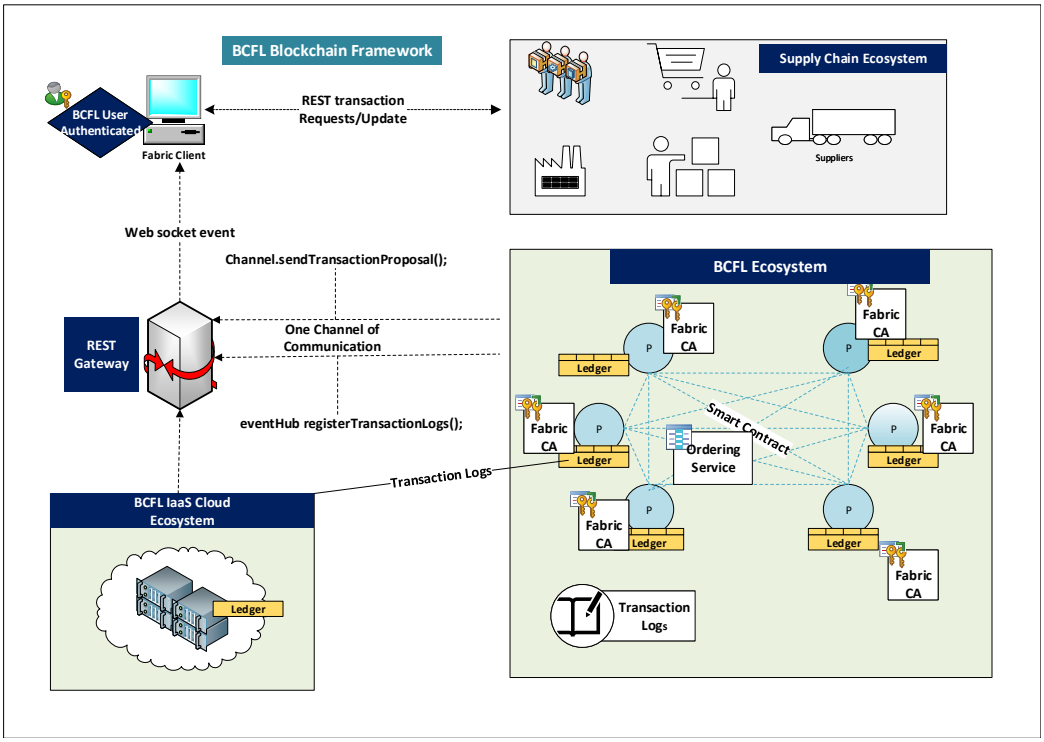

Fig. 6: BCFL Framework

Chaincode implements a business logic, which enables good communication between all the parties in our BCFL environment. The functionality is entrusted to client requests to invoke a transaction, provided they possess the correct Fabric membership service certificate [61].

The endorsing Fabric peer manages the lifetime of the chaincode, and the transaction requests [60]. In response to client requests, the chaincode queries and updates the ledger and generates a transaction proposal using the Fabric SDK to the BCFL network. The endorser validates the

transaction and sends it back to the Fabric client with the signature and together with the read-write record of the block, which includes all the records of the read-write of the operation which completes the validation, [60]. It also includes all the Blockchain records that were read or written during the transaction's execution. When the Fabric client accumulates enough transactions, it can then forward them to the orderer. The orderer verifies the endorsement if successful it then sends it to the peers. The peers view all the latest proceedings and make a decision on which ones are valid to add to our BCFL. Finally, it informs all the Fabric clients of the current outcome of their proceedings. If there is sufficient endorsement, the transaction is added to the simulated BCFL cloud network.

In addition, due to Fabric's decentralised architecture, the categorisation of transaction's execution can be governed and committed differently in the different Fabric components, which include the endorsers, orderers, and committees, which in turn brings in a timestamp between the deliberation and the assurance of the transaction, within which critical collision can happen. Furthermore, Fig.7 demonstrates how Blockchain technology supports secure logging and provides trustworthiness and immutability of log evidence using distributed ledger technology.

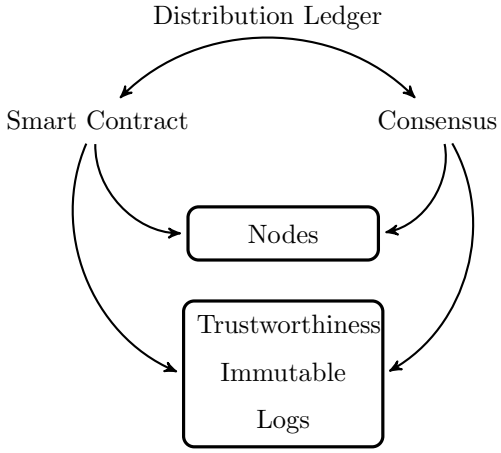

Fig. 7: Blockchain Trustworthiness

4.2. Participants Interaction with BCFL

Participants constitute one of the original core event components that interact with the Hyperledger Fabric Blockchain. On the current cloud ecosystem, participants are the same as cloud customers, who rate a particular service from the cloud service providers. In the case of Blockchain, the architecture participants play a specific part in the network as they control the most data. Even so, in our case, BCFL participants might be unaware that they are interacting with our BCFL Blockchain cloud network.

The members of the supply-chain interact with the Blockchain through Fabric SDK and use the HTTP protocol to access the BCFL resource. Critically, they are doing so on behalf of their

organisations as they are the organisations' agents. Likewise, when it comes to system and device participants, it is unlikely that devices will host a copy of the Blockchain ledger. In this way, devices are a little more like individual participants. Blockchain cloud integration could solve the challenges associated with service level agreement (SLA). It was a unilateral agreement that does not protect the interest of cloud customers in the digital forensic investigation process [62]. However, the Hyperledger Fabric membership service agreement has solved this problem as each network member has equal right through a distributed ledger technology.

The current supply-chain cloud ecosystem has faced challenges in the area of trust, transparency, data integrity, traceability of order and shipment [63], [64]. The different actors that make up the supply chain from the raw material, supplier, manufacturer, distributor, retailer and the customer have found it challenging to establish trust between their different domains in the current cloud ecosystem as highlighted in Fig. 8. These have led to a lack of confidence in transaction processes as each actor is protecting their trade secrets. This is due to the current system can not provide trust and transparency. Furthermore, clear visibility of the supply-chain ecosystem is needed to maintain data integrity and transparency across all domains. The BCFL Blockchain framework will solve this problem by providing endpoint visibility of all the network nodes. An organisation needs to have a forensics readiness plan to investigate an incident and bring the adversary to justice, [26]. For example, a media report has highlighted that the United States (US) retail food giant Walmart has launched Hyperledger Fabric Blockchain food retail to facilitate traceability of food items [65].

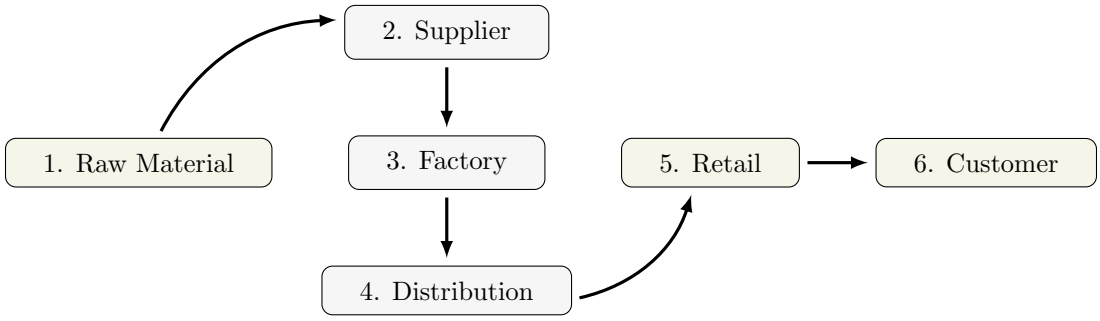

Fig. 8: BCFL Supply-Chain

Algorithm

The Hyperledger Composer REST server was used to facilitate an endpoint API that interacts with the BCFL ecosystem. This enables an authorised client to access simulated BCFL cloud resources through a secure REST server endpoint Application Program Interface (API). It also ensures transaction integrity through a signed certificate. As demonstrated on the BCFL Pseudo Code RESTFUL Server Algorithm 1, a successful client authentication generates code 200 while

unsuccessful client authentication on the system will throw up a 401 code error.

Algorithm 1: Pseudo Code for BCFL RESTFUL Server Algorithm

```
Data: Connect to composer REST Server (s)
//submit a GET request
Result: generate = httpRequest.send("GET",locathost:3000);
if generate.code = = 200 then
    Successful system authentication
else
    (generate.code s = 401)
    Server authorisation error
    Update Hyperledger Fabric chaincode
end
```

Simulating the BCFL Environment

The virtualised hybrid lab was designed, built and deployed on a Window 10 enterprise operative system, 64-bit with 1TB HDD and 32GB RAM. This deployment's first step was to login into the Window 10 operative system (OS) as a system administrator. Following that, the directory containing the downloaded installer file was selected from the Window start menu. Further administrative right permission was granted to install the VMware workstation 15.0. The software license agreement was accepted, and the installation directory was specified. All the default steps were then taken to the end. This installation process was carried out to mimic a cloud ecosystem that will enable us to perform the research experiment. In addition, other commercial cloud infrastructures would not fit this experiment's purpose as there are limitations such as firewall rules and user service level agreements that need to be adhered to. After installing Linux Ubuntu 20.04 in the VMware virtual environment, then continued with the installation of Hyperledger Fabric Blockchain locally on the virtualised Ubuntu 20.04. The following computer resources were allocated to the virtualised Ubuntu OS, 32GB RAM and 500GB HDD from the Microsoft Window 10 host operating system (OS). The computer resources should be sufficient to run the Hyperledger Fabric and Docker components on top of the Ubuntu virtual machine (VM). Finally, the BCFL logging algorithm was integrated to enhance and strengthen Blockchain forensic capability.

4.3. BCFL Single-case mechanism experiments Scenario

Single-case mechanism experiments enable simulation of the scenario presented by a model of Blockchain cloud context. The experiment was conducted in a virtual lab environment, as earlier mentioned 4.2. The scenario was simulated to capture and observe the mechanisms, evaluate, draw conclusions and view test results as demonstrated in the next section.

Scenario

Alice is the director of Tag Shop in a thriving high street chain with excellent online visibility. Tag Shop is running a Hyperledger Fabric Blockchain network and has VMs workstation and server rented from the cloud service provider (CSP) for day to day running of the business. However, Tag Shop just hired a new system administrator called Bob, whose responsibility is to maintain the system and update applications when necessary. During a system update, Bob accidentally deleted a week's worth of transactions and one VM. This incident had negatively impacted Alice's business in terms of profit and reputation. Consequently, Alice hired a digital forensic company (ACMD Ltd) to investigate and recover all deleted VM transactions. After analysing the Blockchain logs, forensic investigators were able to reconstruct how the incident happened. The forensic investigators looked at the following steps to solve the case:

Digital Forensic Investigation and Result: In forensics, it is vital to maintain data and evidence integrity at all times. The investigation in this scenario establishes that Hyperledger Fabric Blockchain uses hashing, encryption and immutability to maintain log evidence integrity and preserve evidence chain of custody.

In a cloud ecosystem, defining and securing the digital crime scene could be problematic due to the multi-tenancy, geo-locality and GDPR compliance. However, as shown on the acquired digital log evidence in Fig. 9, the Hyperledger chaincode maintains a secured, accurate and immutable timestamp.

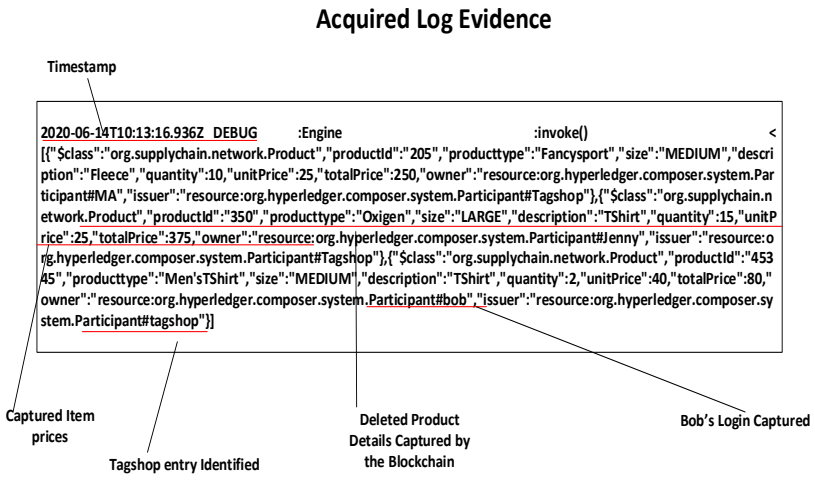

Fig. 9: BCFL Supply-Chain Case-study Log Evidence

All Bob's transaction entries ID's were acquired by Alice's hired forensic investigators, as high-

lighted on the evidence snapshot. The acquired digital log evidence also highlights BCFL's capability to enabling effective traceability to forensic readiness mechanisms in the supply-chain ecosystem.

4.4. Digital Forensic Investigation

Evidence Preservation and Chain of Custody: Throughout the investigation, the chain of custody was maintained. The most important part of the investigation is how BCFL enables a log filtering mechanism that facilitates real-time evidence acquisition that does not interfere with the daily running of Tag Shop's business operations. The Tag Shop case Table, 5 highlights the chain of custody and how it was maintained throughout the investigation process by ACMD Ltd. Even when the investigation is over and evidence destroyed or returned. An entry will still be made on the chain of custody form to identify all actions taken by investigators. ACMD also included the chain of custody entries in their report, which highlights all log evidence that was acquired as part of evidence reconstruction and admissibility. Thus, the case study has proven that integrating Blockchain in the cloud ecosystem will mitigate many of the challenges faced by digital forensic investigators and police first responders in ensuring the admissibility of digital evidence from the cloud ecosystem.

Table 5: BCFL Framework Scenario: CHAIN OF CUSTODY

Tracking No:	Date/Time:	From:	TO:	Reason:
1	Date:14-06-20 Time:10:13 am	ACMD Ltd John Smith Signature N/A	Name Org: Jo Brown /ACMD Ltd. Signature J.Brown	Log Evidence Seizure from Tagshop Cloud Blockchain Network
2	Date:14-06-20 Time:10:40 am	Mark Johnson/ACMD Ltd Signature M.Johnson	Name ON: Evidence locker/ ACMD Signature N/A	ACMD Cloud Blockchain Secure Storage

4.5. Performance Metrics

Elasticsearch, Logstash and Kibana (ELK) is open source software used for real-time system monitoring and components system application performance monitoring as shown in Fig. 10, Fig. 11, and Fig. 12. The integration of ELK into our framework supports real-time performance monitoring and analysis. It has a data channel or pipeline mechanism that processes data from multiple end nodes simultaneously, transforms it and forwards it to Elasticsearch for further processing.

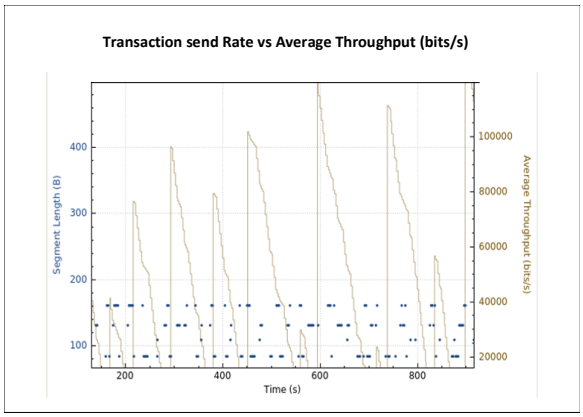

Fig. 10: Transaction Rate Throughput

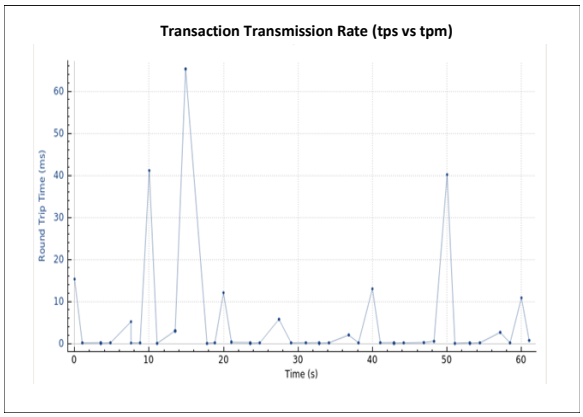

Fig. 11: Transaction Rate tps

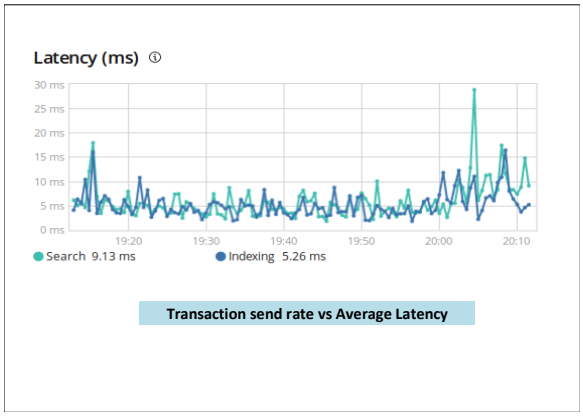

Fig. 12: Transaction Rate tps vs Latency

Kibana visualisation dashboard gives us a holistic performance view of the CPU and memory usage in a graphical format. ELK performance measurement technology has therefore facilitated our framework. For example, suppose any peer or node in our BCFL goes down. In that case, the system administrator can activate the forensic readiness plan and respond to the cyber incident in

real-time. A vital element of the incident response plan is the use of escalation procedures. The monitoring of average throughput performance metrics enables a more unobstructed view of how the send transaction rates are recorded in second and minutes.

5. Limitation

Permissioned and permissionless Blockchain technology is at its infant stage. It can facilitate decentralised smart logging mechanisms that ensure data security in transit and storage compared to the traditional centralised cloud logging mechanisms. Although at this early stage of Blockchain technology is useful to highlight its limitations as demonstrated by [66, 67] before deploying the technology in the operational environment.

- Operational Environment: This research experimental case study was carried out on a virtualised cloud network and has not been tried in an operational cloud environment. However, the BCFL implementation mimics the real operational environment with a real permissioned (Hyperledger Fabric) Blockchain technology and a VMware cloud platform.

- Legal Framework: There is no global standard framework for adopting Blockchain into an organisation existing network infrastructure. Lack of standards has delayed potential businesses to secure data logging, monitoring, and storage, including data decentralisation mechanisms that Blockchain offers [68, 69].

- Limited Flexibility: Blockchain immutability mechanisms ensure tamperproof of all transactions within the Blockchain consensus mechanisms. The immutability mechanisms have prevented legitimate use cases that need some level of changes to the transaction data.

6. Conclusion and Future work

Cloud computing offers customers on-demand shared resources in a virtual environment where human intervention is highly limited with benefits such as cost efficiency, scalability, agility, convenience and elasticity. However, this comes with risk, threats and challenges identified by cloud stakeholders, which have been exploited by cybercriminals, and which, in turn, add another layer of complexity in the cloud forensic investigations. With the involvement of cloud computing, as many organisations have adopted the technology, there is a need to define a forensic process technique suited for a cloud ecosystem that can create trustworthiness and preserve log evidence integrity both on transit and in storage in the cloud. We propose that a Blockchain cloud as a service platform incorporating our BCFL will resolve difficulties in cloud forensic investigation and will support the investigator, including the administrator, in real-time forensic analysis. Our BCFL framework establishes how participants interact with the assets and then understand how transaction logs can

be used as forensic evidence in the Blockchain cloud ecosystem. Little attention has been paid to GDPR compliance where the cyber incident first responders, such as law enforcement agencies, tread carefully in securing the crime scene and maintain chain of custody and also have GDPR compliance to deal with in order to avoid contamination of digital evidence. In this paper, we have provided a BCFL methodology and framework that will mitigate the challenges faced by digital forensic investigators in acquiring admissible log evidence from the cloud ecosystem.

Future works will focus on developing an innovative framework that integrates Blockchain and Artificial intelligence (AI) in the cloud ecosystem to enhance digital forensic investigation, system monitoring, endpoint visibility and traceability.

References

[1] X. Han, N. Kheir, D. Balzarotti, The role of cloud services in malicious software: Trends and insights, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2015, pp. 187–204.

[2] C. Hooper, B. Martini, K.-K. R. Choo, Cloud computing and its implications for cybercrime investigations in australia, Computer Law & Security Review 29 (2) (2013) 152–163.

[3] A. Pichan, M. Lazarescu, S. T. Soh, Cloud forensics: Technical challenges, solutions and comparative analysis, Digital Investigation 13 (2015) 38–57.

[4] B. Manral, G. Somani, K.-K. R. Choo, M. Conti, M. S. Gaur, A systematic survey on cloud forensics challenges, solutions, and future directions, ACM Computing Surveys (CSUR) 52 (6) (2019) 1–38.

[5] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, M. Villari, An approach for the secure management of hybrid cloud–edge environments, Future Generation Computer Systems 90 (2019) 1–19.

[6] N. H. Ab Rahman, W. B. Glisson, Y. Yang, K.-K. R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Computing 3 (1) (2016) 50–59.

[7] J. Krystlik, With gdpr, preparation is everything, Computer Fraud & Security 2017 (6) (2017) 5–8.

[8] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, X. Zhang, Bbds: Blockchain-based data sharing for electronic medical records in cloud environments, Information 8 (2) (2017) 44.

[9] C. Pahl, Containerization and the paas cloud, IEEE Cloud Computing 2 (3) (2015) 24–31.

[10] C. Stelly, V. Roussev, Scarf: A container-based approach to cloud-scale digital forensic processing, Digital Investigation 22 (2017) S39–S47.

[11] M. N. K. Boulos, J. T. Wilson, K. A. Clauson, Geospatial blockchain: promises, challenges, and scenarios in health and healthcare (2018).

[12] T. Prakash, M. Kakkar, K. Patel, Geo-identification of web users through logs using elk stack, in: 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), IEEE, 2016, pp. 606–610.

[13] S. J. Son, Y. Kwon, Performance of elk stack and commercial system in security log analysis, in: 2017 IEEE 13th Malaysia International Conference on Communications (MICC), IEEE, 2017, pp. 187–190.

[14] C. P. Garrison, Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data, Syngress, 2010.

[15] J. Cucurull, J. Puiggalí, Distributed immutabilization of secure logs, in: International Workshop on Security and Trust Management, Springer, 2016, pp. 122–137.

[16] S. Zawoad, A. K. Dutta, R. Hasan, Towards building forensics enabled cloud through secure logging-as-a-service, IEEE Transactions on Dependable and Secure Computing 13 (2) (2015) 148–162.

[17] D. Birk, C. Wegener, Technical issues of forensic investigations in cloud computing environments, in: 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE, 2011, pp. 1–10.

[18] M. E. Alex, R. Kishore, Forensics framework for cloud computing, Computers & Electrical Engineering 60 (2017) 193–205.

[19] C. D. Weissman, S. Bobrowski, The design of the force. com multitenant internet application development platform, in: Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, ACM, 2009, pp. 889–896.

[20] R. Marty, Cloud application logging for forensics, in: proceedings of the 2011 ACM Symposium on Applied Computing, 2011, pp. 178–184.

[21] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, R. Chen, Nutbaas: A blockchain-as-a-service platform, Ieee Access 7 (2019) 134422–134433.

[22] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles, IEEE Communications Magazine 56 (10) (2018) 50–57.

[23] E. Nyaletey, R. M. Parizi, Q. Zhang, K.-K. R. Choo, Blockipfs-blockchain-enabled interplanetary file system for forensic and trusted data traceability, in: 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 18–25.

[24] A. H. Lone, R. N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer, Digital Investigation 28 (2019) 44–55.

[25] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, IEEE Press, 2017, pp. 468–477.

[26] B. Putz, F. Menges, G. Pernul, A secure and auditable logging infrastructure based on a permissioned blockchain, Computers & Security 87 (2019) 101602.

[27] Z. Tian, M. Li, M. Qiu, Y. Sun, S. Su, Block-def: A secure digital evidence framework using blockchain, Information Sciences 491 (2019) 151–165.

[28] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation computer systems 28 (3) (2012) 583–592.

[29] M. Hogan, F. Liu, A. Sokol, J. Tong, Nist cloud computing standards roadmap, NIST Special Publication 35 (2011) 6–11.

[30] M. Ali, S. U. Khan, A. V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information sciences 305 (2015) 357–383.

[31] A. N. Moussa, N. Ithnin, A. Zainal, Cfaas: bilaterally agreed evidence collection, Journal of Cloud Computing 7 (1) (2018) 1–19.

[32] S. Simou, C. Kalloniatis, S. Gritzalis, H. Mouratidis, A survey on cloud forensics challenges and solutions, Security and Communication Networks 9 (18) (2016) 6285–6314.

[33] H. N. Noura, O. Salman, A. Chehab, R. Couturier, Distlog: A distributed logging scheme for iot forensics, Ad Hoc Networks 98 (2020) 102061.

[34] D. Quick, K.-K. R. Choo, Big forensic data reduction: digital forensic images and electronic evidence, Cluster Computing 19 (2) (2016) 723–740.

[35] K. Salah, M. H. U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for ai: Review and open research challenges, IEEE Access 7 (2019) 10127–10149.

[36] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Tech. rep., Manubot (2019).

[37] M. Tang, M. Alazab, Y. Luo, Big data for cybersecurity: Vulnerability disclosure trends and dependencies, IEEE Transactions on Big Data 5 (3) (2017) 317–329.

[38] M. Lemoudden, B. El Ouahidi, Managing cloud-generated logs using big data technologies, in: 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, 2015, pp. 1–7.

[39] S. NIST, 800-145: The nist definition of cloud computing (2012).

[40] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, J. Xu, Multi-tenancy in cloud computing, in: 2014 IEEE 8th International Symposium on Service Oriented System Engineering, IEEE, 2014, pp. 344–351.

[41] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, S. Mangard, Malware guard extension: Using sgx to conceal cache attacks, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2017, pp. 3–24.

[42] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, R. Buyya, Ddos attacks in cloud computing: Issues, taxonomy, and future directions, Computer Communications 107 (2017) 30–48.

[43] S. Venkatraman, M. Alazab, Use of data visualisation for zero-day malware detection, Security and Communication Networks 2018 (2018).

[44] K. Ruan, J. Carthy, T. Kechadi, I. Baggili, Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, Digital Investigation 10 (1) (2013) 34–43.

[45] T. Islam, D. Manivannan, S. Zeadally, A classification and characterization of security threats in cloud computing, Int. J. Next-Gener. Comput 7 (1) (2016).

[46] S. Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system.(2008) (2008).

[47] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. Kayes, M. Alazab, P. Watters, A comparative analysis of distributed ledger technology platforms, IEEE Access 7 (2019) 167930–167943.

[48] J. Li, J. Wu, L. Chen, Block-secure: Blockchain based scheme for secure p2p cloud storage, Information Sciences 465 (2018) 219–231.

[49] M. Berberich, M. Steiner, Blockchain technology and the gdpr-how to reconcile privacy and distributed ledgers, Eur. Data Prot. L. Rev. 2 (2016) 422.

[50] R. J. Wieringa, Design science methodology for information systems and software engineering, Springer, 2014.

[51] H. Takeda, P. Veerkamp, H. Yoshikawa, Modeling design process, AI magazine 11 (4) (1990) 37–37.

[52] K. Peffers, T. Tuunanen, M. A. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, Journal of management information systems 24 (3) (2007) 45–77.

[53] A. Dresch, D. P. Lacerda, J. A. V. Antunes, Design science research, in: Design Science Research, Springer, 2015, pp. 67–102.

[54] F. Amato, A. Castiglione, G. Cozzolino, F. Narducci, A semantic-based methodology for digital forensics analysis, Journal of Parallel and Distributed Computing 138 (2020) 172–177.

[55] M. Li, C. Lal, M. Conti, D. Hu, Lechain: A blockchain-based lawful evidence management scheme for digital forensics, Future Generation Computer Systems (2020).

[56] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie, Cloud forensics, in: IFIP International Conference on Digital Forensics, Springer, 2011, pp. 35–46.

[57] S. Rane, A. Dixit, Blockslaas: Blockchain assisted secure logging-as-a-service for cloud forensics, in: International Conference on Security & Privacy, Springer, 2019, pp. 77–88.

[58] D. Reilly, C. Wren, T. Berry, Cloud computing: Pros and cons for computer forensic investigations, International Journal Multimedia and Image Processing (IJMIP) 1 (1) (2011) 26–34.

[59] W. Viriyasitavat, T. Anuphaptrirong, D. Hoonsopon, When blockchain meets internet of things: characteristics, challenges, and business opportunities, Journal of industrial information integration (2019).

[60] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, ACM, 2018, p. 30.

[61] C. Cachin, et al., Architecture of the hyperledger blockchain fabric, in: Workshop on distributed cryptocurrencies and consensus ledgers, Vol. 310, 2016, p. 4.

[62] K. Saravanan, M. Rajaram, An exploratory study of cloud service level agreements-state of the art review., KSII Transactions on Internet & Information Systems 9 (3) (2015).

[63] N. Gaur, L. Desrosiers, V. Ramakrishna, P. Novotny, S. A. Baset, A. O'Dowd, Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer, Packt Publishing Ltd, 2018.

[64] R. Azzi, R. K. Chamoun, M. Sokhn, The power of a blockchain-based supply chain, Computers & industrial engineering 135 (2019) 582–592.

[65] P. Olsen, M. Borit, S. Syed, Applications, limitations, costs, and benefits related to the use of blockchain technology in the food industry, Nofima rapportserie (2019).

[66] V. J. Morkunas, J. Paschen, E. Boon, How blockchain technologies impact your business model, Business Horizons 62 (3) (2019) 295–306.

[67] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, V. Akella, Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda, International Journal of Information Management 49 (2019) 114–129.

[68] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, International Journal of Production Research 57 (7) (2019) 2117–2135.

[69] M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani, A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors, International Journal of Information Management 50 (2020) 302–309.