Digital Investigation 28 (2019) 44–55

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer

Auqib Hamid Lone*, Roohie Naaz Mir

Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, 190006, India

ARTICLE INFO

Article history:
Received 4 September 2018
Received in revised form
1 January 2019
Accepted 2 January 2019
Available online 10 January 2019

Keywords:
Evidence integrity
Digital forensics
Chain of custody
Permissioned blockchain
Hyperledger Composer

ABSTRACT

Advancements in Information Technology landscape over the past two decades have made the collection, preservation, and analysis of digital evidence an extremely important tool for solving cybercrimes and preparing court cases. Digital evidence plays an important role in cybercrime investigation, as it is used to link individuals with criminal activities. Thus it is of utmost importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy in the chain of custody during cybercrime investigation. Modern day technology is more advanced in terms of portability and power. A huge amount of information is generated by billions of devices connected to the internet that needs to be stored and accessed, thus posing great challenges in maintaining the integrity and authenticity of digital evidence for its admissibility in the court of law. Handling digital evidences poses unique challenges because of the fact they are latent, volatile, fragile, can cross jurisdictional borders quickly and easily and in many cases can be time/machine dependent too. Thus guaranteeing the authenticity and legality of processes and procedures used to gather and transfer the evidence in a digital society is a real challenge. Blockchain technology's capability of enabling comprehensive view of transactions (events/actions) back to origination provides enormous promise for the forensic community. In this research we proposed Forensic-Chain: A Blockchain based Digital Forensics Chain of Custody, bringing integrity and tamper resistance to digital forensics chain of custody. We also provided Proof of Concept in Hyperledger Composer and evaluated its performance.

Introduction

In todays ever-growing digital world with the rapid increase in cybercrimes, digital evidence is gaining more and more importance, because it is used to prove facts or to convict personnel involved in cybercrimes. Therefore, it is of extreme importance to ensure the integrity of digital evidence during its whole lifecycle in any forensic investigation. According to Richter et al. (2010) digital evidence is considered admissible in the court of law if it meets following criteria, viz: authentic, complete, reliable and believable. Furthermore (Schatz, 2007) mentions two important aspects for the admissibility of digital evidence in the court of law: legal aspects (authentic, accurate and complete) and technical aspects (transparent, explainable and chain of evidence). Digital evidence is very hard to handle and preserve compared to physical evidence because of the characteristics like 1) easy to transmit and is fragile in nature 2) vulnerable to tampering and removal 3) time sensitiveness and ability to cross borders and legal jurisdictions on the fly. Thus digital evidence comes with its own unique challenges related to chain of custody because of complex and volatile nature.

Digital Forensic Chain of custody (CoC) can be defined as a process used to maintain and document the chronological history of handling digital evidence (Giova, 2011a). CoC plays an important role in any digital forensic investigation because it records every minute detail pertaining to digital evidence during its passage through different levels of hierarchy i.e. from the first responder to higher authorities responsible for handling cybercrime investigation. CoC logs the information like how evidence was gathered, analysed and preserved for production, when, where and who came in contact with the evidence etc. However, Forensic CoC is susceptible to compromise if documentation is not properly maintained and preserved during the lifecycle of digital evidence, thus making it inadmissible in the court of law to prove any fact related to cybercrime. Thus it is extremely important to preserve

* Corresponding author.
E-mail addresses: ahl@nitsri.net (A.H. Lone), naaz310@nitsri.net (R.N. Mir).

https://doi.org/10.1016/j.diin.2019.01.002
1742-2876/© 2019 Elsevier Ltd. All rights reserved.

the integrity of digital forensic CoC for the evidence to be admissible in the court of law.

As a matter of fact, the need of the hour is to have a system that guarantees transparency, authenticity, security and auditability. Blockchain in its simplicity is a series of connected data structures called blocks, which contain or track everything that happens in any distributed systems on a peer to peer network. Each block is linked to the previous block with a special pointer called as hash pointer forming a chain, resulting in an append-only system: a permanent and irreversible history that can be used as a real-time audit trail by any participant to verify the accuracy of the records by simply reviewing data itself (Nakamoto). Blockchain by design guarantees transparency, authenticity, security and auditability and thus making it best fit for maintaining and tracing chain of custody for forensic applications (Lone and Mir, 2587).

Rest of the paper is organized as follows: Section 2 provides a brief background of Digital Forensics, Hyperledger Composer and Hyperledger Caliper and also discusses the feasibility of Blockchain for digital forensics chain of custody. Section 3 provides motivation behind the work. Section 4 presents the proposed Forensic-Chain with PoC in Hyperledger Composer. Section 5 provides a brief overview of previous attempts for improving Chain of Custody (CoC). Finally, section 6 concludes the paper and references are listed in the end.

Background

Digital forensics

Digital Forensics refers to the scientific process of identification, preservation, collection and presentation of digital evidence so that it is admissible in the court of law. As a matter of fact, any information that is stored or extracted from digital media can be a piece of digital evidence for analysis during the digital forensics investigation. The aim of any forensic investigation is to ensure that the discovered digital evidence is admissible in the court of law, therefore maintaining chain of custody is a critical requirement and must be established throughout the entire investigation process (Ćosić et al., 2011).

Chain of custody (CoC) refers to the process of documenting and maintaining the chronological history of handling digital evidence. Extreme care is required to protect CoC from being altered or destroyed unauthorizedly. The ultimate aim of CoC is to demonstrate that alleged evidence is, in fact, relevant to the alleged crimes instead of being falsely planted. Weak CoC leads to inadmissibility of digital evidence in the court of law.

The digital forensic investigation requires well-defined procedures that comply with industry standards, appropriate laws and organizational practices (Ami-Narh and Williams, 2008). Tools and techniques used by forensic investigators may vary but generally, investigative process involves planning, acquisition, preservation, analysis and reporting as summarized in Fig. 1.

Hyperledger Composer

Hyperledger Composer (Introduction — Hyperledge, 2018; Dhillon et al., 2017) is one of the popular and fastest growing projects hosted by The Linux Foundation. It is a framework as well as an open development toolset for developing Blockchain applications rapidly. Hyperledger Composer relatively smoothens the process of Blockchain use-case design and deployment and drastically reduce the development time from months to weeks. One of the several advantages of Hyperledger Composer is that it is fully open source with an open governance model that allows anyone to contribute towards the project.

Hyperledger Composer supports and resides on the top of existing Hyperledger Fabric Blockchain infrastructure and runtime, which allows for pluggable Blockchain consensus protocol to ensure that the transactions are validated according to the policy defined by the designated business network participants.

Hyperledger Composer provides a simplified domain-specific modeling language for modeling business network (Assets, Participants, and Transactions) and JavaScript for implementing transaction logic. Model files can be written in any development platform but a simple web-based tool called Composer- Playground simplifies the job by assisting in the development, packing, deployment, testing of the projects and a command line utility for scripting. Applications can be deployed to the instances of the Hyperledger Fabric or simulated locally in the web browser. Hyperledger Composer allows for creating web, mobile or native Node.js applications. Hyperledger Composer also includes composer-rest-server (Based on Loopback technology) to automatically generate REST API for business network and hyperledger-composer code generation plugin for Yeoman framework is used to generate a skeleton Angular application. Hyperledger Composer also has a rich set of JavaScript API's to build native Node.js applications (see Fig. 2).

Hyperledger Caliper

Hyperledger Caliper (GitHub, 2018) is a performance evaluation benchmark framework for Blockchain and is one of the several Hyperledger projects hosted by Linux Foundation. Caliper allows users to measure the performance of different Blockchain solutions with predefined set of use-cases and generate reports with a set of performance test results. Reports produced by Caliper contain a set of performance indicators such as transactions per second(tps), transaction latency, resource utilization etc. Caliper currently supports following Blockchain based solutions: Fabric, Sawtooth, Iroha and Composer.

Hyperledger Caliper architecture comprises three Node.js layers viz:

- Benchmark Layer: It contains predefined benchmark test cases and pluggable benchmark engine.
- Interface and Core Layer: It comprises of *Blockchain NBI* (collection of common Blockchain interfaces) for installing, invoking and querying Blockchain, *Resource Monitor* for monitoring resource (cpu, memory etc.) utilization, *Performance Analyzer* for analyzing performance indicators (latency, throughput etc.) and *Report generator* for generating html based reports. Caliper *NBI* provides operations that are required to communicate with backend Blockchain system. Furthermore *NBI* can be used to write tests for multiple Blockchain systems.
- Adaption Layer: It translates *Blockchain NBIs* into Blockchain (DLT) protocols.

Hyperledger Caliper works in multiple phases. Starting phase being Preparation phase wherein test context is prepared by installing smart contracts. The second phase is Tests Execution phase where tasks are assigned to clients for running predefined test cases which can either be transaction count based or duration based. The final phase is Performance Analysis phase where all the test results are gathered for report generation.

Blockchain feasibility test for digital forensics chain of custody

To determine whether a Blockchain is a viable solution for maintaining digital forensics chain of custody, we performed Blockchain feasibility test by seeking answers to the questions proposed by Wüst and Gervais (2017) pertaining to requirements of digital forensics chain of custody:

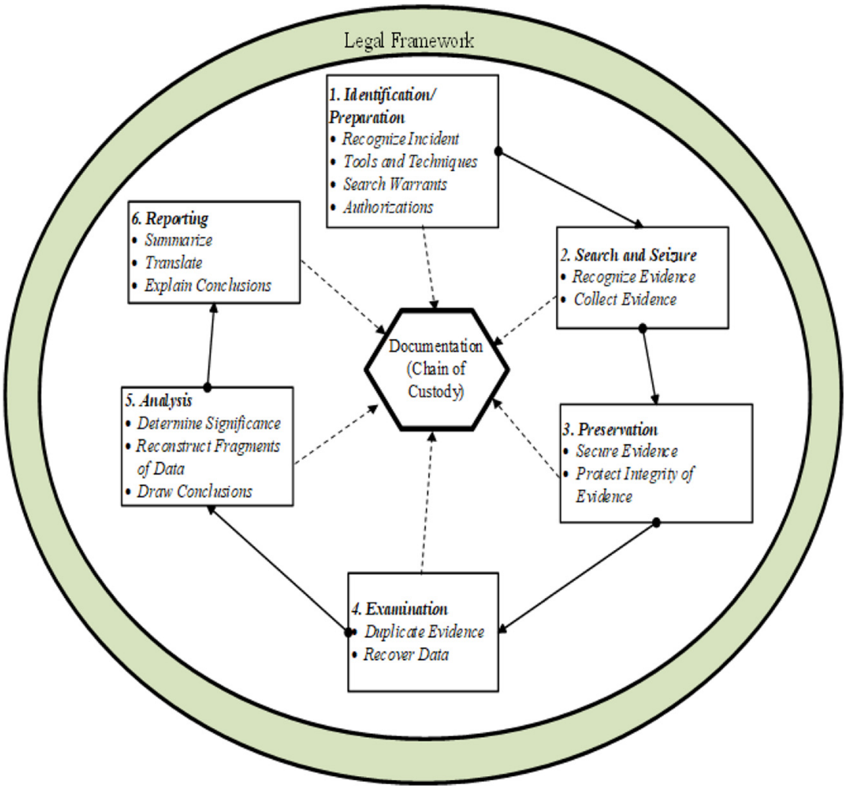


Fig. 1. Process model of digital forensic investigation adapted from Ami-Narh and Williams (2008).

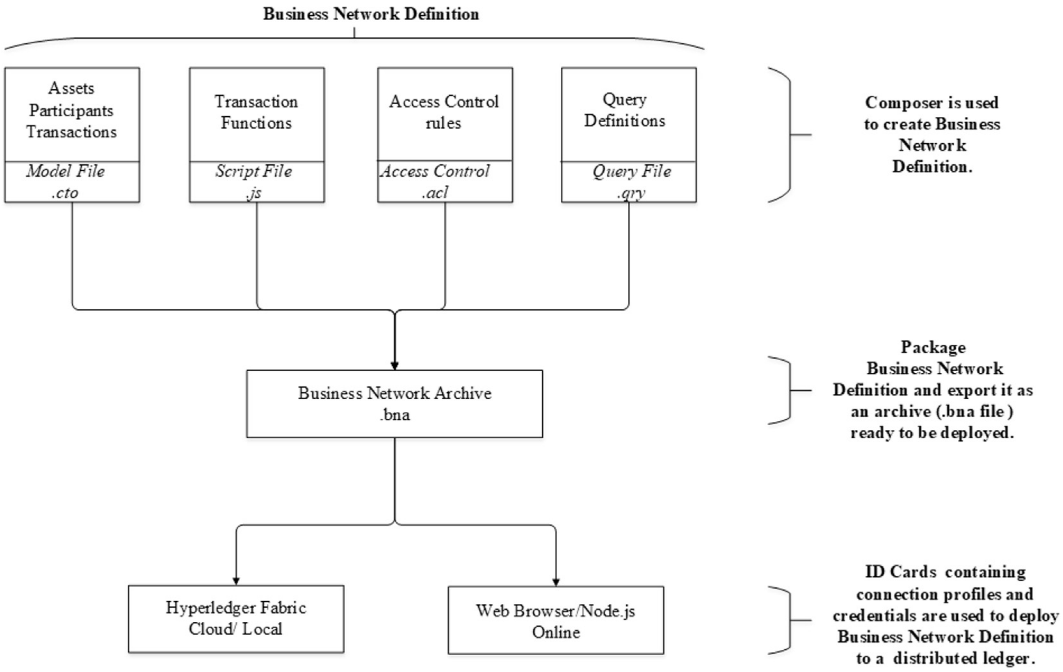

Business Network Definition
Assets Participants Transactions
Model File .cto
Transaction Functions
Script File .js
Access Control rules
Access Control .acl
Query Definitions
Query File .qry
Composer is used to create Business Network Definition.
Business Network Archive .bna
Package Business Network Definition and export it as an archive (.bna file) ready to be deployed.
Hyperledger Fabric Cloud/ Local
Web Browser/Node.js Online
ID Cards containing connection profiles and credentials are used to deploy Business Network Definition to a distributed ledger.

Fig. 2. Hyperledger Composer Architecture adapted from Introduction — Hyperledge (2018).

Q1 Is there any requirement of storing the state?

Q2 Do we have multiple writers in the system?

Q3 Can we afford to have trusted third party (TTP) online always?

Q4 Are all writers in the system known?

Q5 Are all writers in the system trusted?

Q6 Is there any requirement of public verification?

The answer to Q1 is yes because evidence passes through different levels of hierarchy during the investigation so we need to store the state of the evidence. The answer to Q2 is yes because we have multiple investigators and other stakeholders involved in the system. Answer to Q3 is no because the requirement here is the elimination of the central point of trust and failure. Answer to Q4 is yes, because only known and authenticated parties have to write

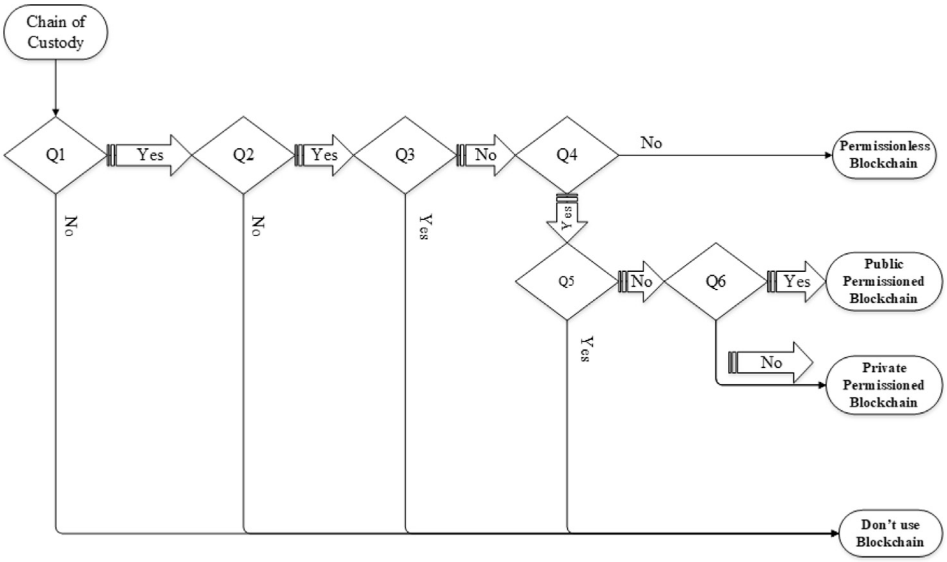

Chain of Custody
Q1
Yes
Q2
Yes
Q3
No
Q4
No
Permissionless Blockchain
No
No
Yes
Yes
Q5
No
Q6
Yes
Public Permissioned Blockchain
Yes
No
Private Permissioned Blockchain
Don't use Blockchain

Fig. 3. Blockchain feasibility test for digital forensics chain of custody adapted from Wüst and Gervais (2017).

access in the system. The answer to Q5 is no the because requirement is of decentralized trust(trusting everyone in aggregate). Finally, answer to Q6 depends on whether or not we require public verification, if public verification is required then public permissioned Blockchain is the feasible solution else private permissioned Blockchain as described in Fig. 3.

Motivation

In todays ever-growing digital world, dealing with digital evidence is getting harder and harder day by day because of its complex and volatile nature. Handling digital evidence poses unique challenges because of the fact they are latent, volatile, fragile, can cross jurisdictional borders quickly and easily and in many cases can be time/machine dependent too. Thus guaranteeing the authenticity and legality of processes and procedures used to gather and transfer the evidence in a digital society is a real challenge.

In principle evidence received from practitioners is perceived as accurate by the courts. However, on any dispute more in-depth

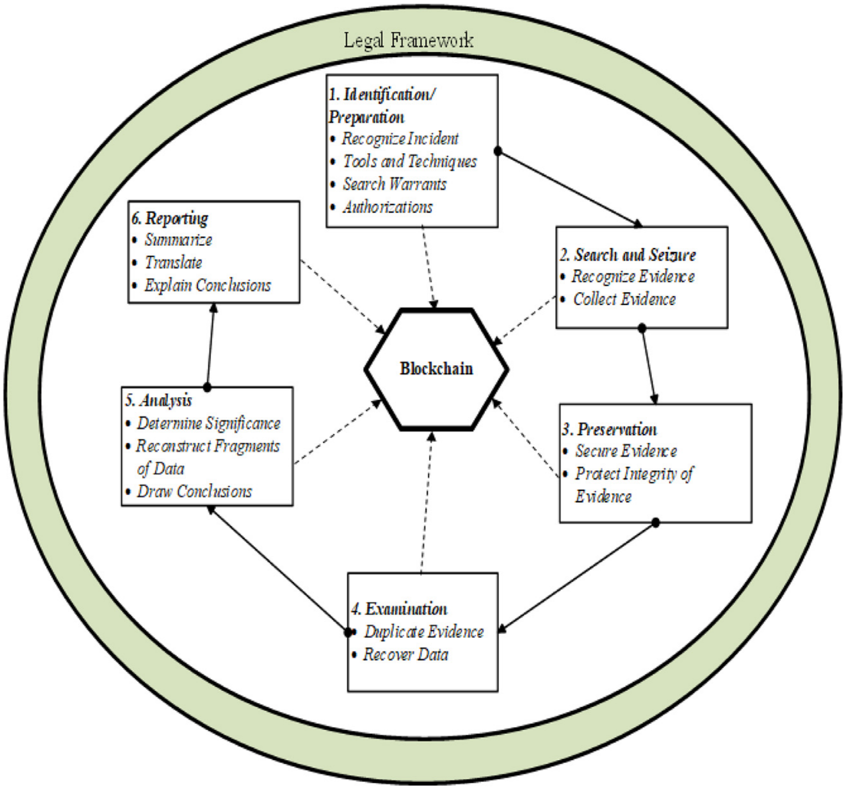


Fig. 4. Blockchain driven Process model of digital forensic investigation.

study is carried out to find the authenticity and integrity of reports. Hash code of digital files, the location of the crime scene and name of investigators are no longer sufficient for the admissibility of the evidence in the court of law. The artefacts like the digital signature of each object, the exact location where each piece of digital evidence was handled, the correct identity of all the persons involved in the forensic investigation and the people who had access to evidence and a complete log of all the transactions are also required. Furthermore, forensic investigator relies on automated forensic tools, thus reliability of investigation outcome heavily depends on the correctness of these tools and their application procedures.

To solve above-mentioned problems there is utmost need of a strong automated system for maintaining the artefacts of the evidence, providing auditing facility to assure the correctness of forensic tools and their application procedures and maintain the integrity of evidence itself so that digital evidence is admissible in the court of law.

Proposed model

Forensic Investigation tends to operate in regulated environments and requirements such as the identity of investigators who are investigating the crime related cases. While Bitcoin and Ethereum network is all about anonymity (pseudo-anonymity) where everyone can see the transactions but it is nearly impossible to infer who were involved in these transactions. Thus Bitcoin and Ethereum are not possibly the best choices for Crime scene investigation more particularly Digital Forensic Investigation which requires privacy and where the investigation is carried out by the authentic and trusted practitioners of Intelligence organizations (NSA, CIA etc.). The assets (Digital Evidence) need to be prevented from being corrupted by untrusted participants. Hyperledger Composer by design provides all the requirements for building an automated system that is both robust and secure in recording all the details pertaining to evidence gathering of a particular cyber forensic case. The proposed model will serve as a backbone for any forensic investigation or an audit trail in general done by an organization allowing them to use a process model for investigation or audit trail that is driven by Blockchain as shown in Figs. 4 and 5.

Forensic-Chain architecture has five main components namely Participants, Front-End, Core Modules, Blockchain Network and Distributed Storage as shown in Fig. 6.

1. **Participants**: They are considered to be the real actors in any network which needs to store transaction information. Participants usually represent business but have the potential of representing people, regulators or other stakeholders. In proposed

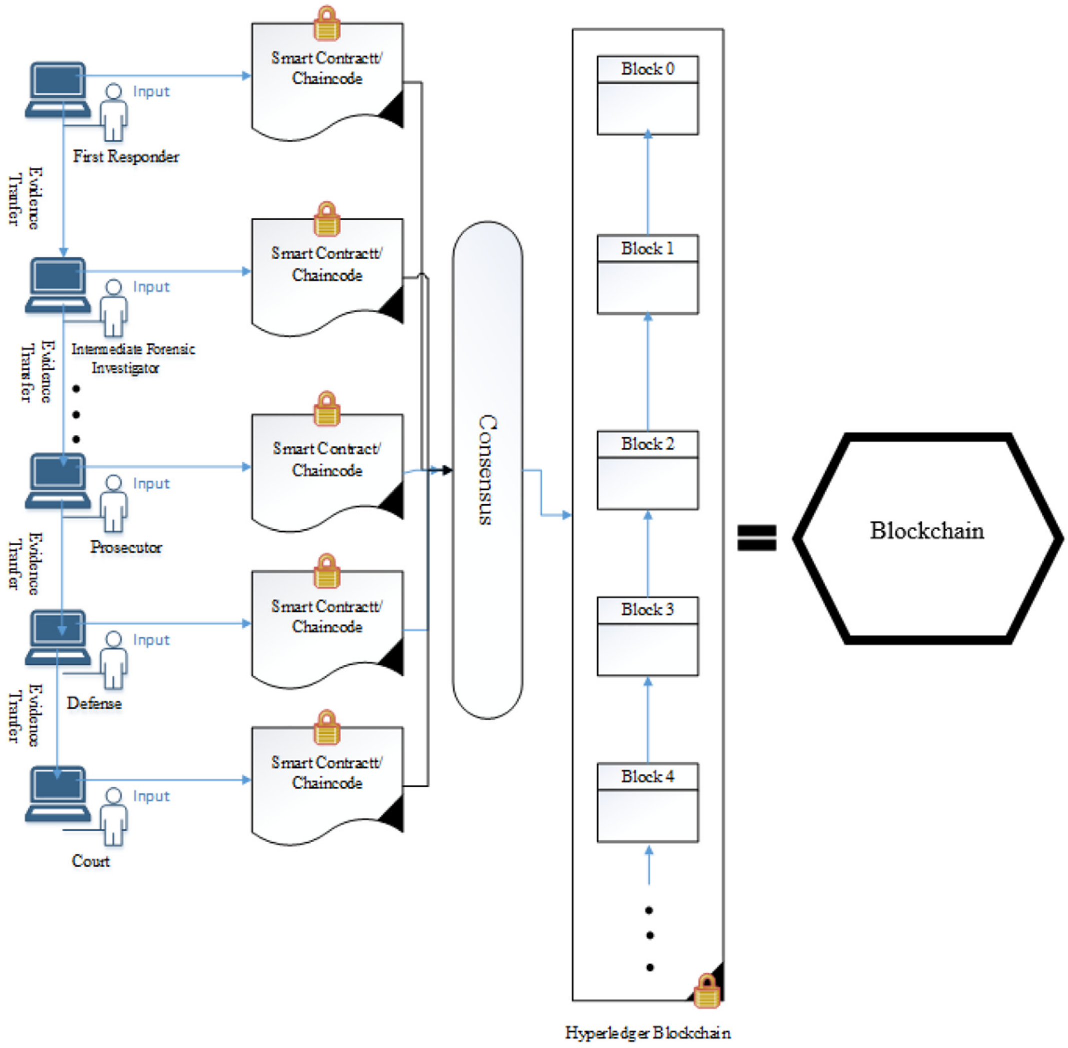


Fig. 5. Simplified architecture of Forensic-Chain.

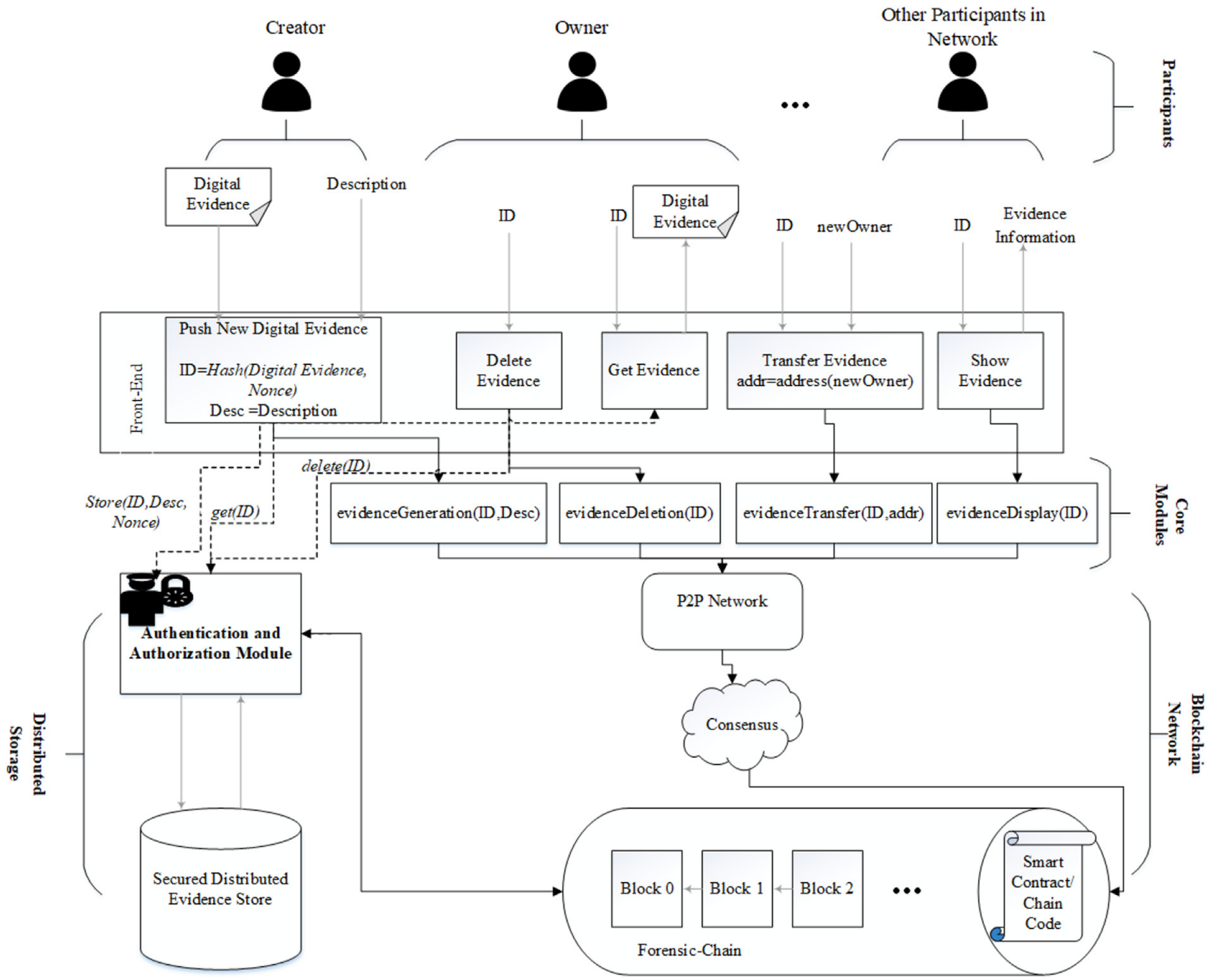


Fig. 6. Operational flow of forensic-chain.

Forensic-Chain model participants are the Forensic Investigators whose work is to gather as much as possible information about the digital evidence and record it in Blockchain. Prosecutor, Defense and Court also act as participants because at any point in the forensic investigation they require details about the chain of custody in our case maintained and preserved with the help of Blockchain. Only authorized participants are allowed to modify the state of Forensic-Chain and to view the details of the particular evidence.

2. **Front-End**: Forensic-Chain model front-end is developed with the help of composer-rest-server and Yeoman framework all bundled with Hyperledger Composer. Composer-rest-server helps in REST API generation for forensic-chain business network and Yeoman framework helps in generating skeleton angular application for the forensic-chain model. Participants communicate with Forensic-Chain via application generated as shown in Fig. 7.
3. **Core Modules**: Facilitates the communication with Blockchain Network. Participants store and retrieve the evidence details from the Forensic-Chain by calling an appropriate core module.
4. **Blockchain Network**: It comprises of Peer-to-Peer (P2P) network and Consensus protocol that governs the communication over P2P network.
5. **Distributed Evidence Store**: It comprises of distributed storage with authorization and authentication module for safely storing and preserving the original evidence.

PoC in Hyperledger Composer

Enterprise Blockchain applications can be best described in terms of Assets, Participants, and Transactions that are stored within the network.

- **Assets** can be anything of value that can be transacted or shared over the network. Assets can range from tangible ones like cars, houses or diamonds to intangible ones like securities, intellectual property or even it can be data to be referenced. In our proposed Forensic-Chain model digital evidence and the detailed information pertaining to a lifetime of digital evidence is the asset and is stored in the asset registry of Hyperledger Composer.
- **Participants** are considered to be the real actors in a network which need to store transaction information. Participants usually represent business but have the potential of representing people, regulators or other stakeholders. In proposed Forensic-Chain model participants are the Forensic Investigators whose work is to gather as much as possible information about the digital evidence and record it in Blockchain. In Hyperledger Composer, the structure of a participant is modelled in a model file. New instances of the modelled participant can be created and added in the participant registry. Hyperledger Composer also requires Blockchain identities as a form of identity and a set of mappings of identities to participants are saved in Identity

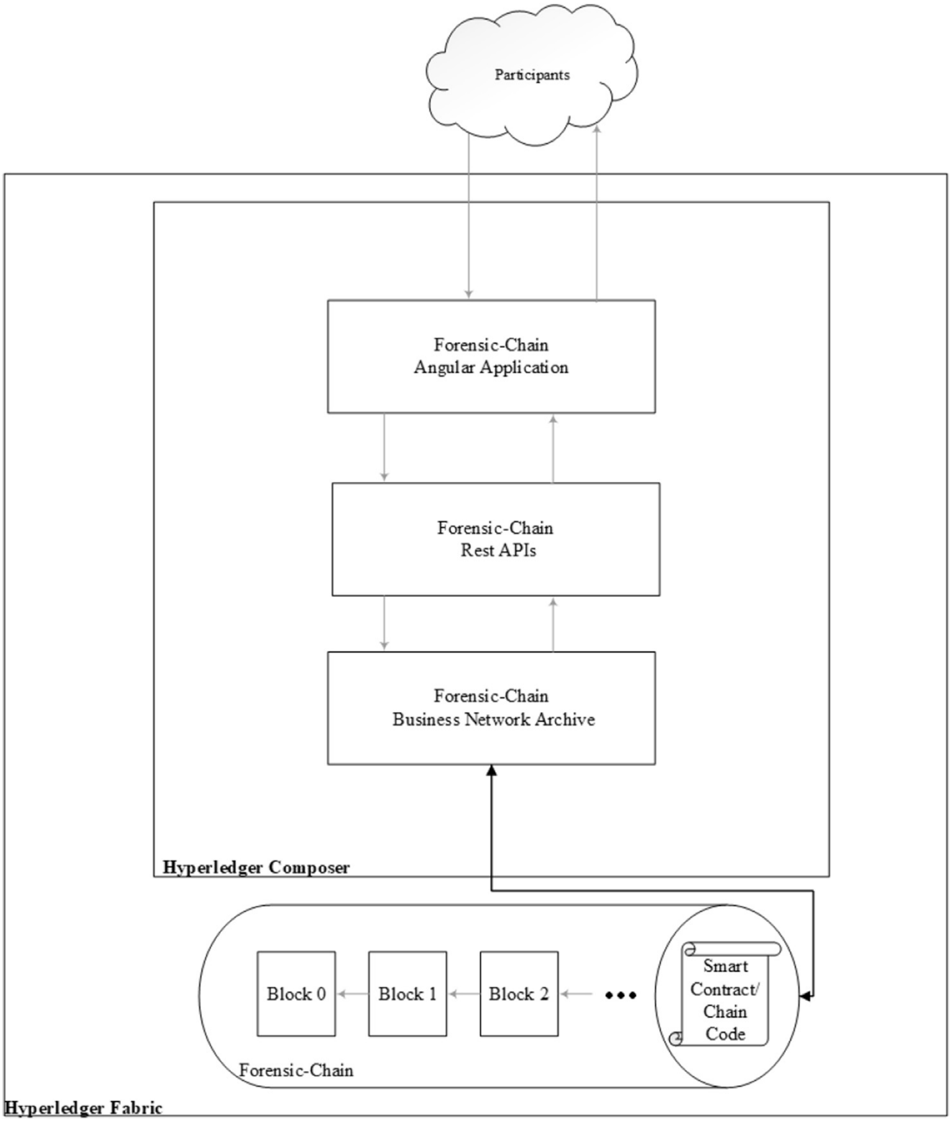


Fig. 7. Forensic-chain communication with participants via front-end.

registry. All identity management operations are carried by admin peers owned by consortium organisations which deploy Blockchain. In Forensic-Cain model at any instance of time, new participants (investigators) with appropriate identity roles can be added to handle a particular case by admin peers governed by organizations of Hyperledger composer Blockchain consortium. As an example, if the new judge comes to investigate the case, he will act as a new participant with proper identity role and privileges. Access control for what roles exist and which roles can execute which types of transactions are defined in permissions.acl file of Hyperledger Composer. Authorization to new judge will be given by admin peer owned by organizations of Blockchain consortium.

- **Transactions** describe the actions that could be done on the assets by participants as they move along the network. In proposed Forensic-Chain model transactions either record the details about the evidence or the evidence transfer event on the network.

We first defined the digital evidence as a data structure comprising the following information:

```
Struct Evidence contains
    string/bytes32 evidenceID ;
    address creator;
    address owner;
    string evidenceDescription;
    uint caseID;
    address TransferChain[ ];
    DateTime TransferTime[ ];
    // other optional stuff
```

- evidenceID: Uniquely identifies the digital evidence. Obtained by taking the SHA256 of digital evidence and other related information.
- creator: Participant who inserts the digital evidence into Blockchain at first place.
- owner: Participant with evidence in possession.
- evidenceDescription: Contains the essential attributes related to digital evidence.

- caseID: Unique number assigned to a case, to which digital evidence belongs. In our model caseID is initialized with a chain id at the time of chaincode/smart contract initialization. In fact, every single instance of a chaincode/smart contract represents a different case.
- TranferChain: An array containing the addresses of participants who have been the owner of digital evidence during its life cycle
- TransferTime: An array containing date and time of evidence transfers.

The Forensic-Chain model comprises four basic functions for creating, deleting, transferring and displaying the evidence information from the Blockchain. These functions can be viewed as Hyperledger Composer transactions triggered by the participants in the network. The constraints like who should access what function and under what conditions access should be granted to participants, are all defined in access control rules in permissions.acl file of Forensic-Chain model in Hyperledger Composer. Pseudocode of the functions is presented below in the form of algorithms.

- **Evidence Creation:** Evidence Creation function takes Evidence ID and Evidence Description as input and submits the evidence to Forensic-Chain. As ID is generated by taking the hash of digital evidence, therefore, it helps in maintaining its integrity of digital evidence throughout the lifecycle. Other attributes like creator and owner are also set to participant address/ID who created it first time. Participant address/ID is pushed to TransferChain array thereby indicating it is the creator as well as first owner of the digital evidence. Evidence creation time is pushed to TransferTime array. Note, Evidence Creation function first checks whether the evidence exists with the same ID if so it returns without creating the duplicate evidence.
- **Evidence Transfer:** Evidence Transfer method takes Evidence ID and address as input and in return transfers the ownership to address supplied. The function first checks whether evidence exists and the participant who invokes the function is the owner of the evidence if so, it sets the evidence owner to the new owner. It also pushes a new owner to the TransferChain array and current time to TranferTime array thereby maintaining the auditable chain pertaining to evidence transfer.
- **Evidence Deletion:** Evidence Deletion function takes Evidence ID as input and deletes the corresponding evidence from the Forensic-Chain. It first checks whether evidence exists and participant who invokes it is the creator of the evidence if so it removes the evidence entry from Blockchain. In Forensic-Chain model evidence is an asset, thus Evidence Deletion function removes the corresponding evidence from asset registry. This is required sometimes evidence is no longer relevant or valid for the case under investigation. No participant can delete actual evidence, however, can issue a transaction indicating particular evidence is no longer relevant to a particular case. Moreover, participants mostly deal with evidence metadata and clones of original digital evidence. Actual evidence is safely stored at first place. In forensic investigation, the first responder may acquire multiple sources of evidence and record the information in Forensic-Chain, however after investigation some sources of evidence may not produce any conclusive evidence pertaining to the case and hence recorded information about such sources is to be removed by invoking Evidence Deletion function of the proposed Forensic-Chain model.
- **Evidence Display:** Evidence Display function takes Evidence ID as input and returns the evidence information from Blockchain. The only check this function does is to ensure evidence already exists.

Algorithm 1
Evidence Creation.

```
Algorithm 1: Evidence Creation
  Input: Evidence ID,Evidence Description
  Result: Creates the Evidence with appropriate values in
          Forensic-Chain
  if evidence exists then
    return
  else
    Set the Evidence attributes with Evidence Description
    Set participants(who invoked this function) address as creator
      and owner of the evidence
    Push the address to TransferChain array
    Push the current time to TransferTime array
```

Algorithm 2
Evidence Transfer.

```
Algorithm 2: Evidence Transfer
  Input: Evidence ID, Address
  Result: Transfers the Evidence to the appropriate address in
          Forensic-Chain
  if  evidence exists && owner then
    Set the Evidence owner to new owner.
    Push the address to TransferChain array
    Push the current time to TransferTime array
  else
    return
```

Algorithm 3
Evidence Deletion.

```
Algorithm 3: Evidence Deletion
  Input: Evidence ID
  Result: Removes the Evidence from Forensic-Chain
  if evidence exists && creator then
    Remove the Evidence from Forensic-Chain.
  else
    return
```

Algorithm 4
Evidence Display.

y

```
Algorithm 4: Evidence Display
  Input: Evidence ID
  Output: Displays the appropriate Evidence instance from
          Forensic-Chain
  if evidence exists then
    Return the Evidence view from Forensic-Chain.
  else
    return
```

Proposed Forensic-Chain model is built on the top of Hyperledger Composer which is permissioned Blockchain (where the member identities and roles are known to the other members) and runs in a controlled environment governed by a consortium or single organization which deploy it. Thus information about the evidence is only confined to the participants who are part of the Blockchain, authorized by admin peers owned by organizations of the consortium. Participants can share information confidentially with the help of channels in Hyperledger fabric/composer. The structure, ease of integration with non-Blockchain applications and model re-usability functionality of permissioned Blockchains more specifically Hyperledger Composer makes it more suitable choice for simulating the functions of current criminal justice system in practice compared to permissionless counterparts like Bitcoin and Ethereum due to their inherent public nature and heterogeneity and complexity of the current judiciary system.

Performance evaluation

Performance is most sought-after feature of any problem solution, so is for Blockchain-based solutions. In order to evaluate the performance of our prototype, we used Hyperledger Caliper as performance evaluation benchmark framework. Performance evaluation was carried with Ubuntu 16.04 machine with 4 GB memory. We modified Caliper's basic-sample-network to simulate the behaviour of our prototype for evaluation purposes. We evaluated our prototype with Caliper's 2-organization-1-peer and 3-organization-1-peer network models with 4 clients. To determine transactional efficiency of our proposed model we designed test file specifically targeting two main functions of our model viz Evidence Creation and Evidence Transfer, the reason being their direct involvement in modifying the Blockchain state. We designed 10 rounds of test with a varied number of transactions and send transaction rate. Test was run multiple times to achieve the average values of performance indicators with less probability of error. Latency and Throughput in different rounds of 2-organization-1-peer and 3-organization-1-peer network models is given in Tables 1 and 2 respectively. Storage and Computational utilization of different components of 2-organization-1-peer and 3-organization-1-peer network models are given in Tables 3 and 4 respectively (see Figs. 8–10).

Performance evaluation results show that the prototype throughput reaches to peak point and then it starts decreasing with increase in send rate. In 2-organisation-1-peer and 3-organization-1-peer network models maximum throughput achieved is 15 tps and 10 tps respectively. Furthermore, it is evident from the results that the increase in a number of peers decreases the throughput of the prototype, which is in compliance with the property of Hyperledger based consortium Blockchains.

Benefits of proposed model

Forensic-Chain: Blockchain based solution for a digital forensic chain of custody has great potential to bring substantial benefits to forensic applications in particular and to audit trails in general by maintaining integrity, transparency, authenticity, security, and auditability of digital evidence and operational procedures applied during the investigation to achieve the desired end. Some of the significant benefits are summarized below:

1. Collecting, preserving and validating evidence can be strengthened with the help of Forensic-Chain.
2. Forensic-Chain model allows for the provenance of any event or action to be traced back where it originally entered the process in question.
3. Reduction of fraud by increasing transparency of the audit trail.
4. Blockchain driven Forensic-Chain eliminates the requirement of the trusted third party for validation of certain claims or evidence transfer and achieving consensus.
5. Forensic-Chain as an auditing tool assures the correctness of processes and procedures used by forensic analysis tools.
6. The proposed model allows organizations to embed the verification of the event or action within the evidence record itself, thereby enabling trust for the evidence which is both accessible and verifiable.
7. The proposed model opens a possibility of a cross-border forensic investigation.

Table 1
Performance evaluation results with 2-organization-1-peer network model.

Round	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	6 tps	0.85 s	0.70 s	0.77 s	5 tps
2	11 tps	1.18 s	0.74 s	0.98 s	9 tps
3	16 tps	1.46 s	0.49 s	1.13 s	13 tps
4	21 tps	2.89 s	0.61 s	1.93 s	14 tps
5	26 tps	4.06 s	0.84 s	2.72 s	14 tps
6	30 tps	5.80 s	1.05 s	4.37 s	15 tps
7	35 tps	7.27 s	1.32 s	5.76 s	15 tps
8	40 tps	21.61 s	8.36 s	16.15 s	8 tps
9	43 tps	11.49 s	2.49 s	8.38 s	15 tps
10	49 tps	13.88 s	8.57 s	11.85 s	13 tps

Table 2
Performance evaluation results with 3-organization-1-peer network model.

Round	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	6 tps	1.24 s	1.01 s	1.16 s	5 tps
2	11 tps	8.32 s	2.74 s	6.34 s	4 tps
3	16 tps	4.60 s	1.00 s	3.13 s	8 tps
4	21 tps	8.42 s	5.24 s	7.01 s	8 tps
5	26 tps	9.56 s	3.95 s	7.11 s	10 tps
6	30 tps	11.62 s	3.85 s	9.07 s	10 tps
7	33 tps	14.16 s	3.22 s	10.99 s	10 tps
8	39 tps	17.01 s	10.77 s	14.34 s	9 tps
9	46 tps	47.84 s	19.93 s	34.37 s	5 tps
10	50 tps	19.35 s	12.21 s	16.29 s	10 tps

Table 3
Memory and CPU utilization in 2-organization-1-peer network model.

Component Name	Memory(avg)[1]	CPU(avg)[2]
dev-peer0.org2.example.co…0.1.0	134.7 MB	18.00%
dev-peer0.org1.example.co…0.1.0	111.3 MB	32.95%
peer0.org1.example.com	288.5 MB	52.74%
peer0.org2.example.com	294.2 MB	25.88%
couchdb.org1.example.com	143.6 MB	136.37%
orderer.example.com	32.4 MB	1.79%
ca.org2.example.com	16.1 MB	0.00%
ca.org1.example.com	8 MB	0.01%
couchdb.org2.example.com	143.7 MB	74.68%

Table 4
Memory and CPU utilization in 3-organization-1-peer network model.

Component Name	Memory(avg)[a]	CPU(avg)[b]
dev-peer0.org1.example.co…0.1.0	95.5 MB	25.39%
dev-peer0.org3.example.co…0.1.0	106.8 MB	14.69%
dev-peer0.org2.example.co…0.1.0	98.0 MB	14.16%
peer0.org2.example.com	368.4 MB	19.95%
peer0.org3.example.com	286.8 MB	19.92%
peer0.org1.example.com	296.9 MB	39.29%
orderer.example.com	36.0 MB	1.61%
couchdb.peer0.org1.example.com	122.0 MB	102.93%
couchdb.peer0.org3.example.com	120.7 MB	58.67%
ca.org3.example.com	5.38 MB	0.00%
couchdb.peer0.org2.example.com	123.8 MB	58.95%
ca.org2.example.com	4.4 MB	0.0%
ca.org1.example.com	9.6 MB	0.04%

[a] Memory(avg) = Average(Memory(avg) of all rounds).
[b] CPU(avg) = Average(CPU(avg) of all rounds).

Related work

Several attempts have been made in the recent past for improving the quality of digital Chain of Custody which can be

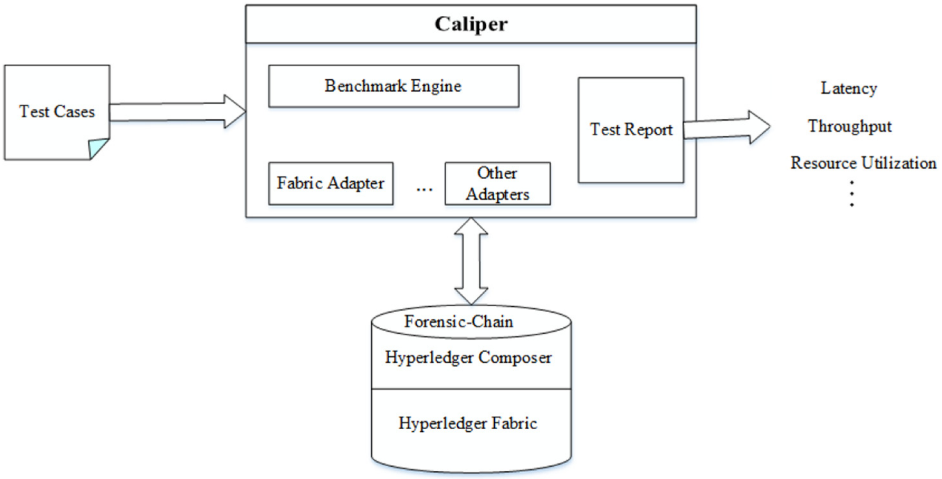
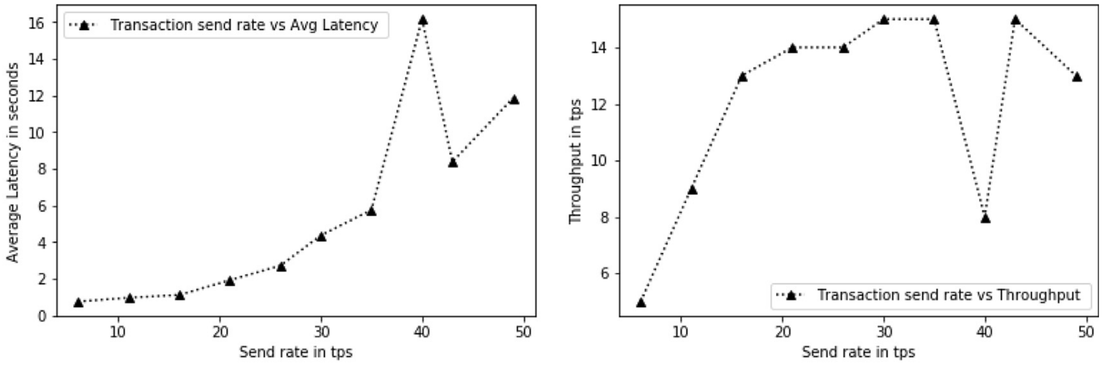
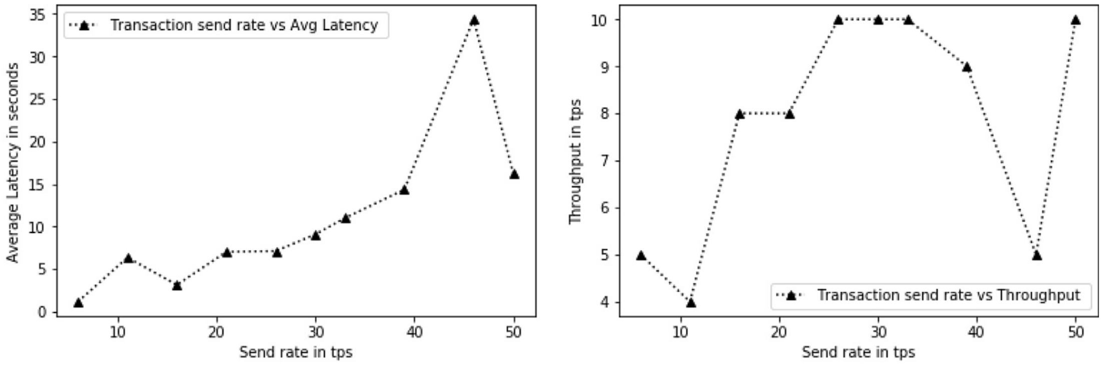


Fig. 8. Forensic-Chain Performance Evaluation setup.



(a) Transaction send rate vs average latency (b) Transaction send rate vs throughput

Fig. 9. Performance Evaluation using 2-organization-1-peer network model.



(a) Transaction send rate vs average latency (b) Transaction send rate vs throughput

Fig. 10. Performance Evaluation using 3-organization-1-peer network model.

broadly classified into two categories: Direct attempts and Indirect attempts.

Direct attempts

The work presented by the authors in Cosic and Baca (2010a) introduces the concept of Digital Evidence management Framework (DEMF), that seeks to develop secure and reliable CoC and answers the questions like Who, What, Why, Where and How of digital evidence. In Giova (2011b) the author proposed the idea of using new network facilities existing in AFF and exploiting the RDF structures to increase the quality of CoC. Authors in Cosic and Baca

(2010b) proposed the concept of using valid timestamps from a trusted third party for guaranteeing digital evidence integrity and CoC preservation. Authors in Prayudi et al. proposed the concept of Digital Evidence Cabinets (DEC) for enhancing the handling of digital evidence and recording of its chain of custody. DEC concept in general comprises of three parts viz: digital evidence management framework which is responsible for handling the interaction of investigators at different levels of investigation process, the tag cabinet concept responsible for the representation of digital evidence cabinet, the access control concept and secure communication responsible for providing support in terms of trustworthy-based computing environment. Recently the work presented in Shah et al. (2017) proposed the concept of using smart cards for storing the private keys of forensic investigators and generating signatures for ensuring the integrity of digital evidence. Work carried was the development of an automated tool that extracts not only the bit by bit image of the whole disk containing evidence but also creates the digital CoC and appends it to the image extracted. CoC is created in the forms rings. Initially, CoC has a sing ring containing the important information pertaining the digital evidence. Rings get added to CoC on each handover of evidence in the forensic investigation process.

Indirect attempts

Indirect attempts mainly involve approaches like knowledge representation and forensic formats for (Im)Proving digital CoC. The work presented in Bogen and Dampier (2004) applies Unified Modelling Language (UML) for representing knowledge and unified modelling methodology framework (UMML) for planning, performing and documenting forensics tasks. Work provided in Schatz et al. (2004) also attempts to improve indirectly the CoC through representation and correlation of digital evidence. In Al-Fedaghi and Al-Babtain (2012) authors proposed an abstract model of the digital forensic procedure based on a new flow-based specification methodology. This methodology efficiently specifies the forensic process in various phases and different roles by using the Flowthing Model (FM) that involves six operations(create, release, transfer, arrive, accept, and process).

The format in which digital evidence is presented and stored also plays an important in improving digital CoC. The most common and publicly available formats for digital evidence storage are Advanced Forensics Format(AFF), Raw, Digital Evidence Bag(DEB), EnCase Expert Witness Format (EWF), Gfzip, ProDiscovery, and SMART (DFRWS et al.). AFF originally developed by Garfinkel et al. (2006) is an open format for storing disk images and related forensic metadata. In Cohen et al. (2009) authors presented AFF4 as the extended version of AFF. AFF4 is built on the top of AFF with support for multiple data sources, logical evidence, and several other improvements. EWF is generated by Encase's imaging tools. It contains hash and checksum for image integrity verification and error information about bad sectors of source media. The work presented in Turner (2007) proposed the idea of using containers for storing forensic metadata, crime scene artefacts, integrity information, access and audit records. The work also demonstrated the application and use of Digital Evidence Bags as an integral and essential part of the forensic investigation process. Authors in Gayed et al. (2013) presented the idea of using Linking Data Principles (LDP) for managing tangible CoC. The work provides a framework explaining how the semantic web principles could be applied to CoC.

Conclusion and future work

Blockchain by design enforces integrity, transparency, authenticity, security, and auditability thus making it possibly the best choice for maintaining and tracing the forensic chain of custody. Blockchain helps in conflict reduction through increased trust and thus brings the real promise for the forensic community. This paper presented Forensic-Chain: A Blockchain based digital forensics chain of custody. We provided the prototype of Forensic-Chain model based on Hyperledger Composer and evaluated its performance. The prototype has shown acceptable overhead in terms throughput and resource utilization with the scope of optimization for full-scale end to end application. The future work aims at developing a complete optimized end to end integrated framework for storing digital evidence and maintaining chain of custody backed by IPFS and Hyperledger Blockchain. We also aim at developing Blockchain-based plug-in for automated forensic tools for recording every action that forensic investigator takes while processing digital evidence to ensure the consistency and integrity of forensic tools and also we have a future plan of developing Blockchain driven forensics as a service where Blockchain service will run in critical infrastructures as a proactive measure for recording actions and state of the system prior to the incident.

Appendix A. Forensic-Chain modules in Hyperledger Composer

Appendix A.1. Evidence class.

Appendix A.1. Evidence class

```
{
  "$class": "org.example.basic.Evidence",
  "Id": "0xABCDEFGHIJK",
  "creator": "resource:org.example.basic.
     Investigators#1234",
  "owner": "resource:org.example.basic.Investigators
     #1234",
  "Description": "Sensitive information pertaining
     to evidence",
  "tansferChain": [
    "resource:org.example.basic.Investigators#1234"
  ],
  "timechain": [
    "2018-08-31T15:46:15.864Z"
  ]
}
```

Appendix A.2. Investigator class.

Appendix A.2. Investigator class

```
{
  "$class": "org.example.basic.Investigators",
  "InvestigatorId": "1234",
  "firstName": "ABCDE",
  "lastName": "XYZ"
}
```

Appendix A.3. Evidence Transfer class.

Appendix A.3. Evidence Transfer class

```
{
 "$class": "org.example.basic.EvidenceTransfer",
 "ID": "resource:org.example.basic.Evidence#0xABCDEFGHIJK",
 "newowner": "resource:org.example.basic.Investigators#3456",
 "transactionId": "828b3578-b821-4991-a0a0-c604ceb7f536",
 "timestamp": "2018-08-31T15:48:42.050Z"
}
```

Appendix A.4. Evidence state after several transfers between Investigators.

Appendix A.4. Evidence state after several transfers between Investigators

```
{
  "$class": "org.example.basic.Evidence",
  "Id": "0xABCDEFGHIJK",
  "creator": "resource:org.example.basic.Investigators#1234",
  "owner": "resource:org.example.basic.Investigators#3456",
  "Description": "Sensitive information pertaining to evidence",
  "tansferChain": [
    "resource:org.example.basic.Investigators#1234",
    "resource:org.example.basic.Investigators#2345",
    "resource:org.example.basic.Investigators#3456"
  ],
  "timechain": [
    "2018-08-31T15:46:15.864Z",
    "2018-08-31T15:48:01.746Z",
    "2018-08-31T15:48:42.050Z"
  ]
}
```

References

Al-Fedaghi, S., Al-Babtain, B., 2012. Modeling the forensics process. Int. J. Secur. Appl. 6 (4), 97–108.

Ami-Narh, J.T., Williams, P.A., 2008. Digital forensics and the legal system: a dilemma of our times. In: Australian Digital Forensics Conference, vol. 41.

Bogen, A.C., Dampier, D.A., 2004. Knowledge discovery and experience modeling in computer forensics media analysis. In: Proceedings of the 2004 International Symposium on Information and Communication Technologies, Trinity College Dublin, pp. 140–145.

Cohen, M., Garfinkel, S., Schatz, B., 2009. Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Digit. Invest. 6, S57–S68.

Cosic, J., Baca, M., 2010a. A framework to (Im) prove" chain of custody" in digital investigation process. In: Central European Conference on Information and Intelligent Systems. Faculty of Organization and Informatics Varazdin, p. 435.

Cosic, J., Baca, M., 2010b. (Im) proving chain of custody and digital evidence integrity with time stamp. In: The 33rd International Convention MIPRO.

Ćosić, J., Ćosić, Z., Baća, M., 2011. An ontological approach to study and manage digital chain of custody of digital evidence. J. Inf. Organ. Sci. 35 (1), 1–13.

DFRWS, C. W. Group, et al., Survey of Disk Image Storage Formats .

Dhillon, V., Metcalf, D., Hooper, M., 2017. The hyperledger project. In: Blockchain Enabled Applications. Springer, pp. 139–149.

Garfinkel, S.L., Malan, D.J., Dubec, K.-A., Stevens, C.C., Pham, C., 2006. Disk imaging with the advanced forensic format, library and tools. In: Research Advances in Digital Forensics (Second Annual IFIP WG 11.9 International Conference on Digital Forensics). Springer.

Gayed, T.F., Lounis, H., Bari, M., Nicolas, R., 2013. Cyber forensics: representing and managing tangible chain of custody using the linked data principles. In: The International Conference on Advanced Cognitive Technologies and Application (IARIA 2013). Citeseer, pp. 87–96.

Giova, G., 2011a. Improving chain of custody in forensic investigation of electronic digital systems. Int. J. Comput. Sci. Netw. Secur. 11 (1), 1–9.

Giova, G., 2011b. Improving chain of custody in forensic investigation of electronic digital systems. Int. J. Comput. Sci. Netw. Secur. 11 (1), 1–9.

GitHub - hyperledger/caliper: A Blockchain Benchmark Framework to Measure Performance of Multiple Blockchain Solutions, 2018. https://github.com/hyperledger/caliper (Accessed on 08/30/2018).

Introduction — Hyperledger Composer, 2018. https://hyperledger.github.io/composer/latest/introduction/introduction.html. (Accessed 30 August 2018).

A. H. Lone, R. N. Mir, Forensic-chain: Ethereum blockchain based digital forensics chain of custody, Sci. Pract. Cyber Secur. J. ISSN 2587-4667 .

S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System.

Y. Prayudi, A. Ashari, T. K. Priyambodo, Digital evidence cabinets: a proposed framework for handling digital chain of custody, Int. J. Comput. Appl. 107 (9).

Richter, J., Kuntze, N., Rudolph, C., 2010. Securing digital evidence. In: Endicott-Popovsky, B., Lee, W. (Eds.), Proceedings of the 5th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2010), vol. 2010. IEEE, Institute of Electrical and Electronics Engineers, United States, ISBN 9780769540528, pp. 119–130. https://doi.org/10.1109/SADFE.2010.31.

Schatz, B.L., 2007. Digital Evidence : Representation and Assurance. Ph.D. thesis. Queensland University of Technology. URL. https://eprints.qut.edu.au/16507/.

Schatz, B., Mohay, G., Clark, A., 2004. Rich event representation for computer forensics. In: Proceedings of the Fifth Asia-Pacific Industrial Engineering and Management Systems Conference, vol. 2. APIEMS 2004, pp. 1–16.

Shah, M.S.M.B., Saleem, S., Zulqarnain, R., 2017. Protecting digital evidence integrity and preserving chain of custody. J. Digit. Forensics, Secur. Law 12 (2), 12.

Turner, P., 2007. Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags. Digit. Invest. 4 (1), 30–35.

Wüst, K., Gervais, A., 2017. Do you need a Blockchain? IACR Cryptol. ePrint Archive 2017, 375.