IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management

Article *in* International Journal of Computer Applications · December 2021

DOI: 10.5120/ijca2021921808

Yudi Prayudi
Universitas Islam Indonesia

Ahmad Luthfi
Universitas Islam Indonesia

IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management

Jefrul Hanafi
Department of Informatics
Indonesian Islamic University
Indonesian Yogyakarta

Yudi Prayudi
Department of Informatics
Indonesian Islamic University
Indonesian Yogyakarta

Ahmad Luthfi
Department of Informatics
Indonesian Islamic University
Indonesian Yogyakarta

ABSTRACT

Dematerialization of physical evidence is an asset of digitizing information, where information from physical evidence becomes more important than physical evidence itself. In principle, to preserve digital evidence, an accurate and reliable distributed storage system is needed that is packaged in terms of asset digitization which are summarized in chain of custody (CoC) documents. In addition to addressing all the needs related to the storage system, one thing that is no less important is to focus on the ease of distributing evidence on the network safely and reliably. This is one of the most important parts of interpreting the effectiveness of digital forensic investigations. However, several problems arose regarding the concept of managing digital evidence asset storage which still cannot be distributed, and is difficult to track. The purpose of this research is to complement the concept of Digital Evidence Cabinet (DEC) by combining InterPlanetary File System (IPFS) and Hyperledger Fabric (HF) as a distributable storage system. By proposing an alternative approach to the IPFSChain model, it is possible to achieve ease of data transfer, better data trust and protection of its ownership. The contribution of this research is to provide the concept of IPFSChain as a distributed storage model and all activities on assets can be audited properly by considering the rules of chain of custody.

General Terms

IPFS, Blockchain, Chain of Custody

Keywords

Digital Forensic, IPFS, Hyperledger, Chain of Custody, Digital Evidence

1. INTRODUCTION

Management of complex chain of custody assets and digital evidence, both in the process of retrieval, acquisition, preservation, and reporting [1]. Each process has its own vulnerability to assets. Among them are untrusted transaction processes, namely recording, storage, access control, and transfer of digital evidence in an insecure and effective network. Insecurity arises when the person creating the record is not digitally certified, the assets stored are not automatically encrypted, communications and data transfers are not transparent and cannot be traced. Assets are objects that move between participants [4]. Ineffectiveness occurs when the storage system is not distributed. Centralized storage causes delays when the central server is down or exposed to a DoS attack causing data availability to be hampered. In addition, the presence of a third party can lower the level of trust.

Given the importance of maintaining the integrity of the evidence from the beginning to the disposal of the evidence, the procedure for documenting evidence must be carried out chronologically [2] which will ensure that the evidence can be received in the courtroom [3]. Known as chain of custody (CoC). In other words, digital audit information for each stage of the investigation containing the what, who, when, where, why and how will be included in the chain of custody document. In addition, it takes the policy of the authority that controls all these activities.

Policies related to the authorization of all activities in the network that are not transparent can lead to distrust between one member and another. A member is a person registered in the system who occupies the position of one of the four certified parties. Members can consist of one or more in one party. In this study, parties are participants who will be formed in making a policy consisting of five participants, namely admin, officer, first responder, investigator, and extern. Each party's function is regulated based on a pre-agreed policy. The policy is flexible which can be set in an access control script. Therefore, it will be easier to identify and reliable.

In this research, a combined prototype of blockchain technology and IPFS distributed storage system is carried out, namely the IPFSChain model with off-chain and on-chain concepts. The concept refers to research conducted by [1], [6]-[8]. The approach taken is with the Digital Evidence Management Framework, distributed storage, access control, transparency, and auditable transaction security. The contribution of this research is to provide the concept of IPFSChain as a distributed storage model and all activities on assets can be audited properly by considering the rules of chain of custody.

2. RELATED WORK

Chain of custody which refers to efforts to record the state of an evidence chronologically during an investigation. As defined by The National Institute of Justice (NIJ) and The National Institute of Standards Technology (NIST) [31], [32]. In addition, the implementation of blockchain technology is carried out by various agencies for security, tracing track records in the system and maintaining the integrity of their data. In this case indirectly, the track record of activity by the blockchain system is a chain of custody.

Blockchain is a distributed database that tracks all transactions to ensure data set integrity [11], and safeguards copyright [12], without the involvement of third parties with efficient data management solutions [13] that use hash structures and consensus mechanisms. On the other hand, blockchain can only store data in the form of metadata but not the original file.

In terms of security, data storage on external platforms brings an important problem. As an alternative, IPFS can perform data security in protecting copyright. Data is encrypted and secured with the ELGamal encryption algorithm [14]. While the cloud service center structure has increased in recent years, concerns about privacy, security and traceability have also increased. For this purpose, a study of the combination of blockchain technology and IPFS has been carried out which can provide efficient results [19]. The solution given in this research is more focused on how to secure the copyright of a product designed by one of the members.

The heterogeneity of evidence and the lack of transparency in efforts to record, access, store, transmit data are essential for the forensic team to pay attention to. Apart from matters related to security, research focus on transparency and ease of data transmission in the management process of a digital asset, can provide a better level of trust. Previous research and development on digital evidence management, starting from the design of a framework formulated with a simple XML structure [9] with a centralized storage system Digital Evidence Cabinet (DEC) [1] to a complex framework using blockchain [6] - [8]. Vulnerabilities in an open and easily modified XML structure [6].

As previously mentioned, blockchain can only record information in the form of metadata, while the original files of digital evidence are stored in IPFS as one of the popular distributed storage technologies [18]. However, if it is integrated with IPFS and blockchain, it can provide an overhead that consumes resources and computational time [8].

3. THEORETICAL BACKGROUND

3.1 Blockchain

Blockchain is a distributed, open source, immutable, public digital ledger that is distributed among network peers [15]. This ledger keeps a permanent record of the transactions and interactions that take place between participants accessing a distributed and decentralized blockchain networkin a secure, verifiable and transparent manner[17].

3.1.1 Blockchain elements

Blockchain elements as the main driving principles they have the nature of[19]:

Decentralization:An essential element of a blockchain that does not require a central node for several tasks including recording and storing data. The task is distributed between nodes.

Consensus Model(s):The consensus protocol serves as the guardian of data privacy on the network. There are three characteristics of this protocol, namely fault tolerance, liveliness, and security. These characteristics are based on two things, namely efficiency and applicability.

Transparent: Self-review by blockchain network every 10 minutes, to reconcile between transactions in the network.

*Open Source:*This element means that anyone can set up an application or use the services of a public blockchain.

*Identity & Access:*The public blockchain allows anyone to review and verify any transaction. Data in private blockchain is restricted.

*Autonomy:*Data on the blockchain can be sent and can be updated securely.

*Immutable:*An essential element of a blockchain that does not require a central node for several tasks including recording and storing data. The task is distributed between nodes.

*Anonymity:*An essential element of a blockchain that does not require a central node for several tasks including recording and storing data. The task is distributed between nodes.

3.1.2 Blockchain components

*Blockchain components*as part of their main constituent elements in the form of[26]:

Transaction and Block: Records of events, cryptographically secured with digital signatures, which are verified, ordered and bundled together into blocks, form transactions on the blockchain. Thus, each block consists of transaction data along with a timestamp, a cryptographic hash of the previous block (the parent block) and a nonce. A nonce is a random number or bit string used to verify the hash.

Cryptography: It provides security and immutability by linking blocks in chronological order using a hash function. Legal ownership is given to transactions using digital signatures.

Smart Contract: The term smart contract was originally coined by Nick Szabo [27]. They are computer programs that run automatically when certain criteria are met in the system.

Consensus: Mutual agreement on one data state in a distributed network. Support for preventing malicious nodes from changing the state of data in a distributed environment.

Per-to-Peer (P2P) Networks: Blockchain runs on a P2P network over the Internet without a central server. As a result, they do not have a single point of failure or attack. Each peer contributes storage and processing power for network maintenance.

3.1.3 Advantages of the blockchain

a) Troubleshooting synchronization problems that occur in traditional databases [19].
b) Adding any transaction in the network will be reflected in the database in all existing copies [20].
c) Data will be available, integrated, secure and immutable [21].
d) Trust between nodes [22].

3.1.4 Disadvantages of the blockchain

a) Since data is written and stored, no one can change it [19].
b) Storage of data on the network in more than one place will increase costs [20].

3.2 Hyperledger Fabric (HF)

Hyperledger Fabric [24] is an enterprise-grade open source platform with permission Distributed Ledger Technology (DLT) focused on developing a suite of frameworks, tools, libraries for stable blockchain deployments, hosted by the Linux Foundation. In research [25] described Hyperledger Fabric as a revolutionary framework because of its features that enable membership services and plug-and-play properties for blockchain solutions.

3.2.1 Main Components: Client, Peer, Order, CA [28].

*Client:*The client is a command line or application developed by the SDK. In other words, the person/member who owns and maintains the peer node. A peer is a network entity that maintains a ledger that runs the system. Two client functions, first is for node management including start, stop, node configuration, etc. Second, for chaincode lifecycle management including installation, upgrade, chaincode execution etc.

*Peer:*Equal footing nodes in a distributed system. Two types of peers: endorsers and committers. The endorser is responsible for verifying, simulating, and supporting transactions. The Committer is responsible for verifying the legitimacy of transactions and updating the status of the

blockchain and ledger.
Orderer:A collection of nodes known as bookers who are responsible for receiving transactions sent by peer nodes, sorting transactions according to certain rules into blocks.
CA:Authority component that provides or cancels member identity certificate.

3.2.2 Channel

Channels are private blockchain overlays that allow the isolation and confidentiality of data. Channels defined by Configuration-Block.

3.2.3 Chaincode

Chaincode is a program written in golang, java that generates transactions so that external parties can interact with the blockchain [28]. In general, a smart contract is the transaction logic that controls the lifecycle of a business object. Smart contracts are the regulator of transactions, while the chaincode regulates how smart contracts are packaged for implementation [24].

3.2.4 Ledger

A ledger is a database that contains the current value of a set of key-value pairs that have been added, modified, or removed by a validated and committed set of transactions on the blockchain [24].

3.3 Hyperledger Composer

The Hyperledger composer is a modular tool from Hyperledger Fabric containing a modeling language, and a set of APIs that make it easy for developers to create blockchain applications [29]. It is a collaboration tool that accelerates the development of smart contracts and distributed ledger structures [7]. The Hyperledger composer contains eleven components, namely: *Blockchain Satet Storage*: Hyperledger basically has two storage areas, a distributed ledger and a state database [16]. The distributed ledger contains all transactions sent over the network, the state database contains the current status of assets and participants [29]. *Connection Profile:* The part of the business network card that is a JSON document as a link to the Fabric runtime executin. *Assets:* Goods, services, or tangible or intangible property, and are kept on a register. *Participants*: Members of the business network. *Identities*: Digital certificates and private keys that are used to transact on a business network and must be mapped to participants in the network. *Bussines Network Card*: A combination of identity, connection profile, and metadata, metadata that optionally contains the name of the business network to which it is connected. The business network card will be stored in the wallet. *Transactions*: The mechanism by which participants interact with assets. *Queries*: Queries are used to return data about the world-state blockchain. The query is sent using the Hyperledger Composer API. *Events*: defined in the business network definition in the same way as assets or participants. *Access Control*: Contains a detailed set of control rules over which participants have access to what assets and under what conditions. *Historian Registry:* Historian is a special registry that records successful transactions, including the participants and the identity that submitted them. Historians store transactions as HistorianRecord assets, which are defined in the Hyperledger Composer system namespace [29].

3.4 InterPlanetary File System (IPFS)

The need for reliable storage areas is increasing. In addition, the availability and ease of access to data to achieve better effectiveness is very much needed, especially in the realm of digital forensics. IPFS provides services with a distributable file storage environment. IPFS is a peer-to-peer distributed file system that attempts to connect all computing devices with the same file system [18].

Research conducted [30] states that, IPFS is not suitable for use cases where performance or security is critical. IPFS lacks authentication and the ability to track access and authentication [8]. However, IPFS is well suited for use cases where availability and fault tolerance are important [30]. Therefore, the need for data access and availability services can be met. As for security, implementing blockchain technology as a block chain to store metadata as an alternative.

3.5 Chain of Custody (CoC)

The principle of chain of custody is that ensuring the integrity of evidence by establishing and maintaining a chain of custody is essential for investigation. This will protect against further charges of destruction, theft, planting, and contamination of evidence [31]. Chain of custody is the process of maintaining and documenting the chronological history of evidence [32]. Through proper documentation, collection and preservation, the integrity of evidence can be assured. A well-maintained chain of custody and rapid transfer will reduce possible challenges to the integrity of evidence [31].

4. IPFSCHAIN: ALTERNATIVE PROPOSED

4.1 Architecture and Components Overview of IPFSChain

This section provides information on an overview of the architecture and components that make up the IPFSChain system. The information is given in Figure 3. User is an ordinary user who will be a participant or client if he has registered on the HF network and has certain authority rights. The client will return to normal user status when interacting with IPFS, because it is an off-chain part of another system. Additionally, IPFS is configured by default or publicly.

Participants or parties that have been previously determined will only be able to access files on the IPFS system if that party has received information from within the HF system in the form of a link for raw file access. The link is obtained if only that party is registered as an official member or registered in HF as a member or client.

If it turns out that there are parties working with unknown outsiders, then these unknown parties can access the file into the IPFS system and change it, then the alternative is to compare the hash value of the file. Comparison of the hash value of the file that has been recorded and stored in the HF system with the hash value of the file obtained from the IPFS system. If the hash value of the file is not the same as the hash value of the file in HF, it can be ascertained that the file is contaminated or invalid. The integrity of the file is considered valid, based on the information that has been documented into the HF system.

Broadly speaking, the components that make up the IPFSChain model consist of four components, namely: IPFS, HF, and the hyperledger composer. IPFS has the advantage of a distributable storage system with good performance and data availability. However, it is difficult to track access and authentication. The overview of the Hyperledger Composer as a modular HF is that it can make it easier to design business network systems, create policies with flexible access control, while both are an integral part of the Hyperledger project that can trace access to data. These components can be seen in Figure 1 and Figure 2.

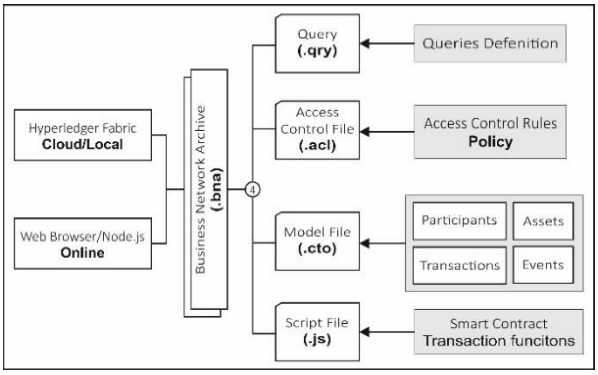


Fig 1: Hyperledger composer components

4.2 Design and Hyperledger Composer Tool

IPFSChain's aim is to provide a new alternative to the adoption of the Digital Evidence Cabinet (DEC) concept in digital evidence management and chain of custody. With this on-chain and off-chain concept design on IPFSChain, it is hoped that it will contribute to data availability, ease of access and transfer, and auditability of all activities on data. To achieve this objective, the representation of the components that will be focused on are: Participants: This section, as previously explained, basically consists of five parties, namely: Admin, officer, first responder, investigator, extern. Admin is the main person who gets full authority by default, which is given by the HF system to implement agreed policies. This admin can be interpreted as a super admin. By default from the HF system, this admin is hidden and invisible. So that later, only four participants will be seen, which can be seen in Figure 2. Meanwhile, the officer is the admin who is given the authority through the super admin to manage the system that has been designed for digital evidence management and chain of custody. The first responder is the party who plays an important role in recording information from the evidence, then transferring it by using the transaction rights to transfer assets to members of other parties. Thus, the ownership of the status of the transferred evidence assets will change. Investigators are members who will identify and search for evidence. Extern is a party whose members can consist of prosecutors or judges in the realm of law at the trial later. So that members from external parties can see directly the activities that occur in the IPFSChain system transparently. Thus, it is hoped that it can provide a better level of trust to the prosecutor/judge and make it easier to make decisions.

*Assets:*There are two assets created in the HF on-chain system in the form of metadata, namely: digital evidence and chain of custody. The raw evidence files are: video, audio, image, text, and document. The format and names are evidence01.txt, evidence02.jpg, evidence03.pdf, evidence04.mp3, and evidence05.mp4. This raw file is stored into IPFS off-chain system.

*Transactions:*Transactions in this case are activities that can only be carried out by first responders on assets. The transaction is in the form of evidence transfer and CoC transfer. Thus, the purpose of this transaction is related to the ownership of the asset. That is, the status of the asset will change ownership when the transaction is successful.

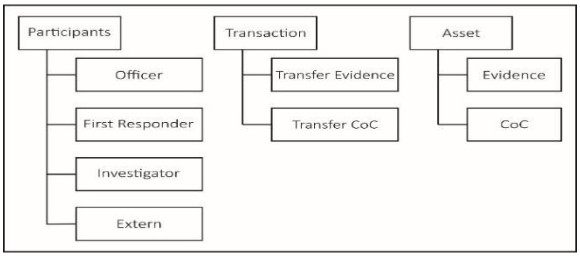


Fig 2: Particpant, trasaction, and asset components in IPFSChain model

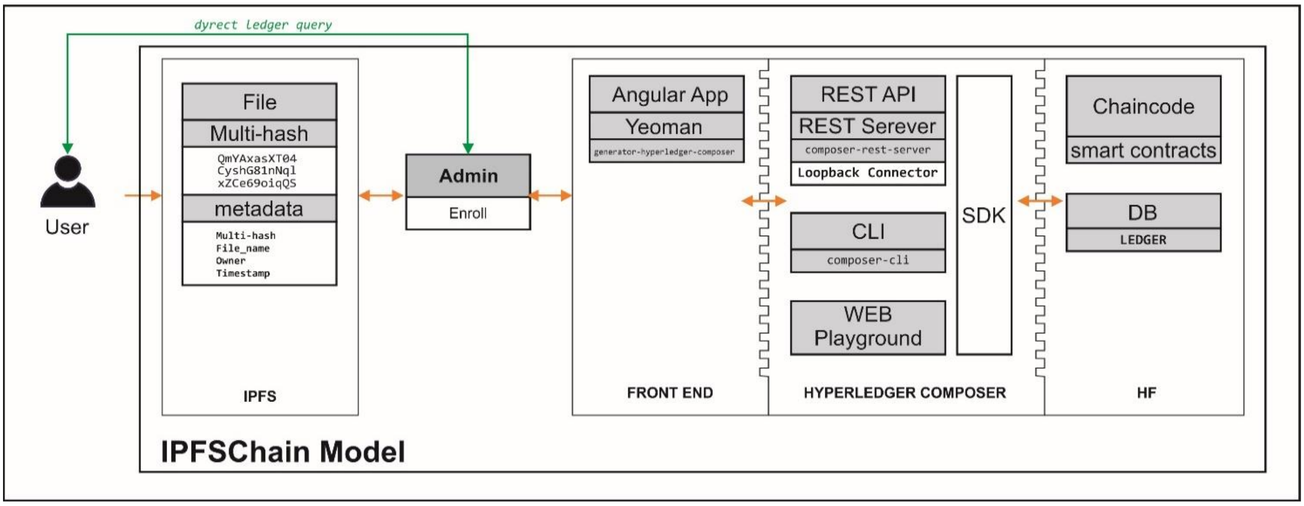


Fig 3: IPFSChain model architecture and components

5. IMPLEMENTATION AND RESULT

5.1 Create Business Network Archive

In this stage, the super admin uses the hyperledger composer tool on the Fabric platform via a web playground to create four participants, assets, and transactions. The archives used in this paper are: model file (.cto), script file (.js), and access control file (.acl). As shown in Figure 3, the business network archive (.bna) file is used to interact with the Fabric network. File.cto is a modeling language that defines who the participants are, what assets will be kept, and what assets can be transacted. The rules and policies are written in the file.acl. Furthermore, file.js is a script for how transactions work.

5.2 Angular Application and Authority

Yeoman generates a skeleton angular web application for users to interact with the HF network. Then, all participants who have been registered by the admin/officer have the same read rights to the assets. The rights are in the form of create, read, update, and delete. These rights are given in table 1. The representation of recording information from digital evidence evidence002.jpg into the blockchain is given in Figure 4.

Table 1. Authorization of participants and assets

Participants	**Assets**							
	Evidence				**CoC**			
	C	**R**	**U**	**D**	**C**	**R**	**U**	**D**
Officer		✓		✓		✓		✓
First Responder	✓	✓	✓		✓	✓	✓	
Investigator		✓				✓		
Extern		✓				✓		

5.3 Functions of the Pseudocode IPFSChain model in Hyperledger Composer

5.3.1 Registration Participants

The participant registration function is to register related parties into the HF network with the hyperledger composer tool. The registration function enters (email, firstName, lastName) as input and makes a request via an API in the system. After the participants are registered, an identity card is created for each participant and stored in the identity wallet. Algorithm 1 summarizes the member registration function on the first responder party in detail as a member representation of the other party.

5.3.2 Assets Creation

This asset creation function will take the ID from the digital evidence and the ID from the chain of custody as input and send it to the system. For every digital evidence there is one chain of custody, so the ID of the digital evidence will be in the chain of custody asset and vice versa. Detailed information is seen in algorithms 2 and 3.

5.3.3 Delete Assets

The delete asset function takes ID tokens as input and deletes tokens from IPFSChain. This asset write-off function is only given to members from the official side. As can be seen in table 1. Detailed information is given in algorithm 4..

5.3.4 Transfer Assets

This evidence asset transfer method takes the ID proof and inputs the participant's email. The participant's email is the ID of one of the party members. Whether members are publishers or new owners. With a note that the email used is already registered in the system. So that the transfer of evidence is successful and the ownership status of the asset changes. The same conditions apply to CoC assets. Detailed information is given on algorithm 5.

Algorithm 1 FirstResponder Registration

```
Input: email, firstName, lastName
Output: Register the FirstResponder as a participant
if (FirstResponder exists) then
    Return;
else
    Set email ← FirstResponder ID (email as ID of each party's member);
    Set firstName ← FirstResponder First Name;
    Set lastName ← FirstResponder Last Name;
end if
```

Algorithm 2 Evidence Assets Creation

```
Input: evidenceID, cocID, Url, Issuer, Owner
Output: Creates the Evidence appropriate values in IPFSChain
if (Evidence exists) then
    Return;
else
    Set evidenceID ← Evidence;
    Set cocID ← CoC;
    Set Url ← (Evidence raw file download address in IPFS);
    Set Issuer ← participants (Creator of evidence);
    Set Owner ← participants (Owner of evidence);
end if
```

Algorithm 3 CoC Assets Creation

```
Input: cocID, evidenceID, Description, Issuer, Owner
Output: Creates the CoC appropriate values in IPFSChain
if (CoC exists) then
    Return;
else
    Set cocID ← CoC;
    Set evidenceID ← Evidence;
    Set Desc ←complete information related to evidence (5W+1H);
    Set Issuer ← participants (Creator of CoC);
    Set Owner ← participants (Owner of CoC);
end if
```

Algorithm 4 Evidence Assets Delete

```
Input: evidenceID
Output: Remove the Evidence from IPFSChain
if (Evidence exists) then
    Remove the Evidence from IPFSChain;
else
    Return;
end if
```

Algorithm 5 Evidence Assets Transfer

```
Input: evidenceID, cocID, Email Owner, Email newOwner
Output: Transfer the Evidence appropriate values in IPFSChain
if (Evidence exists) then
    Set evidenceID ← Evidence;
    Set Owner ← Email Owner;
    Set newOwner ← Email newOwner;
else
    Return;
end if
```

5.4 Evidence and IPFS

Users are clients who will interact with two systems, namely IPFS and HF. All operations that the user can perform on the HF are described in the subsection above. Operations that users can perform on IPFS such as add, cat, and get.

5.4.1 Add Evidence to IPFS

Representation, the add operation is carried out by the first responder on the asset evidence02.jpg as follows:

```
$ ipfs add evidence02.jpg
```

Furthermore, the IPFS system provides the multi-hash value Qmd4vF6R7GfKqhPVPdakL3cKD5YhNUrwdhTRc88UigQbxM from the evidence02.jpg file as a link to access the file. The link in the form of a multi-hash is recorded by the first responder into the evidence assets in the HF system. See figure 4.

```
{
“$class”: “org.example.empty.Evidence”,
“$evidenceID”: “image01”,
“$cocID”: “coc01”,
“$typeEvidence”: “IMAGE”,
“$File_Name”: “evidence02.jpg”,
“$Url”:
“ipfs.io/ipfs/Qmd4vF6R7GfKqhPVPdakL3cKD5YhNUrwdhTRc88Uig
QbxM”,
“$Issuer”:
“resource:org.example.empty.Officer#or.samri@gmail.com”,
“$Owner”:
“resource:org.example.empty.Officer#fr.romi@gmail.com”
}
```

Fig 4: Display of metadata information on evidence assets

5.4.2 File Accessto IPFS

IPFS provides several commands for access, one of which is the 'cat' command and the 'get' command. The 'cat' command is used to display the data object and the 'get' command is used to download the object. The 'cat' and 'get' operations are executed locally as follows:

```
$ ipfs cat /ipfs/
Qmd4vF6R7GfKqhPVPdakL3cKD5YhNUrwdhTRc88UigQbxM
```

```
$ ipfs get /ipfs/
Qmd4vF6R7GfKqhPVPdakL3cKD5YhNUrwdhTRc88UigQbxM
```

As for the ease of access for users, by utilizing the url that has been recorded in the asset evidence as shown in Figure 4. The user pastes in the search field of his browser with the following url:ipfs.io/ipfs/Qmd4vF6R7GfKqhPVPdakL3cKD5YhNUrwdhTRc88UigQbxM.

6. PERFORMANCE EVALUATION AND DISCUSSION

In the IPFSChain implementation experiment the model uses the Ubuntu 16.04 LTS operating system running on VirtualBox version 6.1.26 r145957 with 20GB storage capacity, 4GB RAM, 1 core processor, NAT network connection, Hyperledger Composer: Docker Engineer v20.10, Docker Compose v1.28 , Node v8.15, Npm v6.4, Python v2.7, CLI Tool v0.20, Git v2.7. Hyperledger Fabric v1.2 (hlfv12). IPFS v0.9.

Performance on the IPFSChain model is measured based on the effectiveness of time or ease of access and data transfer. Performance tests were carried out using the JMeter v5.3 tool installed on the Ubuntu operating system. The experiment was carried out with 10 rounds, each round was five sample requests per second (rps) which made http requests on a rest server api in a HF system consisting of 1 organization 4 partners. The http request activity is a post on the transaction. In other words, in one round the transfer of CoC and evidence is carried out simultaneously as shown in table 2 and table 3.

Table 2. Performance evaluation on CoC transfer

Round	Send (rps)	Avg. Latency (s)	Throughput (rps)	Received (KB/s)	Sent (KB/s)
1	5	2.24	0.37	0.25	0.16
2	10	2.09	0.34	0.23	0.15
3	15	1.85	0.34	0.23	0.14
4	20	2.50	0.34	0.23	0.14
5	25	3.05	0.33	0.26	0.14
6	30	3.00	0.33	0.25	0.14
7	35	3.01	0.33	0.26	0.14
8	40	2.98	0.33	0.25	0.14
9	45	2.73	0.33	0.25	0.14
10	50	3.09	0.33	0.27	0.14

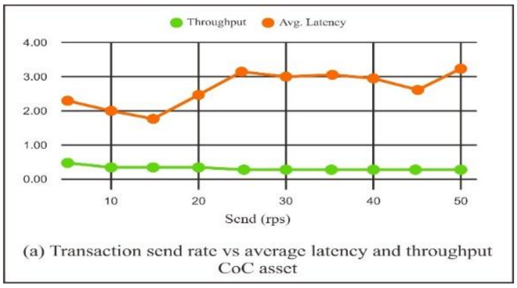
Table 3. Performance evaluation on evidence transfer

Round	Send (rps)	Avg. Latency (s)	Throughput (rps)	Received (KB/s)	Sent (KB/s)
1	5	2.24	0.37	0.25	0.16
2	10	2.72	0.34	0.23	0.15
3	15	2.70	0.34	0.23	0.15
4	20	2.87	0.34	0.23	0.15
5	25	2.98	0.33	0.23	0.15
6	30	2.99	0.33	0.23	0.15
7	35	2.99	0.33	0.23	0.15
8	40	2.99	0.33	0.23	0.15
9	45	2.91	0.33	0.23	0.15
10	50	2.98	0.33	0.23	0.15

Table 4. Performance evaluation on downloading and uploading digital evidence from and/or to IPFS

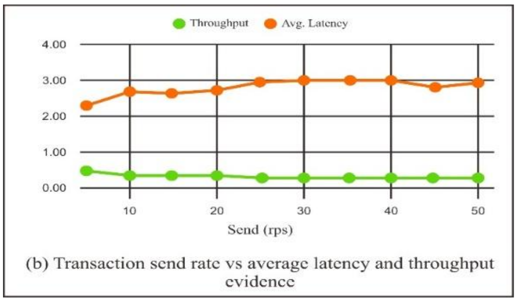
Digital Evidence	**Response Time (s)**		**Size (KiB)**
	Upload	**Download**	
evidence01.txt	0.04	0.04	5
evidence02.jpg	0.04	0.04	50
evidence03.pdf	0.15	0.34	500
evidence04.mp3	1.42	2.45	5000
evidence05.mp4	6.96	18.73	50000

As for the two assets with a total of 100 data transfer transactions on the IPFSChain api rest server system, it reduces the throughput value with sent and received times, an average of less than 3 seconds with an error of 5.5%. The results in this study show the same argument as in the research conducted [9], namely by increasing the number of partners reducing throughput. The histograms are shown in Figures 6 and 7. The performance of uploading and downloading files on IPFS is shown in Figure 8. Figure 8 shows that small files do not have a significant impact on the performance of IPFS. The details of the performance of the file are given in table 4.



(a) Transaction send rate vs average latency and throughput CoC asset

Fig 6: Performance on CoC asset transfer transactions



(b) Transaction send rate vs average latency and throughput evidence

Fig 7: Performance on evidenceasset transfer transactions

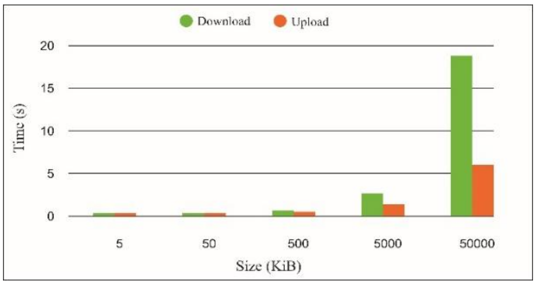


Fig 8: Comparison of download and upload times

7. CONCLUSION AND FUTURE WORK

This paper proposes an IPFSChain model system that provides convenience in transparent and secure data transfer. Technically, IPFSChain operates on the Hyperledger Fabric framework with the Hyperledger Composer tool as modular to simplify the design of permission-based blockchain networks. Hereinafter referred to as on-chain. On the other hand, large raw data is stored into the IPFS system. This is called off-chain. Experimental results confirm that this IPFSChain model provides sensitive digital evidence and chain of custody data to ensure time efficiency, data availability, security and reliability. Future work is to provide capabilities that can audit activity associated with IPFS systems with IPFS Cluster and Prometheus support. This allows users/developers to collect the maximum track record.

8. REFERENCES

[1] Y. Prayudi, A. Ashari, and T. K Priyambodo, “Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody,” Int. J. Comput. Appl., vol. 107, no. 9, pp. 30–36, 2014.

[2] A. Agarwal, M. Gupta, and S. Gupta, “Systematic Digital Forensic Investigation Model,” International Journal of Computer Science and Security, vol. 5, no. 1, pp. 118–134, 2011.

[3] G. Giova, “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” International Journal of Computer Science and Network Security., vol. 11, no. 1, pp. 1–9, 2011.

[4] N. Gaur, L. Desrosiers, A. O’Dowd, et. al., “Blockchain with Hyperledger Fabric,” Mumbai: Packt Publshing Ltd. Novembar 2020.

[5] S. Bonomi, M. Casini, and C. Ciccotelli, “B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics,” 2018.

[6] E. Yunianto, Y. Prayudi, and B. Sugiantoro, “B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management,” International Journal of Computer Applications, vol. 181, pp. 22-29, 2019

[7] A. Lone, R. Mir, “Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer,” Digital Investigation, vol.28, 2019.

[8] E. Nyaletey, R. Parizi, Q. Zaeng, K. Choo, “BlockIPFS - Blockchain-enabled interplanetary file system for forensic and trusted data traceability,” Proceedings - 2019 2nd IEEE International Conference on Blockchain, pp.18-25, 2019.

[9] K. Widatama and Y. Prayudi, “The Concept of Digital Proof Storage Cabinets Using XML Language Structures,” 3rd Natl. Semin. Inf. Appl., no. September, p. 23, 2017 : In Indonesia language.

[10] J. Nord, A. Koong, J. Paliskewicz, “The Internet of Things: Review and theoretical framework,” Vol. 133, pp. 97-108, 2019.

[11] M. Benerjee, J. Lee, K. Choo, “A blockchain future for internet of things security: a position paper,” Digital Communications and Networks, Vol. 4, pp. 149-160, 2017.

[12] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. 2016 Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. IEEE Symp. Secur. Privacy, SP 2016, pp. 839–858.

[13] D. Sharma, S. Pant, M. Sharma et al, “Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications,” Handbook of Research on Blockchain Technology, pp. 323-348, 2020.

[14] W. Peng, L. Yi, L. Fang, D. Xinhua, and C. Ping. 2019 Secure and Traceable Copyright Management System Based on Blockchain. IEEE 5th Int. Conf. Comput. Commun. ICCC 2019.

[15] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Tech. Rep., 2008. Accessed: Jan. 15, 2021. [Online]. Available: https://archive.is/rMBtV

[16] N. Baygin, M. Karakose, “CopyrightChain: Permissioned Blockchain-based Collaboration and Design Right using Hyperledger Composer and IPFS,” International Journal of Computer Applications, vol. 183, pp. 19-26, 2021.

[17] G. Wood, ‘‘Ethereum: A secure decentralised generalised transaction ledger,’’ Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2014.

[18] J. Benet. (2014). ‘‘IPFS-content addressed, versioned, P2P file system.’’ [Online]. Available: https://arxiv.org/abs/1407.3561.

[19] A. Prashanth Joshi, M. Han and Y. Wang, "A survey on security and privacy issues of blockchain technology",

Mathematical Foundations of Computing, vol. 1, no. 2, pp. 121-147, 2018.

[20] H. Halaburda, "Blockchain Revolution Without the Blockchain", SSRN Electronic Journal, 2017.

[21] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain", 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017.

[22] G. Chen, B. Xu, M. Lu and N. Chen, "Exploring blockchain technology and its potential applications for education", Smart Learning Environments, vol. 5, no. 1, 2018.

[23] M. Yassein, F. Shatnawi, S. Rawashdeh et al., “Blockchain technology: Characteristics, security and privacy; Issues and solutions,” pp. 1-8, 2019.

[24] Welcome to Hyperledger Fabric. https://hyperledger-fabric.readthedocs.io/, accessed Oct 2021.

[25] A. Rasti and A. Gheibi, “A coin marketplace implementation on blockchain using the Hyperledger platform,” 2018.

[26] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1–1, 2016.

[27] N. Szabo, “Formalizing and securing relationships on public networks,” First Monday, vol. 2, no. 9, 1997. [Online]. Available: http: //ojphi.org/ojs/index.php/fm/article/view/548.

[28] H. Liu, D. Han, D. Li, “Fabric-iot: A Blockchain-Based Access Control System in IoT,” IEEE Access, vol. 8, pp.18207-18218, 2020.

[29] Hyperledger Composer, “Key Concepts in Hyperledger Composer”, Available at: https://hyperledger.github.io/composer/latest/introduction/key-concepts, accessed Oct 2021

[30] O. Wennergren, M. Vidhall, and J. Sörensen, ‘‘Transparency analysis of distributed file systems: With a focus on interplanetary file system,’’ Tech. Rep., 2018.

[31] NATIONAL INSTITUTE OF JUSTICE. U.S. National Institute of Justice. Death Investigation: A Guide fo The Scane Investigator, 2011. Avalible at: https://www.ojp.gov/pdffiles1/nij/234457.pdf. Acessed Oct 2021.

[32] NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY. U.S. National Institute of Standards Technology. Crime Scane Investigation: A Guide for Law Enforcement, 2013. Avalible at: https://www.nist.gov/system/files/documents/forensics/Crime-Scene-Investigation.pdf. Acessed Oct 2021.