International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Accountability of Course Graduation Records using Permissioned Blockchain in Hyperledger Fabric

Linda Handayani[1], Avinanta Tarigan[2]

[1]Graduate Program of Information System, Gunadarma University. Jl. Margonda Raya no.100, Depok, 16424, Indonesia

[2]Faculty of Magister Information System, Gunadarma University. Jl. Margonda Raya no.100, Depok, 16424, Indonesia

Abstract: ***Blockchain technology could be implemented not only in digital currency, but also in other fields. For example implementation is in education sector, namely graduation information system. Information system aims to facilitate the process of sending information carried out by parties involved in the system. But this often has problems, including caused by the condition of the system that is often down, process that is still manual (not integrated), human mistakes until data security. In this research we propose the system run on the decentralized and stored in distributed ledger and facilitate the audit process by monitoring data transparently, secure, immutable and accountability. This purpose of this research is to implement permissioned blockchain for storing the graduation records (log and course records) and develop a web application based chaincode to ensure the security authorized participants using Hyperledger Fabric. The data used are graduation data and stakeholders as participants (admin system) who will the use the application. Participants, namely bank admin, course admin (based on four regions) and auditor. The results shows developing web applications that implement the permissioned blockchain type consortium in Hyperledger Fabric and performance technology through system testing and data validation testing.***

Keywords: Blockchain, Permissioned Blockchain, Consortium, Accountability, Hyperledger Fabric, Graduation Records, Course Records, Log, Graduation Information System.

1. Introduction

Recent development of information and communication technology is advacing rapidly. The performance and efficiency of hardware and software have continued to improve in the last few decades. Moore's Law, based on Gordon Moore's observations in 1965 and later adjustment in 1975, stated that the size of transistors were shrinking so fast that every two years, twice as many could fit onto a single computer chip [2]. Operating systems, programming languages, and application programs that function as regulators of computer systems made significant updates. This advancement has revolutionized many aspects in our social life, one of which is in the field of education.

Nowdays, educational information system are applied to facilitate services in the form of administration, learning, until graduation. User of information system are not only intended for student, but for staff, teachers, and related parties who take care of services within educational institution. This aims to facilitate the process of sending information carried out by parties involved in the system. But this often has problems, including caused by the condition of the system that is often down, the process of sending information that is still manual (system not yet integrated), human mistakes until data security.

In general, the database is stored in a centralized system. Centralized systems have common weaknesses. The data are stored centrally, so they have central point of failure, which can be exploited by computer crackers. Those systems are usually handled by single organization, so the data can be manipulated secretly by those who have administrative access to the database [3]. Log history can be used as tracking for monitoring systems from human mistake. But saving logs on centralized file is not recommended because if a file is deleted there is no record of this action. This is a problem that occurs in a database [1]. The recent development of blockchain technology can solve this problem

In 2008, Satoshi Nakamoto wrote about a "Bitcoin : A peer to peer electronic cash system" Blockchain – is a distributed ledger technology based on the principles of peer-to-peer network and cryptographic primitive (such as hash, asymmetric encryption and digital signature) [4]. Since then, the blockchain has been introduced to the public. Over time, people started to realize that blockchain could be used beyond cryptocurrency and they started to explore how blockchain could be used for existing systems, including in the data record process in the education system.

Blockchain is provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different block. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. Data is stored in each block that can be verified simultaneously and becomes immutable and accountability. The whole process is open (public), transparent, and secure [5].

Hyperledger is one of the popular permissioned blockchain platform hosted by the Linux Foundation's Hyperledger project [6]. This platform is built for business consortium interested in building and deploying their blockchain applications with shared data. A blockchain deployed using Hyperledger Fabric stores data in the form of chaincode, a programmatic code on the network that functions similar to smart contracts on other blockchain [7]. The success of hyperledger would provide users another way to implement a blockchain and give them control over parameters in the

blockchain network.
The purpose of this study is to implement permissioned blockchain for storing the graduation records (course records and log data) and develop a web application based chaincode to ensure the security authorized users using Hyperledger Fabric platform. The success indicator of this research is stored data on distribute ledger and run on decentralized system that are secure and facilitate the audit process by monitoring data transparently, secure, immutable and accountability.

This study is limited by the following. First, Identification of participants or stakeholders, graduation data, and workflows obtained from the observation of one of the course educational institutions. Second,implementation of a web application on decentralized and distribute ledger system using the Hyperledger Fabric platform, ChainHero template, Fabric SDK and Golang. Third, the system displays event logs, blocks and course records to see the resumes of the course. Fourth, developing and testing are done on the local machine and docker.

This paper is organized as follows. Section II contains literature study. Section III contains research methodology. Section IV contains results and discussion. Section V contains concluding remarks and posibilities of further improvements.

2. Literature Study

2.1 Related Work

In the study of Managing lifelong learning record through blockchain, in 2019, Patrick et al conducted study on implementation for track of learning achievements beyond transcript and certificates. The blockchain of learning logs enables existing learning data analytic platforms to access the learning logs from other institution who originally have ownership of the logs. The results showed that plot difficulty in mining the different blocks representing our learning log transactions over time and performance system offers a high degree of privacy through smart contract based access authorization where learners can actively determine who can collect their learning logs and access them at a later time [8].

Arati et al (2017) conducted study on characterize the performance and scalability features of the current production release of hyperledger Hyperledger Fabric. Through a suite of microbenchmarks, custom-built for Hyperledger Fabric, we tune different transaction and chaincode parameters and study how they affect transaction latencies. The result showed large consortiums can be built, the endorsements per chaincode should be limited to a smaller subset of peers, with an eye on performance [9].

IMS Global Learning Consortium (2017) developed a Comprehensive Learning Record (IMS CLR) to capture and communicate a learner's achievements in verifiable digital form. In particular, it supports traditional academic programs, co-curricular, and competency-based education, IMS CLR contains data such as courses, competencies, employability skills, degrees, and certificates. While IMS CLR contains more detail the usual transcript or certificates, it does not provide digital logs of behaviors and activities performed during learning [10].

2.2 Blockchain

Blockchain is a shared ledger of transactions. The transactions are ordered and grouped into block. Currently, the real-world model is based on private databases that each organization maintains, whereas the distributed ledger can serve as single source of truth for all member organizations that are using the blockchain. Blockchain is also a data structure, a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block [11]. Blockchain employs consensus algorithm to achieve decentralization of control. Consensus provides a way for all peers to agree and accept a single version of truth on the blockchain network.

2.3 Data Structure (Data Ledger Layer)

The data structure of a blockchain, whether public or consortium, corresponds to a list of blocks containing transactions also referred to as the "ledger". Each element of the list, has a pointer to previous block and embodies its hash value as illustrated in Figure 2.1. Consortium chains members can come to an agreement and alter previous blocks (i). In order to prove that data were not tempered and preserve the auditability of the ledger, it is common to periodically publish the hash of a block onto a public blockchain. By doing so, one can be assured that blocks in the interval of two published hashes have not been modified [12].

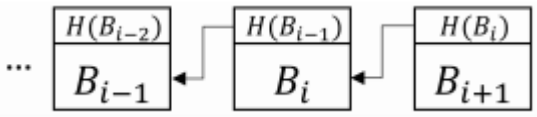

Figure 2.1: List of linked blocks with hash pointers [12].

2.4 Network/P2P Exchange Layer

Along with its data structure, a blockchain is based on a peer-to-peer network that links its members. Members participate to the network through their blockchain client node. Each node has a local copy of the whole linked list (or the most recent part of it in case of light nodes [13]). When retrieving the list for the first time, node verifies the integrity of the blocks by computing all the hashes and keeps verifying each new block.

The identity of a participant is defined by his cryptographic asymmetrical key pair. The public key is derived to obtain his unique address, which serves as his public identity. The private key is used to sign transactions and guarantee their authenticity (i.e., other participants can verify the signature using the associated public key). In order to add data to the blockchain, a node sends a transaction request to the network. The prime data fields of a transaction in most technologies are the addresses of both sender and receiver, data values that are being communicated and the signature of the sender. These transactions' requests are then picked by some special nodes called miners also referred as to block generators or validators on consortium blockchains [12**].**

2.5 Smart Contract

A smart contract is "a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain" [14]. Smart contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in blockchains are copied to each node to prevent contract tampering.

2.6 Hyperledger Fabric

Hyperledger Fabric enables participating organizations within consortium to build and deploy blockchain applications. The blockchain network consists of several nodes (or peers) that host the blockchain, execute smart contracts (known as chaincode) and collectively maintain the state of the ledger. Chaincode can be shared by all entities within a consortium or could be privately deployed to be accessible to a subset of entities. Private chaincode are run only on peers with whom the chaincode is shared and is inaccessible to others. This is achieved via a concept of channels in Hyperledger Fabric where all chaincode and data on the channel is only accessible to entities that are part of the channel.

In the setup phase, the peers need cryptographic material that is generated to identify and authenticate the peers to the blockchain network. In this way, it can be determinedwhether a given peer belongs to a particular channel. In addition to peers, the Hyperledger Fabric network also needs an ordering service/orderer. The ordering service performs a total ordering of the transactions accepted by the Hyperledger Fabric network on a perchannel basis. The current production version does not support any form of consensus algorithm for ordering. It is expected to be incorporated in the future versions. Transactions in Hyperledger Fabric are invocations of chaincode methods. The chaincode itself is run within a Docker container thus isolating itself from the Hyperledger Fabric code as well as other chaincode running on the same peer machine. Each chaincode has a persistent state called the key-value store. Chaincode methods manipulate the values of the key-value store using put and get methods that essentially allow it.
Transactions in Hyperledger Fabric go through the following steps as shown in Figure 2.2:

1) Client initiates a transaction: A client prepares a request proposal to invoke a chaincode function. The request is signed by the client and sent on the channel where the chaincode is deployed. The number of endorsements that it expects to receive is as per the endorsement policy of the chaincode.
2) Endorsing peers verify signature and execute the transaction: The endorsing peers perform all the validity checks for well-formedness, authenticity, replayprotection and client authorization. If all checks are successfully cleared, the peers execute the transaction against their own key-value stores and produce a response that include read-write sets generated as a result of chaincode execution. These values, signed by the peers are sent back to the client as a proposal response or endorsement. No changes to the ledger are made at this point in time.
3) Client collects endorsements and sends to the ordering service: The client examines and compares all the endorsements and verifies that it has met the endorsement policy requirements of the chaincode. If the request was a read request, it does not send a request to the ordering service. If the request is a chaincode invoke (or write), it assembles the endorsements into a transaction and sends it to the ordering service for inclusion into the blockchain. The ordering service verifies transactions and orders them per channel.
4) Transaction is validated and committed: Ordered transactions within blocks are delivered to all peers on the channel by the ordering service. The peers verify the transaction and endorsement policy fulfillment; if all checks go through, the peers add the block to the ledger. Note that all peers have to commit the transaction (and therefore play the role of a committing peer), while endorsement can be delegated to only a subset of peers on the channel and are referred to as endorsing peers (EP).

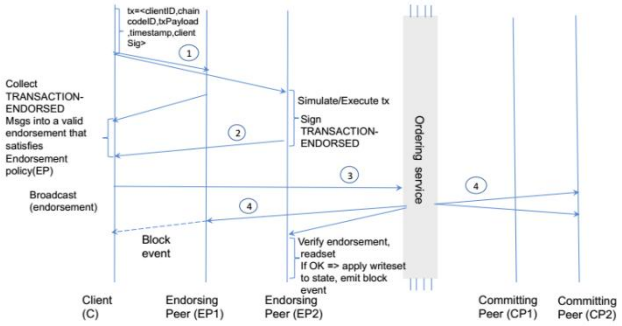

Figure 2.2: List of linked blocks with hash pointers [7].

3. Research Methodology

In this study, researchers adopted the design-based research (DBR) methodology [15]. Wang and Hannafin (2005) define DBR as a research method which focuses on exploring systematic but flexible techniques targeted at improving educational practice through iterative analysis, design, development and implementation requiring collaboration between researchers and practitioners and leasing to new useful principles. In general, the stages of research conducted by researchers can be seen in Figure 3.1. This research is divided into four stages. Stage one is data collection, stage two is system design, stage three is the implementation of blockchain technology in Hyperledger Fabric, and stage four is the result of applying system in Hyperledger Fabric.

The data collection stage consists of two steps, namely: interview, and document observation. The system design stage is preparing a workflow diagram of applications that are run on a web-base, Then the stage of implementing blockchain technology consist of five steps, namely: set up the blockchain network, enroll admin and register user

(participant) enrollment, querying the ledger, and consensus protocol transaction in chaincode. The last stage is the result of implementation. The results stage consists of developing a web-based system using blockchain technology and performance in Hyperledger Fabric.

3.1 Data Collection

The data collection methods in this research used two ways, those are interview and documents observation. The following is explanation of each of the data collection methods:

1) Interview
Interviews were conducted to obtain a more complete description of the issues studied. Interviews were conducted to find out the problems related to the process of implementing system and to determine the performance levels system expected by course institutions in the future.

2) Observation Documents.
Documents observation is done by observing and studying every documentations and report through a source that provides information about the graduation of course student such as graduation data, and an overview of the workflow system is used.

3.2 System Design

Based on data collection, the researchers propose blockchain technology to be implementation in the graduation information system in the course institution. Blockchain is applied to the Log and Course Record of the Course Chain applications web-based. The system will run in the decentralized network and submit transactions that are immutable and secure. Transaction ordering and validates the block of transactions will be carried out by consensus protocol. Validated transactions are stored in the ledger and distributed to all nodes participants on the blockchain.

The permissioned blockchain type consortium is used for participants who will join the blockchain network and can interacts with the system. Participants in system consist of three entities as stakeholder, namely: Bank, Course Institution (there are 4 regional branches), and Auditor. Blockchain will determine the smart contract (chaincode) to access and implement the classification and indexing mechanism easily and quickly when searching for data. In general, the researchers designed the application workflow diagram for the graduation course system in Figure 3.2.

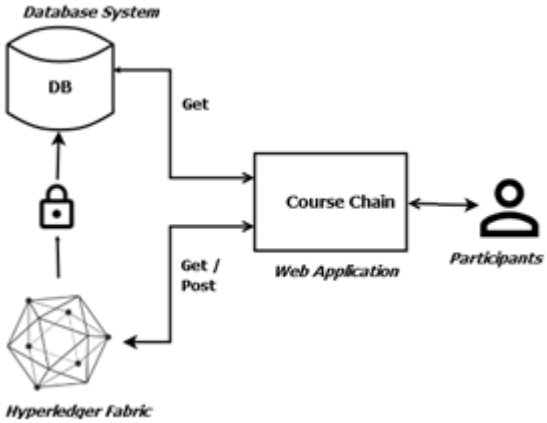

Figure 3.2: Application Workflow Diagram

In Figure 3.2 shows the participants in the diagram consists of the Bank admin, Course admin (based on the Cengkareng, Depok, Bekasi, and Karawaci regions), and Auditor. Participants interacts with the course chain application web interface to do CRUD based on authorization. In Table 3.1 shows the participants authorization on the application. The Course Chain web application interacts with the database system to get data and submit transactions to the Hyperledger Fabric. Transactions in Hyperledger Fabric consist of Log and Course Record data that will be stored in the block and validated using chaincode on the consensus protocol blockchain. If the transaction in the Hyperledger Fabric is successful, then the data will be sent to the database system to update.

Table 3.1: Authorization Participants on the Application

Menu / Participants	Input Data	Course Record	Event Log	Block
Admin Bank	CRUD	-	R	R
Admin F4	CRUD	R	R	R
Admin J5	CRUD	R	R	R
Admin K	CRUD	R	R	R
Admin L	CRUD	R	R	R
Auditor	-	R	R	R

3.3 Implementation of Blockchain in HyperledgerFabric

1) Set up Blockchain Network
In order to make a blockchain network, the researchers use blockchainconfig template from ChainHero and docker to build virtual computers that will handle different roles. Hyperledger Fabric needs a lot of certificates to ensure encryption during the whole end to end process (TLS, authentications, signing blocks and other process).

```
version: '2'
networks:
      default:
      services:
orderer.hf.ChainHero.io: ...
ca.org1.hf.ChainHero.io: ...
peer0.org1.hf.ChainHero.io: ...
peer1.org1.hf.ChainHero.io: ...
```

In the docker configuration, the author defines several services which include:

- Orderer

List of orderers to send transaction and channel create/update requests to. For the time being only one orderer is needed. If more than one is defined, which one get used by the SDK is implementation specific. Consult each SDK's documentation for its handling of orderers.

- Certificate Authorities (CA)
  Certificate Authorities issue certificates for identification purposes in a Fabric based network. Typically certificates provisioning is done in a separate process outside of the runtime network. Fabric-CA is a special certificate authority that provides a REST APIs for dynamic certificate management (enroll, revoke, re-enroll). The following section is only for Fabric-CA servers.
- Peers
  List of peers to send various requests to, endorsement, query and event listener registration.

1) Enroll Admin and Register Participants Enrollment.

In the enroll admin and register user enrollment, researchers configured the Hyperledger Fabric as in the example below.

```
certificateAuthorities:
  ca.org1.hf.ChainHero.io:
        url: http://localhost:7054
        httpOptions:
              verify: false
        registrar:
              enrollId: admin
              enrollSecret: adminpw
        caName: ca.org1.hf.ChainHero.io
```

2) Querying the ledger

In the process of data transactions at ledger, a query is needed to do so as needed. The following is a QueryRecord function that functions to request ("invoke") queries for key records. The function willreturn the results of the query record response from chaincode.

```
func (setup *FabricSetup) QueryRecord() ([]byte, error) {
  var args []string
  args = append(args, "invoke")
  args = append(args, "query")
  args = append(args, "record")

  response, err := setup.client.Query(channel.Request{
      ChaincodeID: setup.ChainCodeID,
      Fcn: args[0],

      Args: [][]byte{[]byte(args[1]), []byte(args[2])}
  })
  if err != nil {
      return nil, fmt.Errorf("failed to query: %v", err)
  }
  return response.Payload, nil
}
```

3) Consensus Protocol Transaction in chaincode

The response obtained in the QueryRecord function comes from the function query in chaincode. In the query function, a process is performed to retrieve the ledger state (GetState) for each key (args [1]) of the requested argument.

```
func (t *HeroesServiceChaincode) query(stub
shim.ChaincodeStubInterface, args []string)
pb.Response {
if len(args) < 2 {
returnshim.Error("The number of arguments is
insufficient.")
}
// Get the state of the value matching the key hello in
the ledger
state, err := stub.GetState(args[1])
if err != nil {
returnshim.Error("Failed to get state of hello")
}
// Return this value in response
returnshim.Success(state)
}
```

The response obtained in the InvokeRecord function from the web application, is obtained from the invoke function in chaincode. In invoke function, a process is performed to give data ledger state (PutState) to the key (args [1]) and contain the value (args [2]) of the requested argument.

```
func(t*HeroesServiceChaincode)invoke(stubshim.Chain
codeStubInterface,args[]string)pb.Response{
iflen(args)<2{
returnshim.Error("Thenumberofargumentsisinsufficien
t.")
}
iflen(args)==3{
//Writethenewvalueintheledger
err:=stub.PutState(args[1],[]byte(args[2]))
iferr!=nil{
returnshim.Error("Failedtoupdatestateofhello")
}
//Notifylistenersthatanevent"eventInvoke"havebeenex
ecuted
err=stub.SetEvent("eventInvoke",[]byte{})
iferr!=nil{
returnshim.Error(err.Error())
}
//Returnthisvalueinresponse
returnshim.Success(nil)
}
//Iftheargumentsgivendon'tmatchanyfunction,wereturn
anerror
returnshim.Error("Unknowninvokeaction,checktheseco
ndargument.")
}
```

3.4 Result Stage

At this stage contains the results of the implementationpermissioned blockchain type consortium technology in a previously designed system in the form of developing a web-based graduation system in Hyperledger Fabric. In addition, the performance of the system will be known through system testing and performance testing. System testing is done using BlackBox testing techniques and data validation testing, while performance testing is done by looking at the character of the latency node per access.

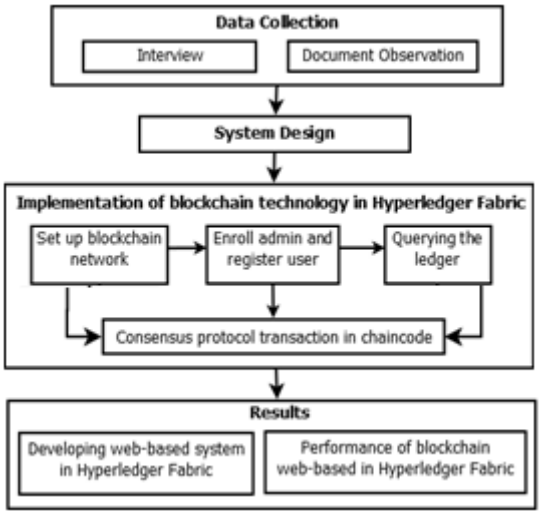

Figure 3.1: Research Stages

4. Results and Discussion

4.1 Results

The results contain developing web application and Performance of system applications.

1. Developing a Web Application

The development of system is carried out by implementing the blockchain technology in Hyperledger Fabric in Chapter III. The development of a web-based system consists of several features used by participants.

Figure 4.1: Run program

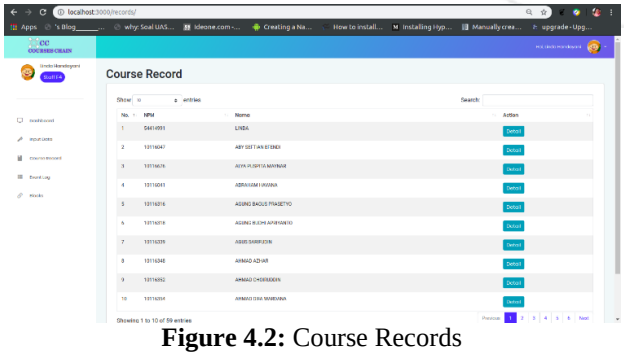

Figure 4.2: Course Records

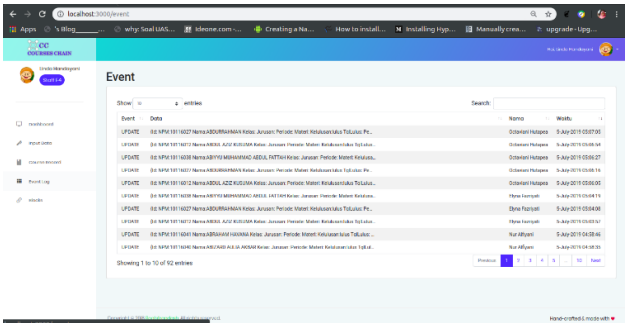

Figure 4.3: Event Log

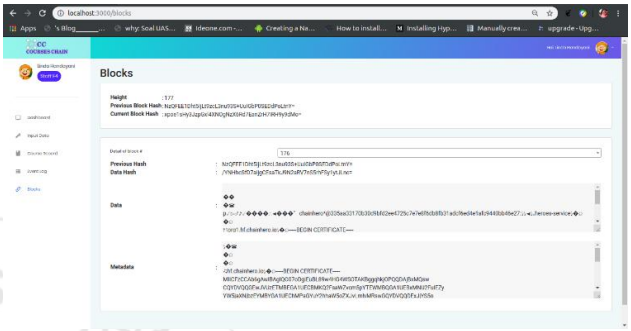

Figure 4.4: Blocks

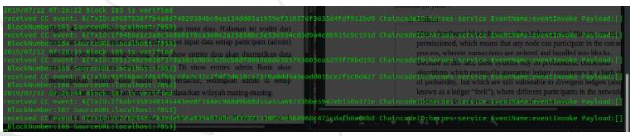

Figure 4.5: Transaction running

4.2 Performance

Performance measurement seen fromsystem testing and data validation testing.

Table 4.1: System Testing

Function	Input	Expected Output	Output	Result
Login	Admin input username and password with match data	Login directs to menu page	Login directs to menu page	Success
Input Data	Admin input graduation data student	The data will be stored in the show entries	The data will be stored in the show entries	Success
Course Record	Admin click course record menu	Display the course record page contain a list of show data entries	Display the course record page contain a list of show data entries	Success
Event Log	Admin click even log menu	Display the event log page contain a list of show data entries	Display the event log page contain a list of show data entries	Success
Blocks	Admin click blocks menu	Display the blocks page contain height block, pervious block hash, current block hash, and detail of block	Display the blocks page contain height block, pervious block hash, current block hash, and detail of block	Success

Table 4.2: Data Validation Testing

No	Scenario	Output	Result
1	If the data is successfully ordered and validated block transactions	The data will be updates in the ledger and sent to the database system	Success
2	If the data is not successfully ordered and validated block transactions	The data will not be updated ledger and there is no sent to the database system	Success

4.3 Discussion

Each participant has the authority in the system to access the blockchain network. In order to make network use the blockchain config template from the ChainHero and docker to build virtual computer that will handle different roles. In that process, the function request ("invoke") queries for key records. The function will be the results of the query record response from chaincode. The prepared argument for invoking the ledger key record. Then make an event declaration and description of the data for request invoke. Then the registration and execute transaction requests chaincode event. The record are stored in ledger is course records and log for monitoring data.

5 Conclusions

Based on the results of development and testing, the system is proposed to work well and answer the problem. Participants interact with the decentralized web application based on authority. The course record and log features are stored in blocks that can be seen in the blocks feature. The blocks feature contains information about the height block, previous block, current block and details of the block. Changes to data are stored in a distributed ledger on each node. Facilitate the audit process by monitoring data transparently, secure, immutable and accountability. In the future, the system could be tested on latency network and database access.

References

[1] McDowall. 2007. “Rd validation of spectrometry software -audit trails for spectrometer software.” *Spectroscopy*, page 16 to 18, April 2007. URL http://spectroscopyonline.findanalytichem.com/spectroscopy/ data/articlestandard/spectrscopy/172007/421873/article.pdf.

[2] J. L. Hennesy& D. A. Patterson. 2017. “Computer Architecture: A Quantitative Approach”. *Book.* Burlington: Morgan Kaufmann, 4th edition.

[3] The Economist. 2015. “The great chain of being sure about things”. *Article*.URL https://www.economist.com/briefing/2015/10/31/ the-great-chain-of-being-sure-about-things.

[4] Satoshi Nakamoto. 2008. “Bitcoin: A peer-to-peer electronic cash system”. *Journal*. URL https://bitcoin.org/bitcoin.pdf..

[5] Lee. &Chien Chi. Jiin-Chiou, Cheng.;Narn-Yih, editor. 2018. “Blockchain and Smart Contract for Digital Certificate”. *Proceedings of IEEE International Conference on Applied System Innovation2018*. ISBN 978-1-5386-4342-6.

[6] Hyperledger. 2019. “Introduction to hyperledger business blockchain design philosophy and consensus”. *Hyperledger Architecture*, 1, 2019.

[7] Patrick Ocheja. 2019. “Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(4):1–19, 2019.doi: 10.1186/s41039-019-0097-0.

[8] AratiBaliga. 2018. “Performance characterization of Hyperledger Fabric”. *In the First Crypto Valley Conference on Blockchain Technology (CVCBT 2018).*

[9] MS Global Learning Consortium. 2017. “Comprehensive learner record”. URL https://www.imsglobal.org/activity/comprehensive-learner-record.

[10] Imran Bashir. 2017. “Mastering Blockchain”. *Birmingham: Packt Publishing Ltd.*

[11] Omar Dib.; Kei-Leo Brousmiche. & Antoine Durand. 2018. “Consortium blockchains: Overview, applications and challenges”. *International Journal on Advances in Telecommunications*, 11(1 & 2), 2018. URL http: //www.iariajournals.org/telecommunications/.

[12] James Ray. 2018. “Light client protocol”. URL https://github.com/ethereum/wiki/wiki/Light-client-protocol.

[13] Xiuping Lin. 2017. “Semi-centralized blockchain smart contracts: Centralized verification and smart computing under chains in the ethereumblockchain”..*Department of Information Engineering, National Taiwan University, Taiwan, R.O.C.*

[14] M.J. Wang, F. &Hannafin. 2005.“Design-based research and technology-enhancedlearning environments”. *Educ. Technol. Res. Dev*, 53(4):5–23.