B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management

Eko Yunianto
Department of Informatics
Universitas Islam Indonesia
Yogyakarta Indonesia

Yudi Prayudi
Department of Informatics
Universitas Islam Indonesia
Yogyakarta Indonesia

Bambang Sugiantoro
Department of Informatics
UIN Sunan Kalijaga
Yogyakarta Indonesia

ABSTRACT
Digital evidence handling and preservation are one stage of digital forensic process. This part is very crucial because digital evidence is the basis of digital forensic process. The credibility of digital evidence must be maintaned for law and court process. Process of preservation of digital evidence known as chain of custody (CoC). CoC is a document that used to ensure that digital evidence remains and does not change. Both during the investigation process until the completion of the forensic process. Electronic evidence documentation is different from digital evidence documentatation. The different are character and the metadata. Some adjustments need to be accomodated on system for digital evidence. Digital evidence is easy to change as well as its CoC document. It needs to be protected. A new technology is needed that can ensure integrity of digital evidence and CoC Document like the blockchain. In this study, digital evidence management will be built on the CoC concept with blockchain technology. More precisely, this design combines the framework of the Digital Evidence Bag (DEC) with blockchain technology. This prototype is known as the Blockchain Digital Evidence Bag (B-DEC). B-DEC utilizes the data storage integrity to accommodate digital evidence management that refers to DEC. In this case, the prototype will build on a smart contract based on Ethereum. The development of the DEC framework also will be adjusted to accommodate DEC applications in the blockchain.

General Terms
Blockchain, Chain of Custody.

Keywords
Digital Forensic, Chain of Custody, Digital Evidence, Blockchain.

1. INTRODUCTION
Every process and step to digital evidence handling must be well documented in accordance with the standards. Referring to ISO 27037: 2014 that it has been clearly regulated with regard to the stages and guidelines for the process of handling digital evidence. There are many step from identification, collection and preservation of digital evidence [1]. In implementation, there are many obstacles due to wrong handling. One reason there is no competent law enforcement staff. This problem refers to the unavailability of officers related to digital evidence and its handling [2].

Basically the problem in digital evidence are authentication and chain of custody (CoC) [3]. The problems can interference with the integrity of evidence in court. Possible for the court do not accept the evidence. Preservation of digital evidence can be realized in the form of CoC documents to ensures the integrity of the evidence. It contains the history of evidence. Starting from the beginning until the disposal of evidence.

CoC documents must be able to accommodate each type of evidence. So the errors that often occur when handling and preservation of evidence can be minimized. One of the mistakes is the overlapping handling of physical evidence and digital evidence. Of course this can be recognized by the existence of a management system that suits your needs [4].

There are many obstacles to implement of evidence preservation documents in various regions. This obstacle is the officers do not separate physical evidence and digital evidence. This makes preservation of digital evidence considered the same as physical evidence. Though digital evidence is the core evidence extracted from physical evidence. The different types of evidence should be accommodated by the Coc document. It means traditional paper-based chain of custody is inefficient and cannot guarantee that the forensic processes follow legal and technical principles in an electronic society [5].

Various types of digital evidence management have been developed. Development is done starting from simple XML documents to complex frameworks. The Digital Evidence Cabinet (DEC) is one of them [6]. DEC is a digital evidence management approach with the concept of storing physical evidence. DEC was built the concept of evidence storage cabinets for digital evidence. In implementation, the rules for using physical cabinets must be able to be accommodated in the digital domain. DEC has some stage. There are cabinet, rack, bag and evidence tag. Some tag explain for the spesific level.

DEC is formulated with an XML structure [7]. This structure is open and easy to change. On the other hand there is blockchain technology. This technology can ensure authentication and verification of stored data. This technology uses a chain of block storage system. The data consistency can be maintained. This can be happen because each block has a hash value. The hash value is interconnect with another block. For this reason, a prototype was developed in this study. The prototype combines blockchain technology with the DEC approach. This prototype is then called the Blockchain Digital Evidence Cabinet (B-DEC)

2. CURRENT ISSUE
Chain of Custody (CoC) is a document for preservation of evidence. The CoC should be able to accommodate various kinds of evidence. According to [8] most country use CoC pyshical document to accomodate all. It will be used during digital forensic period.

Some electronic evidence has a storage media. In this storage media there are data and information. This data and information is digital data that easy to change. CoC's big challenge is handling electronic evidence and digital evidence. This digital evidence is the result of extraction from electronic evidence.

The physical CoC document is only able to record information on electronic evidence. Digital evidence is often ruled out or a separate document is made. The concept of digital evidence management still does not meet the rules. This digital evidence can be shared and accessed easily. Even in the investigator's circle.

The process of accessing digital evidence is also still not accommodated by the CoC document. At most the process of sharing digital evidence access is made in the minutes. And this must be separate from CoC. Or at least the minutes are attached to the CoC document. Some errors will be encountered when using traditional processes. Especially in the data integrity section because digital data is easily changed. The tampering issue will always be there. This happens because the exchange process is not well documented.

Integrated system is needed for all these problems. This system must be able to present data that has proven integrity. This system must be able to accommodate CoC documents for electronic evidence and digital evidence. Based on this, it is possible to build new concepts to use the blockchain as a metadata storage media. The other issue is create DEC to be an concept of digital evidence management.

3. DESIGN SYSTEM

3.1 Private Network Ethereum

Blockchain is a concept of data storage technology. Storage of data on the blockchain is saved on the block [9]. The block on the blockchain is interconnected with a link to the hash value for each block. This makes the blockchain can be proven the integrity of the data stored. Impossible to make data changes in the middle of the block link. Changing data in the middle of the block makes the block link disappear.

The Blockchain uses a consensus concept to verify a transaction. This consensus is like a notary who witnesses a transaction. The consensus make sure each transaction has its own witness mechanism. There are several types of consensus on the blockchain. According to [10] there are at least 6 namely Proof of Work (PoW), Proof of Stack (PoS), PBFT, DPOS, Ripple and Tendermint. All types of consensus depend on the way the blockchain communicates with data storage.

According to [11] there are 3 types of blockchain :

a. Public blockchain is an open type of blockhain. This type of blockchain can be accessed and participated freely. Everyone can make a contribution. Examples of this type of blockchain are Bitcoin and Ethereum

b. Pemission blockchain is a type of blockchain with a limited scale. This type of blockchain requires user management. This type of blockchain has a large scale, but the source code is closed. An example of a system that uses this type is Ripple

c. The private blockchain is a private blockchain for small scale. This blockchain was developed and fully controlled by the internal. Usually used to exchange confidential information.

The ethereum private network is built on a private network and uses PoA consensus. This concept allows implementation without a minner and high computer specifications. This is very suitable for the implementation of Chain of Custody. Confidentiality, convenience and security are very important to this concept. Ethereum's private network design will be represented by Ethereum Virtual Machine (EVM)

3.2 B-DEC Architecture

Blockchain is the technology chosen as the basis for the construction of a B-DEC system (Blockchain-Digital Evidence Cabinet). B-DEC develop with DEC technology and blockchain technology to chain of custody management. Furthermore the architecture of B-DEC can be seen in Fig 1.

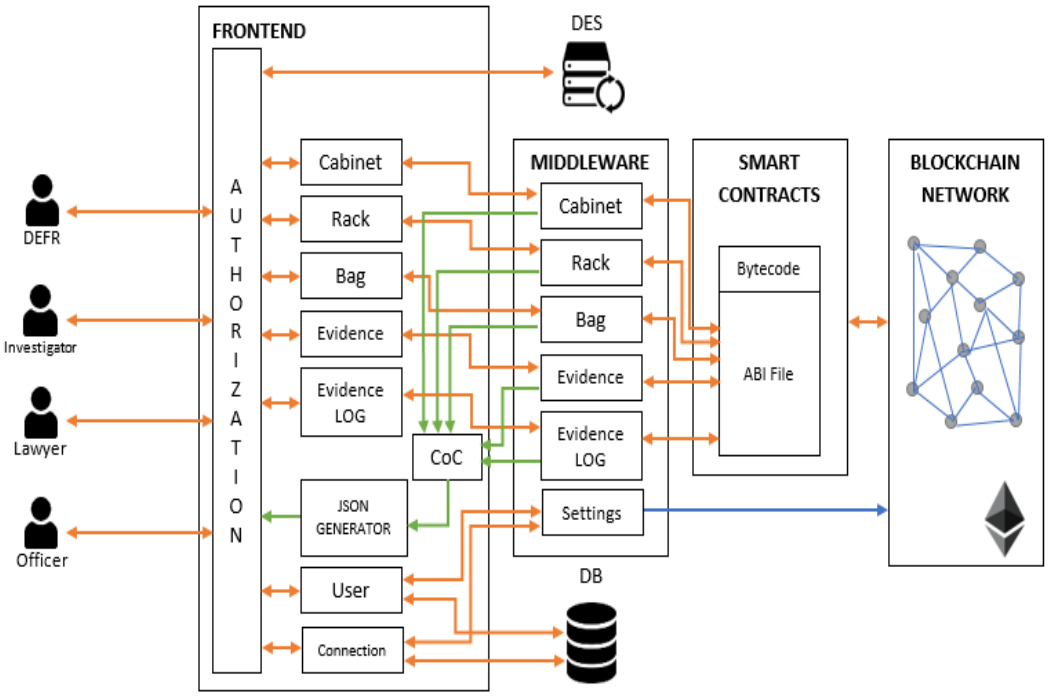

Fig 1: B-DEC Architecture

Fig 1 briefly explain the B-DEC architecture. In the picture, the interaction between the system and the B-DEC architecture has several layers. Some of these layers are:

a. Frontend, is a leading part of the B-DEC system. This section is designed as an interface that contains authorization, access rights and media. It can be used to download digital evidence and chain of custody documents in accordance with access rights and levels.

b. Middleware, is a translating part between the interface part and smart contract.

c. Smart Contract, is the most important part where smart contract is used to interact with the ethereum network on the blockchain network. This section is part of the code written using solidity language that has been adapted to the needs and compiled in byte code.

d. The Blockchain Network, which is a private network built using EVM. In this block, all transactions will be processed through interconnected periods.

e. Evidence Storage and Database are a database of digital evidence that can be accessed by authorization. In this section, it will be separated between evidence sources and evidence work

3.3 Smart Contract and Web 3

Smart Contracts are self-executing programs which run on the blockchain and are capable of enforcing rules, consequences and computation over every transaction happening in the blockchain [12]. Smart Contracts can run on the blockchain as a side chain. It means if something happens in the side chain it will not have an impact on the main blockchain [13].

Most blockchain have ability to execute smart contracts automatically with some conditions. Smart contracts provide transparency for all parties to see the rules relating to automation. Conversely, the code drives the automation provided by a centralized platform is usually hide behind the scenes [14].

Smart contract will communicate using web protocol 3 to be able to access the ethereum node [15]. The smart contracts is a bridge of communication between decentralized applications and ethereum blockchain nodes.

3.4 Middleware

Middleware is a translator between two systems or functions. Can also be interpreted as bridging between programming languages and programming levels. In this study, middleware will translate high-level languages used in the frontend into the bytecode function used by EVM.

Unlike middleware in general, which conducts transactions transparently and often separate from the system (stand alone), in this study middleware will be adjusted with frontend applications as well as smart contracts.

The communication design between decentralized applications (in this case B-DEC) with other system components can be seen in Fig 3.

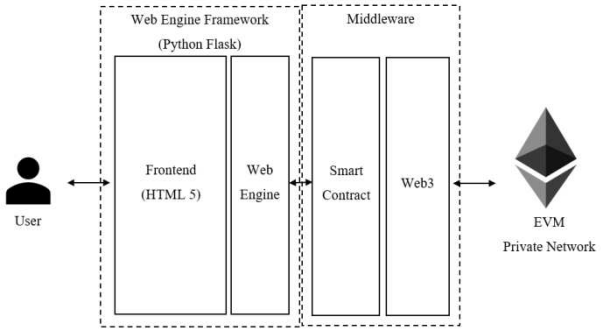

Fig 2: How to B-DEC Communication Schema

3.5 Design DEC on Blockchain

The DEC-making approach is carried out by conventional physical evidence storage (evidence cabinet) approach. Each cabinet will be one or more digital evidence. This cabinet will reflect a special shelf that refers to the acquisition of digital evidence in a case. This is to facilitate identification of the location of digital evidence and can be used to regulate authority management. Because not all authorities will be the same in one or many cases

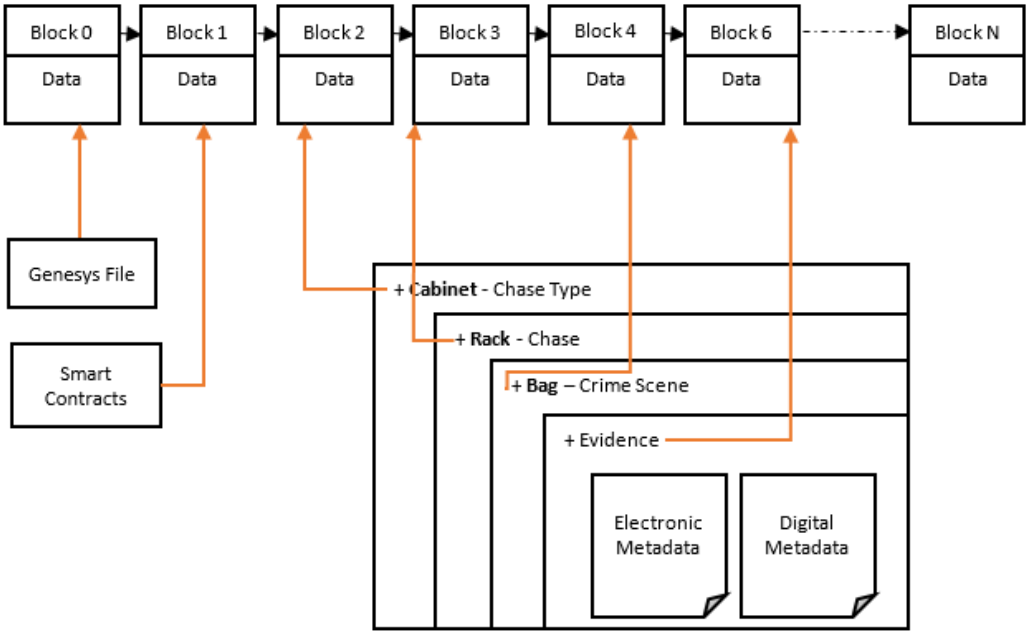

Fig 3: Design DEC on Blockchain

Fig 3 explain how the scheme of storing digital evidence data and Chain of Custody with DEC approaches on blockchain block series. In accordance with the blockchain provisions where block 0 is a basic block that must be filled with genesis files. Genesis file contains a configuration from the blockchain. Then smart contracts must be described in a series of blocks on the blockchain as initialization functions that can be used in the system.

The DEC concept can be seen starting in block 2, which is filled with data cabinet which is translated as the type of case. Data continued on block 3 which contains number of rack with case data. The rack is contain a bag that reflects the crime scene and ends with the storage of evidence data both electronic and digital data. For the record, on Fig 3 only limited to simulations that actually cannot be sequential as in the picture.

3.6 Integrated B-DEC System

At this stage all systems will be integrated starting from EVM (private ethereum network) to the frontend. This integration is expected to be able to implement B-DEC. The system must do optimization and measurement of performance as part of calculating the effectiveness and performance of the system. This is used to get the flow, system design and also the selection of the right topology. This cirlce process can be repeat until get a proportional result.

4. IMPLEMENTATION AND RESULT

4.1 Simulation

Basically the B-DEC architecture is the same as the blockchain architecture in general. Where the system needs also refers to the minimum standard blockchain system. There is a blockchain server that opens ports for connections and also a computer that will run the DEC concept. The requirements from the software side can be seen according to the B-DEC architecture design.

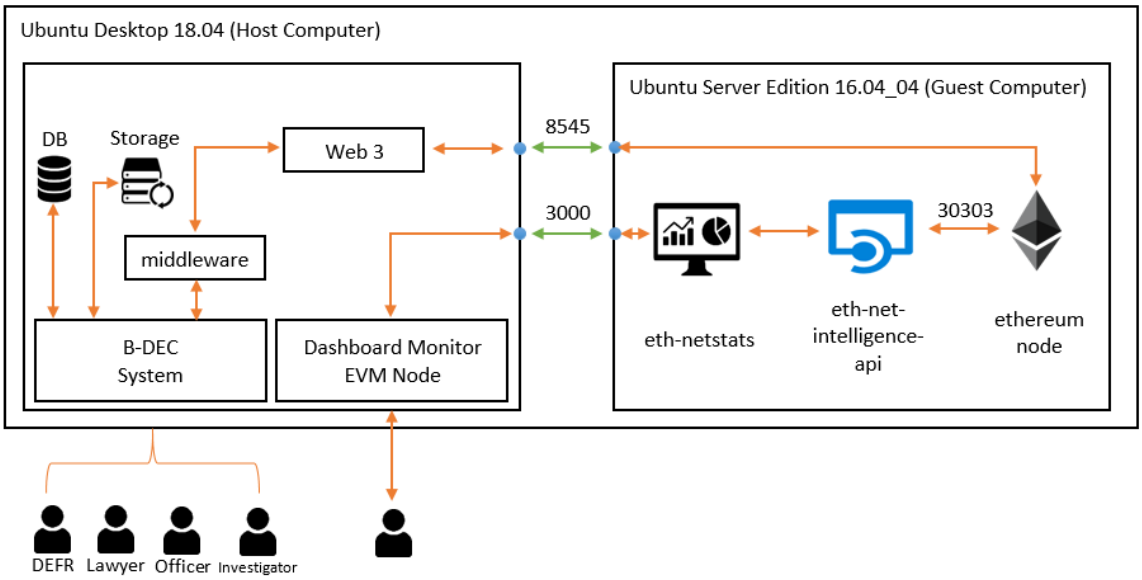

Fig 4: B-DEC Simulation Schema

Fig 4 describe the B-DEC simulation carried out in this study. The simulation meant the author carried out a trial process (experiment) on various types of device arrangement. It will get the ideal B-DEC architecture. As stated, there are many types of implementations on how to build a blockchain server. To simplify the simulation, a single server single node will be built as a reference for standard research specifications. This simulation server made with virtual machine. The virtual machine has 1GB of virtual RAM, 50 GB of hardisk and 1 core Processor.

Fig 4 also shows that the host computer is the main part of the B-DEC implementation basis. This computer is installed with Ubuntu Linux 18.04. In this section, the B-DEC system integrates with the Database (DB). This DB used for storing logs and some basic configurations. This make a decentralization apps as well as blockchain requirement. The other storage used for digital evidence management. In this storage a Digital Evidence Storage (DES) was built. To communicate with the EVM node system that must be translated by middleware and open a connection using a web3 library. The web3 library that used in this study based on python language. This is done to adjust the programming language in the frontend. The port used for communication between EVM nodes and web3 on B-DEC is the default port number of 8545. The port has been used as a RPC call. The other service to guide for management and monitors, on also provides hosts on port 3000. This service will be show of about node performance.

As for the EVM node installed on guest computers. Guest computers installed on Ubuntu ubuntu 16.04_4 server version. On this server node also installed several additional applications to monitor the EVM server node. Some of the support applications are eth-net-intelligence-api, which will monitor and listen to EVM node activities. The listener port used number port 30303 which can basically be changed according to needs. From eth-net-intelligence-api then the data is displayed using the frontend eth-netstats application. The EVM node will be easily monitored with the dashboard, with eth-netstats.

4.2 Result

4.2.1 Implementation DEC Result

The test is continued by comparing DEC with B-DEC through simulation. At this stage, the case scenario in the previous chapter is used as the basis for the simulation. The results of testing the full implementation of B-DEC can be seen on Table 1.

Table 1. DEC vs B-DEC Comparation

No	Clause	DEC	B-DEC	Description
1	Tagging concept for cabinet	√	√	Cabinet struct
2	Cabinet can be provide multiple rack	√	√	Cabinet has an array rack ids
3	Tagging concept for rack	√	√	Rack struct
4	Rack can be provide multiple bag	√	√	Rack has an array bag ids
5	Tagging concept for bag	√	√	Bag struct
6	Bag can be provide multiple evidence	√	√	Bag has an array evidence ids
7	Tagging concept for evidence	√	√	Evidence struct
8	Digital evidence log and CoC Form	-	√	Log struct
9	Split file support on digital evidence storage	-	√	JSON array support on evidence struct

Data on Table 1 is obtained that generally the DEC function can be accommodated by B-DEC. The added value of B-DEC is it has been able to explain and accommodate the types of logs for accessing digital evidence along with detailed chain of custody documents. B-DEC also being able to accommodate the types of evidence split into several files. Examples of display B-DEC can be seen in Fig 5.

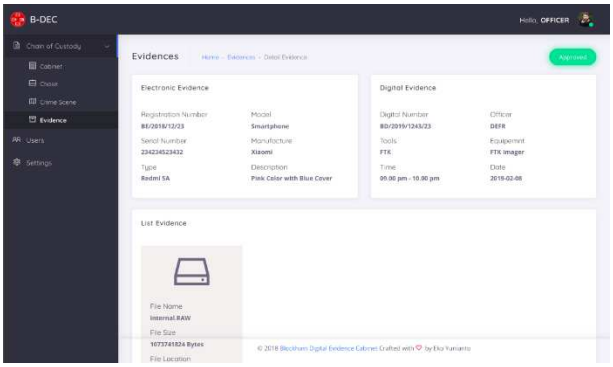

Fig 5: B-DEC GUI Application

B-DEC use evidence log to save historical access for digital evidence. This evidence log is a record of interactions between users and digital evidence. The evidence log on B-DEC is referred to as the evidence timeline. For more details can be seen on Fig 6.

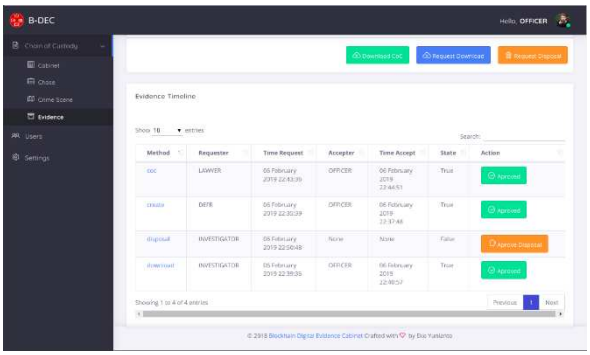

Fig 6: Evidence Timeline on B-DEC

4.2.2 B-DEC Performance

B-DEC is an implementation of DEC using blockchain technology. The testing process follows the blockchain performance. Performance is related to DEC on the blockchain. Peformance measurements must be adjusted to the B-DEC design. Performance is focused on DEC implementation on the blockchain.

To calculate the performance of B-DEC can be done through a performance test of each system function. Some benchmark comparisons are input file size, execution time and gas. System functions refer to the types of functions that are built based on needs such as create cabinets, create rack etc. Input file size depend on string as a input data. Execution time is calculated from the start of the gas estimation process until the transaction is completed. Refer to [16] who is the founder of parity ethereum explains how to calculate gas estimates and trasaction fees.

Gas is a value that must be spent to be able to execute storage on the blockchain. The value of the gas has been determined by calculating the level of difficulty carried out by a function. The way to calculate estimated traction costs can be used as follows:

$$ETH = \frac{G_{used}\ x\ G_{price}}{1x10^6} \quad (1)$$

As with formula (1) that in order to calculate the transaction value (ETH), it is necessary to do calculations according to the formula. For example to calculate the transaction value when making a smart contract requires a gas of 5041153. As a basis for determining the gas value (gas price) is 2.2 gwei. If the calculation is done using formula (1) the following results are obtained :

$$ETH = \frac{5.041.153\ x\ 2{,}2\ \text{gwei}}{1x10^6} = 0{,}0110905\ ETH$$

The smart contract on B-DEC is needed as much as 0.0110905 ETH to initialized the function. In dollar denominated conversion is $ 1.35304 (value taken on February 15, 2019 00:28 am). ETH calculations on private networks don't really matter. The calculation of transaction costs can be a benchmark for development and optimization. The development in is both in terms of the effectiveness of making system functions and simplification.

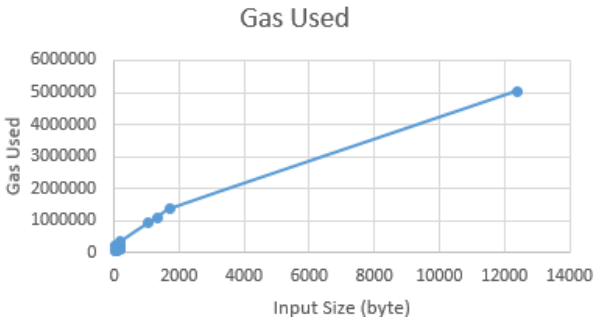

Fig 7: Relevance Size with Gas Used

From the results of the B-DEC performance test. There are relationship between the amount of input files and the use of Gas is drawn. It can be seen in Fig 7. Compared with [16], it is relevant if the larger the input file size will need the more spend of gas. Even though on Fig 7 just approaching proportionally. The reason because the calculation of gas usage is also calculated from the value of the difficulty level of a function. So if more complex functions, the gas needs will be higher.

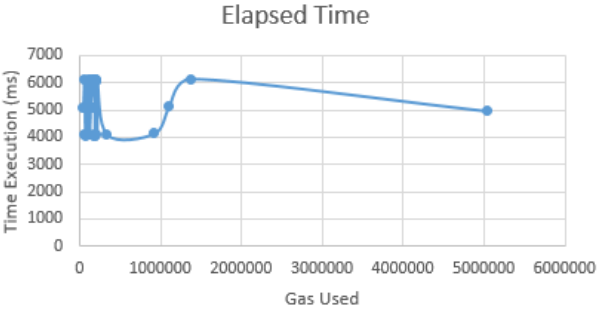

Fig 8: Relevance Gas Used with Time Execution

From Fig 8 can be seen if the execution time is not directly proportional to the use of gas. From the data, it can be read that B-DEC can accommodate various types of functions along with the level of complexity. Of course without any pending execution time. This is very helpful for the implementation of the B-DEC implementation.

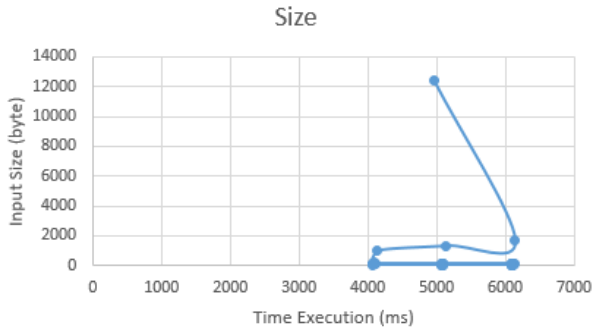

Fig 9: Relevance Time Execution with Input Size

From Fig 9 it can be seen that the performance of B-DEC execution time does not always depend on the amount of the input file value. The prove can be calculated the average execution time in each function ranges from 5000 ms or 5 seconds.

4.3 DEC Framework Optimization

Some DEC adjustments need to be done to be able to accommodate the management needs of digital evidence and chain of custody documents. Some things that need adjustment are as follows:

a. Warehose in DEC that represents a folder we can describe as root as the basis of storage so it does not require special tagging because it represents the type or scope of storage.

b. The cabinet as a tag can be translated as a type of case. It must include the type code and the name of the case type.

c. Rack as tag can be translated as case name. It must include the case code, case name and investigator data.

d. Bag as a tag can be translated as a crime scene. Which in it must contain the crime scene and the explanation.

e. Evidence as a tag that stores electronic and digital metadata. It must contain electronic and digital information.

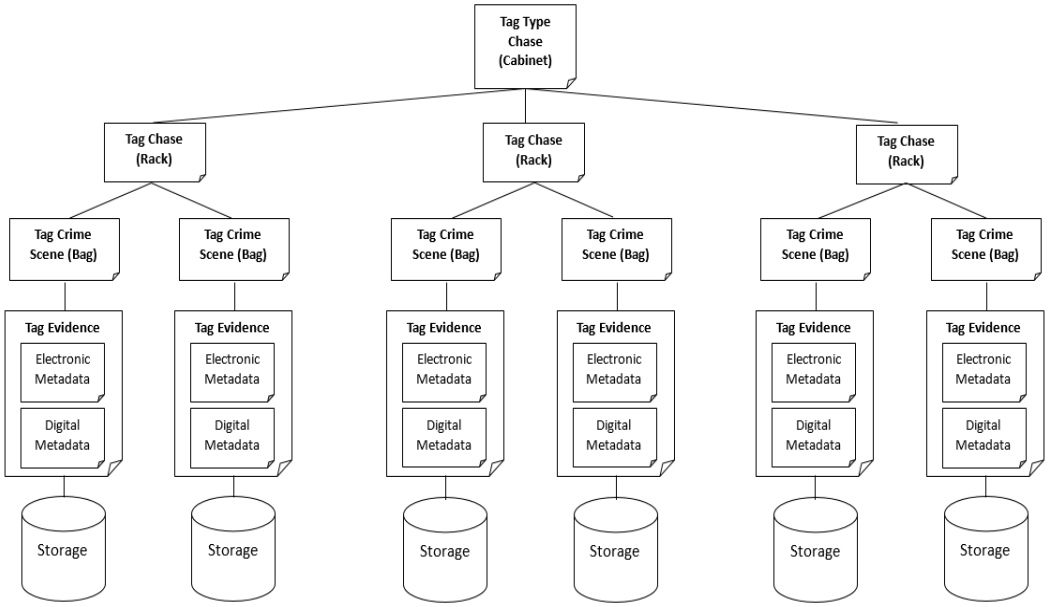

Fig 10: DEC Optimation on B-DEC

From Fig 10 it can be seen that the development of DEC show how the content management of evidence can reach the type of evidence (in this case electronic evidence and digital evidence). The cabinet described as a type of case (T_c) that stores information on the type of case and its description. In T_c there are many cases (C_0). In C_0, you must be able to store case information along with the completeness. Each case is compiled from several crime scenes (CS_0). The crime scene stores information on the location of the crime scene that is detailed in the description. Of course at the crime scene (CS_0) it was possible to confiscate a lot of evidence. It must accommodate electronic evidence containing digital evidence. An electronic proof (B_e) will definitely get digital evidence (B_d) after the acquisition process takes place. B_d will be stored in storage (S_0).

5. RELATED WORK AND DISCUSSION

According to the results of the trial, DEC implementation was obtained on the blockchain. The B-DEC design can be built according to the initial design to work well. This can be seen from the various types of trials that have been carried out. The performance test results and the DEC concept test are appropriate.

As for this test, it uses 3 types of evidence. For more details, refer to Table 2.

Table 2 List Digital Evidence for Simulation

No	Electronic Evidence	Description	Acquisition	Digital Evidence
1	Smartphone	Xiaomi Redmi 4A	FTK Imager	Internal.RAW
2	CCTV video saved on flashdrive	Sandisk 8 GB	Forensik Imager	File_000.aff File_001.aff File_002.aff
3	Memory Card	MMC micro SD Sandisk 4 GB	Encase	mmc.E01 mmc.E02

From Table 2 we can see that the type of evidence used for the trial has different extension from many acquisition tools. It is hoped that trials with different types of digital evidence. That illustrate how B-DEC can accommodate system management. Of the three evidences, all B-DECs can be accommodated. This is regarding B-DEC designed to be able to receive various types of files. B-DEC can be one of solution for digital evidence management.

On other study there are many implementation of blockchain on another fields. Such as [17] thats implement blockchain for quality assurance. On other study [18] create an integration of blockchain with IoT. Another supply chain with blockchain also described refers to [19]. This means that blockchain is an interesting technology to develop. One of reason is blockchain guarantees data integrity and security

Then from the trial, get the chain of custody document as in Fig 11.

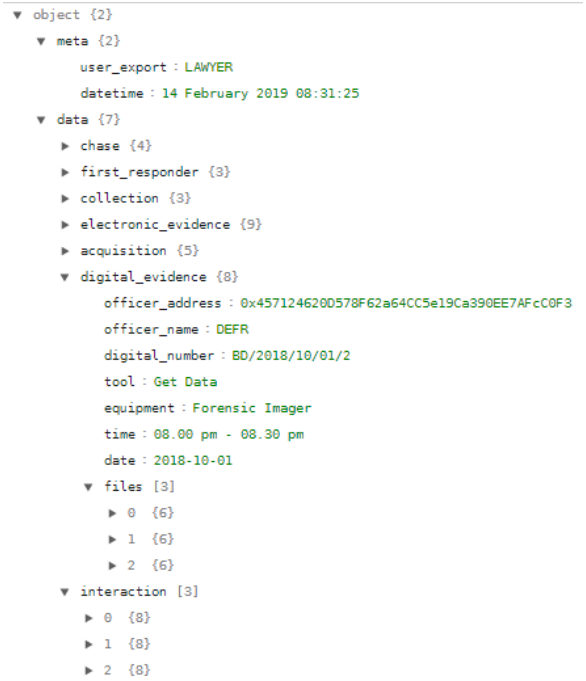

Fig 11: Exported CoC from B-DEC

According to the Fig 11 image, the JSON data structure is obtained. There are several sections to accommodate various types of fields accordingly. This field is adjusted to DEC's needs. There are 44 basic field on this CoC document. All of them support documentation about electronic and digital evidence.

6. CONCLUSION AND FUTURE WORK

The design of DEC concept with blockchain technology (B-DEC) was carried out by translating DEC requirements into a struct data type. Smart contract is responsible for applying DEC on the blockchain when storing data. It has obtained a digital evidence management design. It must accomodate the minimum needs of digital evidence data by storing it safely on the blockchain.

The DEC framework can be built on the blockchain. Some adjustments are needed in the data processing section. One of them is designing a framework development to be able to accommodate a variety of digital data consisting of many files (split files). In addition, some adjustments made are adding the logging concept that accompanies digital evidence. Furthermore, the framework was developed by integrating with the storage location of evidence. It can be concluded if the DEC-based blockchain can be developed up to integration with digital evidence storage (DES).

Later the system must be able to secure digital evidence in a software manner. That it needs to increase the level of security of digital evidence even further such as the use of encryption etc. The same implementation can be done in various types of data that require data integrity such as sending confidential documents etc. Of course, by adjusting needs, especially on smart contracts. The same system can be implemented on other types of blockchain outside of ethereum on the condition that the blockchain is used instead of supporting smart contracts.

7. REFERENCES

[1] National Standardization Agency, "Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (ISO / IEC 27037: 2012, IDT)." National Standardization Agency, Jakarta, pp. 1–44, 2014 : In Indonesia language.

[2] The Guardian, "Police mishandling digital evidence, forensic experts warn | Law | The Guardian," The Guardian, 2018. [Online]. Available: https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn. [Accessed: 24-Nov-2018].

[3] S. E. Goodison, R. C. Davis, and B. A. Jackson, "Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence - Appendix," pp. 1–7, 2015.

[4] Y. Prayudi and A. SN, "Digital Chain of Custody: State of The Art," Int. J. Comput. Appl., vol. 114, no. 5, pp. 1–9, 2015.

[5] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, 2011.

[6] 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.

[7] 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.

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

[9] D. Drescher, Blockchain Basics. 2017.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017.

[11] T. Laurence, Blockchain for dummies. Hoboken, 2017.

[12] S. Asharaf and S. Adarsh, Decentralized Computing Using Blockchain Technologies and Smart Contracts. 2017.

[13] K. Hegadekatti, "Legal Systems and Blockchain Interactions," no. 66085, 2017.

[14] ChainLink, "Blockchain ' s Role in the Produce Supply Chain," 2018.

[15] A. Cameron, M. Payne, and B. Prela, "Research and Implementation of Multiple Blockchain Byzantine Secure Consensus Protocols for Robot Swarms," 2018.

[16] G. Wood, "Ethereum: a Secure Decentralised Generalised Transaction Ledger Eip-150 Revision," Ethereum Proj. Yellow Pap., pp. 1–32, 2014.

[17] Arpan Sarkar and Jibendu Narayan Mazumder, "Quality Assurance in Blockchain," 2017.

[18] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.

[19] E. Hofmann, U. M. Strewe, and N. Bosia, Supply Chain Finance and Blockchain Technology. 2018.