Decentralized Trusted Storage of Audio-Video Log Data Based on Blockchain Technology and IPFS

Bambang Irawan[1*], Dandung Trihatmojo[2]

[1]Department Of Computer Science Informatics Engineering, Esa Unggul University, West Jakarta, Indonesia
[2]Department Of Computer Science, Esa Unggul University, West Jakarta, Indonesia
[*]Corresponding Author:
Email: Bambang.irawan@esaunggul.ac.id

Abstract.
The development of communication and information technology has affected the world of television broadcasting in Indonesia. With the emergence of a new phenomenon, the convergence of digital media industry. The migration of analogue to digital television broadcasting has impacted various industries related to broadcasting. Especially for the sustainability of the television broadcasting community in the country. Station Tv x is one of the television communities, on the other hand the media industry has challenges in managing storage media consisting of audio and video data that has a large capacity. Audio video logs are needed as information on recording audio video files. Blockchain-based Interplenary File System (IPFS) technology is expected to be one of the alternatives that can be applied in the world of broadcasting, storage media and audio video file data distribution methods, data library security and data flexibility are one of the challenges faced in the television broadcasting industry. The purpose of this research is as an effort to decentralise audio video data in distributed storage media to be more optimal and secure. The results of this research can be used to distribute audio video data files in the data library at tv station x.

Keywords: *Desentralisasi, IPFS, Blockchain, konvergensi audio video.*

1. INTRODUCTION

In recent times, there has been significant attention towards blockchain and decentralized applications (DApps) as they explore the potential of this technology. Some experts view blockchain as the most important IT innovation of our era [1], comparable in importance to the World Wide Web. By utilizing blockchain-based technology, there is a chance to address the challenges faced by the media industry, particularly concerning content availability [2].

Blockchains allow for peer-to-peer transactions without the need for a trusted third party [3]. They possess two crucial properties that make them appealing as data stores: immutability, which ensures an auditable record of events that cannot be altered, and redundancy, as exact copies are stored across many independent locations.

Ethereum, the second largest blockchain network by market capitalization, was a pioneering platform introducing the concept of smart contracts within a decentralized blockchain network. The Ethereum protocol's accessibility enables anyone with network access to scrutinize the terms and conditions of each contract [4].

Recognizing the potential of smart contracts on the Ethereum blockchain, researchers have explored their application in various DApps. One such DApp aimed to facilitate secure sharing of commodities while preserving privacy and eliminating the need for users to log in multiple times across platforms [4]. Additionally, a pilot video rights management system utilized blockchain to combine videos with rights information and facilitate transactions issued by licensors [5].

IPFS is a decentralized peer-to-peer hypermedia protocol designed to store digital content with high integrity and global accessibility. Files stored on IPFS generate file hashes and are stored on the Ethereum blockchain. The hash file stored on the blockchain can then be accessed again by calling the file stored on her IPFS[6].

II. METHODS

The blockchain-based distributed application system adopts the FAST method (Framework for the Application of Systems Techniques) as a guiding approach for analysis and design[7]. The FAST methodology encompasses eight distinct phases for analysis and design, which are as follows:

1. Scope Definition.
2. Problem Analysis.
3. Requirements Analysis.
4. Logical Design.
5. Decision Analysis.
6. Physical Design and Integration.
7. Design and Test.
8. Installation and Delivery.

Literature research is a set of activities related to collecting library data, reading, and taking notes, and how research materials are managed. Literature research is research conducted by a researcher by collecting a series of books or journals related to a problem or research goal. This technique is carried out with the aim of exposing various theories related to the issues dealt with and studied as reference material for discussing the research results, another understanding of literature research is to look for theoretical references related to the cases or issues found.

Table 1. 1 Previous Research Table

No	Authors	Year	Research issue	Research Result
1	Dexin Zhu, et al. [8]	2022	Traditional videoconferencing systems heavily depend on computational complexity to maintain system security. Nevertheless, the advancement of high-performance computers has significantly weakened the effectiveness of existing cryptographic systems.	The quantum secure videoconferencing system seamlessly combines the technical benefits of quantum key distribution with the stability of traditional systems, effectively thwarting security threats like channel eavesdropping and high-performance computing attacks. This results in a videoconferencing system that offers a heightened level of security.
2	Hsiao-Shan Huang, et al. [9]	2020	Numerous blockchain methods are focused on addressing the need for distributed transaction recording. Nonetheless, there are certain constraints when it comes to storing substantial files and documents on the blockchain. To overcome this, distributed storage media have been developed specifically to cater to the requirement of storing relatively large volumes of data.	The absence of access control mechanisms in IPFS servers and blockchain networks is apparent. Nevertheless, a secure file-sharing system efficiently manages access control policies, guaranteeing that access to files is restricted to members belonging to specific groups, ensuring that they can only access the files they are authorized to use.

3	Randhir Kumar, et al. [10]	2021	Copyright infringement has a detrimental impact on the interests of copyright holders who have their images and videos uploaded to various websites and peer-to-peer image sharing systems.	Perceptual Hash (pHash) techniques are utilized for identifying piracy in multimedia. When multimedia content is uploaded to IPFS, the system calculates the pHash of the content and subsequently compares it to the existing pHash values on the blockchain network to detect any instances of piracy.
4	Suvadra Barua, et al. [11]	2020	Decentralized blockchain-based video platforms aim to alleviate advertising pressure and remove intermediaries, but they face challenges due to certain content creators uploading low-quality content merely to earn free cryptocurrency generated by blockchain algorithms. This practice demoralizes other creative content creators. Additionally, piracy and illegal distribution of protected content remain significant issues on mainstream video platforms.	A secure encryption scheme and access control system have been created by utilizing a modified version of IPFS and Ethereum smart contracts, resulting in the development of an efficient blockchain-based decentralized video streaming platform.
5	Wan Yeon Lee, et al. [12]	2022	A scheme for analyzing the integrity of video content running on a blockchain system.	The experimental results demonstrate that the proposed scheme achieves a 100% accuracy in integrity analysis of video content and also provides a conversion history of non-original video content with 100% accuracy, given that appropriate parameters are specified.
6	Tony Haryanto, et al. [13]	2021	Cybersecurity Information Sharing (CIS) boosts security through proactive and collaborative sharing of cybersecurity information. However, implementing CIS via cloud services introduces risks such as various cybersecurity concerns, including "man-in-the-middle" (MITM) and distributed denial of service (DDoS) attacks, as well as	The use of a private Ethereum blockchain ensures secure and transparent transaction logging, while a private IPFS network offers distributed storage, eliminating vulnerabilities associated with centralized storage systems. Test results demonstrate that the proposed SCIS (Secure Cybersecurity Information Sharing) system effectively ensures availability,

			vulnerabilities in cloud storage that result in centralized data management.	confidentiality, and integrity of cybersecurity information.
7	Muis, M.D et al. [14]	2021	Forgery of diplomas and certificates is one of the problems in education. In Indonesia, this issue has been a matter of concern as it undermines the credibility of educational qualifications and poses challenges in ensuring the authenticity of academic achievements. Diploma /certificate forgery is a type of letter forgery crime. Additionally, non-digitized diplomas and certificates are easily damaged or lost, making them difficult to manage.	According to the conducted tests, the fake diploma/transcript detection system performs well with 1-5 nodes. However, the optimal throughput value during the diploma/transcript creation and verification process is achieved when using just 1 node.
8	Ananda Rizky Duto Pamungkas, et al. [15]	2021	In this study, we attained a heightened level of security by leveraging the InterPlanetary File System (IPFS), which serves as a peer-to-peer data storage system integrated with the Ethereum blockchain.	Research results prove that IPFS can be used as an additional security for blockchain systems.
9	Irawan, B. [16]	2021	The advancement of information technology has enabled the fulfillment of all payment system requirements, ensuring that processes can be carried out securely and dependably with the aid of blockchain technology.	The Payment Transaction Proof (PTP) system has been developed using blockchain technology, which has significantly increased the security level. The introduction of blockchain ensures that evidence of validated transactions cannot be altered, as the transaction data is securely stored on a distributed ledger, providing tamper resistance to the system's log.
10	Peng Kang, et al. [17]	2022	Piracy of low-quality files is detrimental to the overall goal. Currently, many organizations rely on a central server to store and manage knowledge files shared by users. However, this approach leads to challenges, such as	This approach utilizes the consensus of all participating nodes and shares files on a synchronized blockchain, ensuring traceability throughout the process.

			the need to hire an untrusted third party for file content inspection and encryption, resulting in opaque file storage processes and potential manipulation of intellectual property rights. Furthermore, the lack of uniform standards for managing intellectual files creates inconsistency across institutions, hindering the establishment of a cohesive and efficient file management system.	

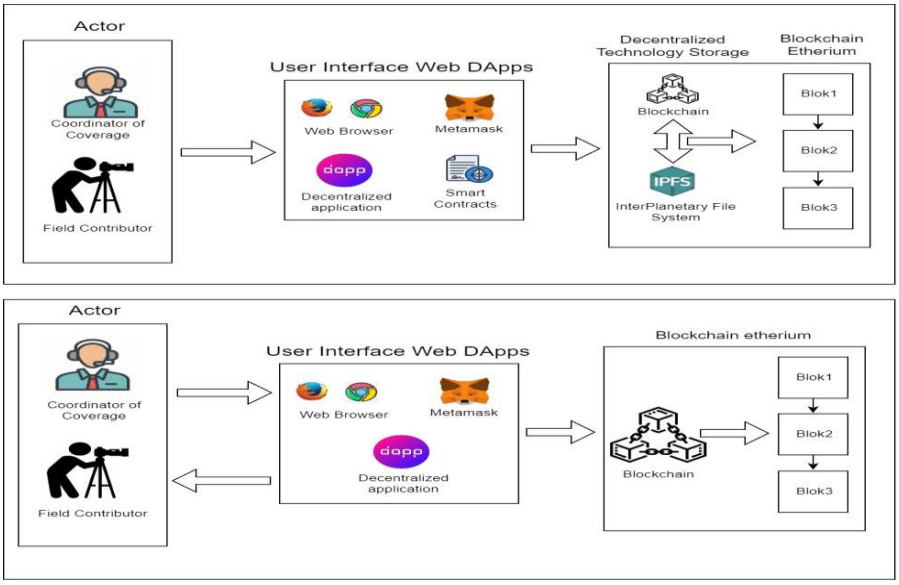


Figure 1. Design Architecture System

Figure 1.1 describes the flow of uploading an audio-video file to the blockchain network with the following information:

1. Field contributors upload audio video files through the DApps Application browser.
2. DApps connect to IPFS to form a CID hash automatically.
3. Field contributor gets the hashed CID in the DApps App browser.
4. The Hash CID of the DApps is inserted into the Ethereum smart contract.
5. Audio Video secure hash data is stored in the Blockchain network.
6. Coordinator Opens the CID Hash Link through the browser.
7. Coordinator downloads the Hash CID Link via browser/IPFS DESKTOP.
8. The Coverage Coordinator makes payments to the contributor's account through the DApps that have been integrated with the metamask e-wallet.
9. Contributors get payments through DApps that have been integrated with metamask e-wallets.
10. The transaction hash from the DApps is inserted in the Ethereum smart contract.
11. Hash CID data is stored in the Blockchain.

III. RESULT AND DISCUSSION

Blockchain can be described as a transaction database that is distributed among multiple nodes, forming a peer-to-peer network. It falls under the category of Distributed Ledger Technology (DLT), and its decentralized nature relies on a consensus protocol to achieve mutual agreement in managing the databases [18].

Ethereum is an evolution of Blockchain technology initially derived from Bitcoin's concept. Its primary objective is to enable more complex computational tasks within the Blockchain framework, surpassing the mere recording of transaction data. Similar to Bitcoin, Ethereum operates as a decentralized digital currency (cryptocurrency) payment system [19]. The proposed business process utilizes Ethereum smart contracts to establish a reliable and decentralized repository of audio-video logs, leveraging both blockchain technology and IPFS. It also includes automated participation of report coordinators (korlip) and contributors. Ether serves as the currency unit used for transactions within this system. The e-wallet consists of an account that includes a private key and a public key, serving as the identity for the owner of both the Coverage Coordinator and Contributor accounts.

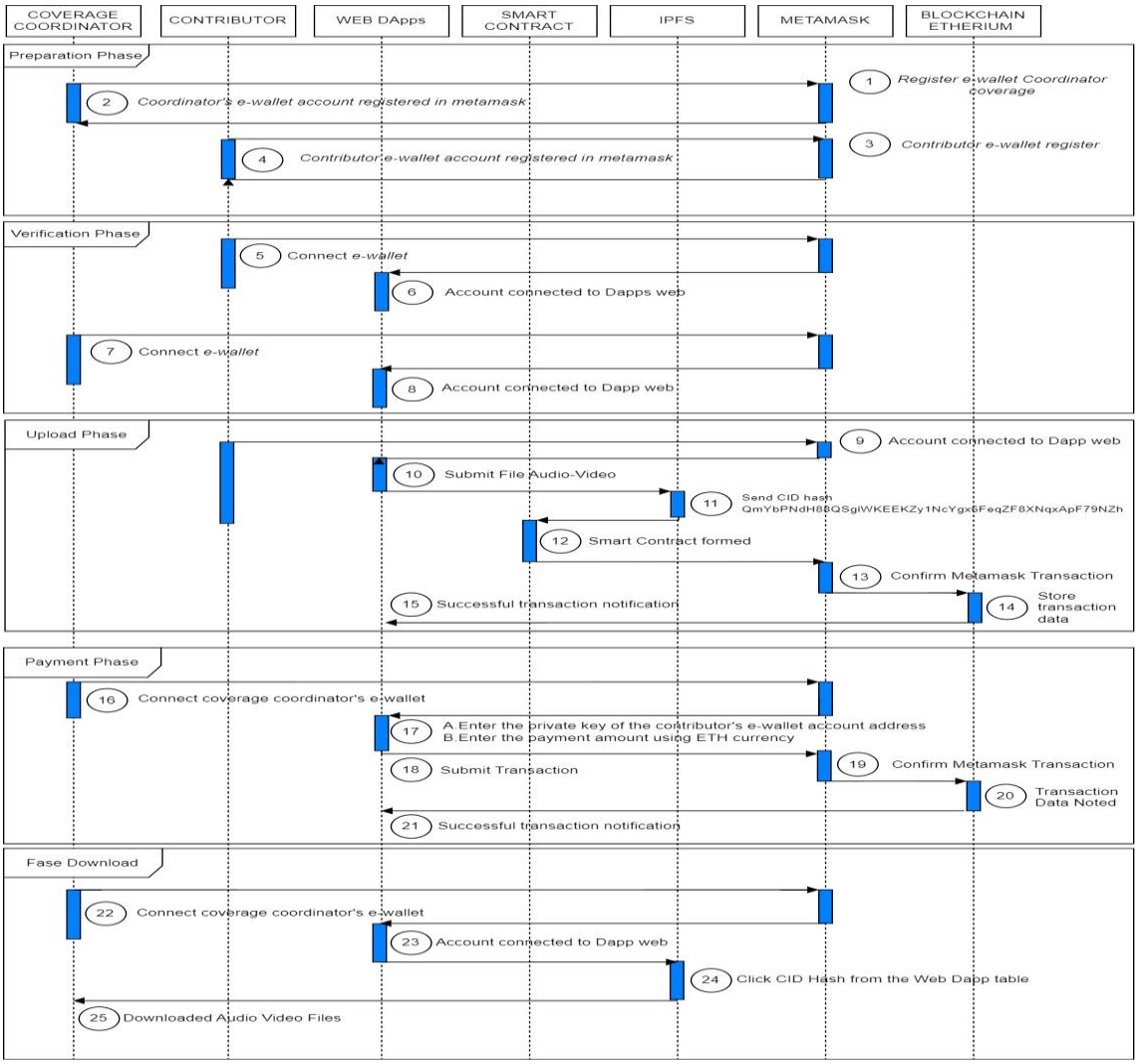


Figure 1. ***Sequence Diagram***

The actors involved in this system are korlip as a coverage coordinator and contributor as an actor uploading audio video files to DApss kobox, Sequence diagram in Figure 1.2 explains the process of korlipbox (Kobox) service in a system from the preparation phase to the download phase to kontirbutor based on the sequence of processes and stages that need to be done by the coverage coordinator and contributor.

- Preparation Phase

The preparation phase preparation phase includes steps 1 - 2 as below:

1. Korlip (coverage coordinator) account registration address on metamask e-wallet.
2. The coverage coordinator's e-wallet account is registered in Metamask.
3. Contributors register an address account on the metamask e-wallet.
4. The contributor’s e-wallet account is registered in metamask.

Verification Phase

- The Verification phase includes steps 3 - 6 as below:
    5. Contributor's account is connected to the metamask e-wallet.
    6. Contributor’s account is connected to the DApps (KoBox).
    7. Korlip (coverage coordinator) account is connected to the metamask e-wallet.
    8. Korlip’s account is connected to the DApps web.
- Upload Phase The Upload phase includes steps 7 – 13 as below:
    9. Contributor’s account is connected to the metamask e-wallet.
    10. The contributor uploads the audio video file through the DApps (KoBox).
    11. The Web DApp uploads the file, IPFS sends back the CID Hash.
    12. Smart Contract is formed.
    13. Contributor Metamask account transaction confirmation.
    14. Transaction data is recorded in the Blockchain network.
    15. Transaction Success Notification.
- Payment Phase The Payment Phase includes steps 14 - 19 as below:
    16. The coverage coordinator's account is connected to the metamask e-wallet.
    17. The coverage coordinator's account is connected to the DApps korlip wallet (Korlet)
        a) Korlip enters the e-wallet account address of the contributor to be paid.
        b) Korlip enters the amount of ETH to be paid.
    18. Coordinator Submit Transaction
    19. Metamask Transaction Confirmation
    20. Transaction data is recorded in the Blockchain network.
    21. Notification of successful transaction
- Download Phase the Download Phase includes steps 20 - 23 as below:
    22. The coverage coordinator's account is connected to the metamask e-wallet.
    23. Coverage coordinator account connects to DApps (KoBox)
    24. Copywriter opens link / CID Hash via Desktop Browser / IPFS.
    25. Audio and Video files are downloaded.

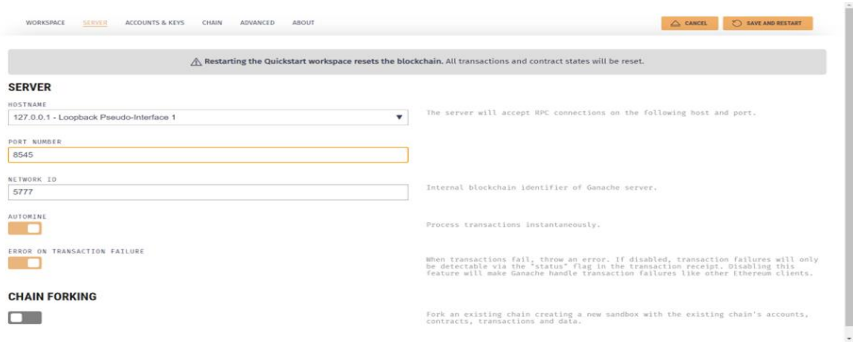
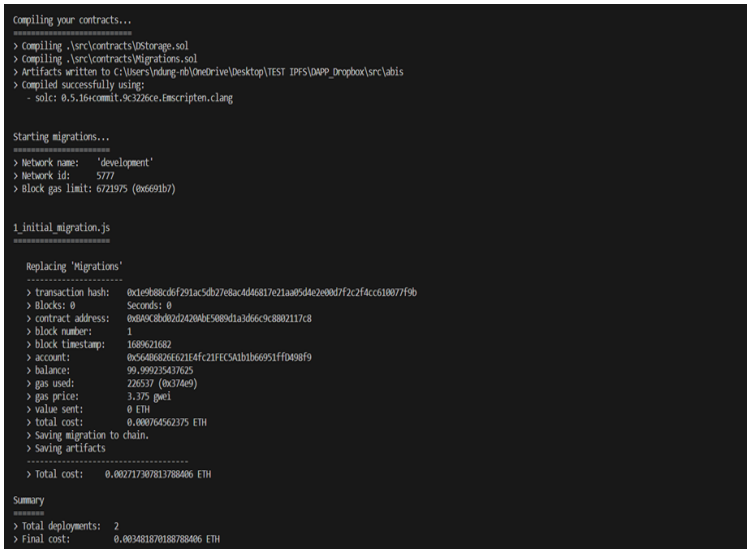


Figure 1.3 is a display of the ganache local server port configuration that will be used to connect with the metamask e-wallet.

Figure 2. Ganache Server Port Configuration



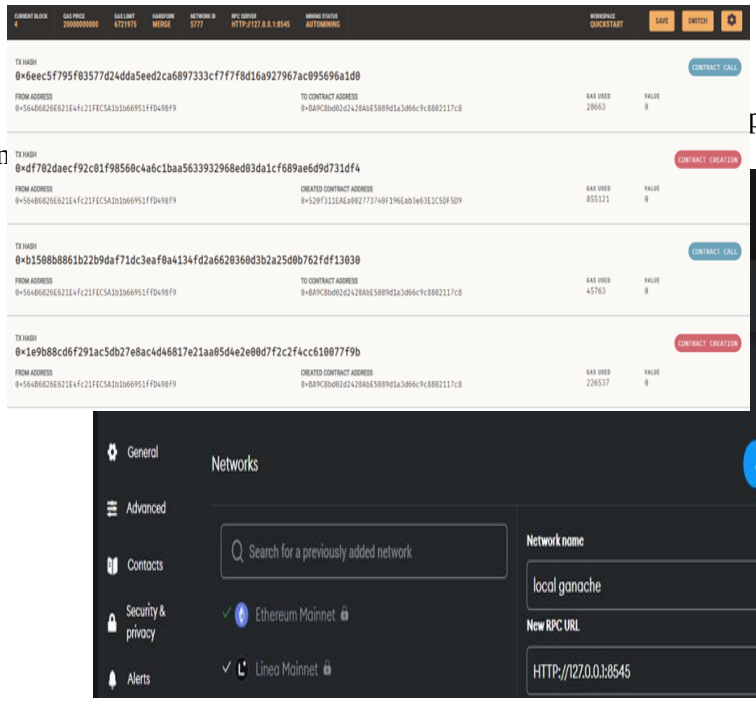


Fig 4. port "ganache8545" as the main network conn

Fig 3. Metamask e-wallet Ganache Network Configuration

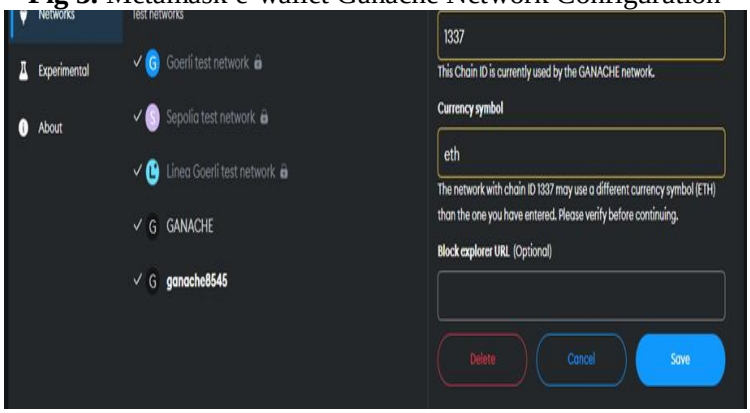


Fig 4. Smart Contract Compile and Migration

Figure 1.5 illustrates the outcome of compiling and migrating a smart contract on a local Ganache network using the Truffle and Solidity programming languages. Once the migration process is complete and the contract address is obtained, the provided smart contract will be utilized to interact with DApps in a web browser with the injected Metamask.

No	File Name	Description	Type	Size	Date	Uploader Account	IPFS Hash
4	ice_video_20220527-194730 - Copy.mp4	materi bandung 2	video/mp4	130 MB	5:06:25 AM 7/18/2023	0x6eA0b22A222766146758 2fa8038dB7D017a2e709	QmZY84anFUrRHimi2YZJQ3JoWihCPLP8WS8U6TBLS3GJrd
3	Bimbingan TA1-ndung-Bambang irawan-270522.mp4	materi bandung 1	video/mp4	216 MB	5:04:37 AM 7/18/2023	0x6eA0b22A222766146758 2fa8038dB7D017a2e709	QmYbPNdH88QSgiWKEEKZy1NcYgx6FeqZF8XNqxApF79NZh
2	ice_video_20220527-194730.mp4	materi bogor 2	video/mp4	130 MB	4:54:14 AM 7/18/2023	0x60F4b3b760C7F51A257e550c6Ff2F59317410326	QmZY84anFUrRHimi2YZJQ3JoWihCPLP8WS8U6TBLS3GJrd
1	Bimbingan TA1-ndung-Bambang irawan-270522.mp4	materi bogor 1	video/mp4	216 MB	4:52:45 AM 7/18/2023	0x60F4b3b760C7F51A257e550c6Ff2F59317410326	QmYbPNdH88QSgiWKEEKZy1NcYgx6FeqZF8XNqxApF79NZh

Figure 5. Kobox DApps

Korlipbox (Kobox) is a media sharing DApps for field workers whose job is to upload content needed for TV Channel X broadcasts, figure 1.6.

In Figure 1.7 contributor 1 uploads an audio video file with a description of bogor 2 material and manages to get a CID Hash value with the suffix "3GJrd", at a different time contributor 2 uploads an audio and video file with a description of bandung 2 material with the same CID Hash value as contributor 1, IPFS maintains reliable data integrity because it does not undergo changes during testing, so these results have fulfilled the aspects of information security based on the (Confidentiality, Integrity, and Availability) Triad Model.

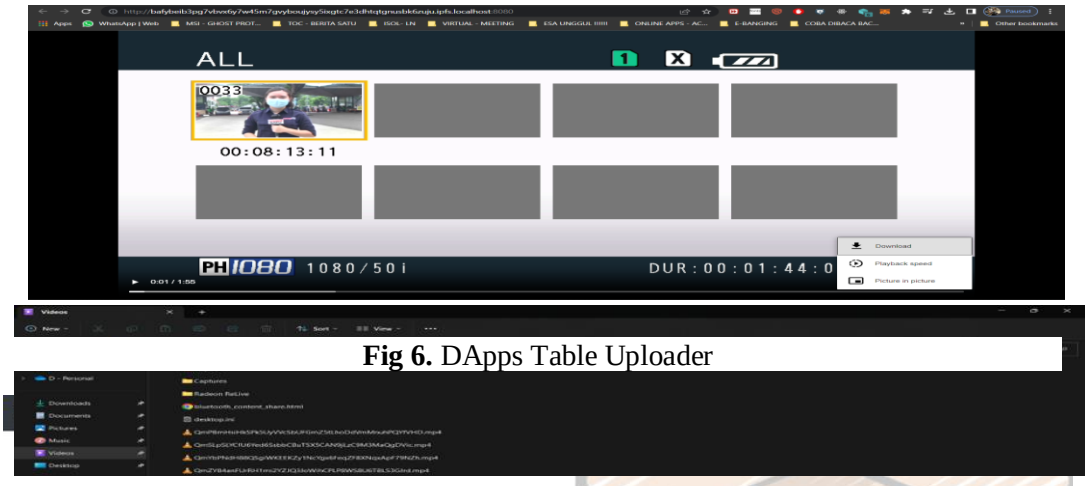


Fig 6. DApps Table Uploader

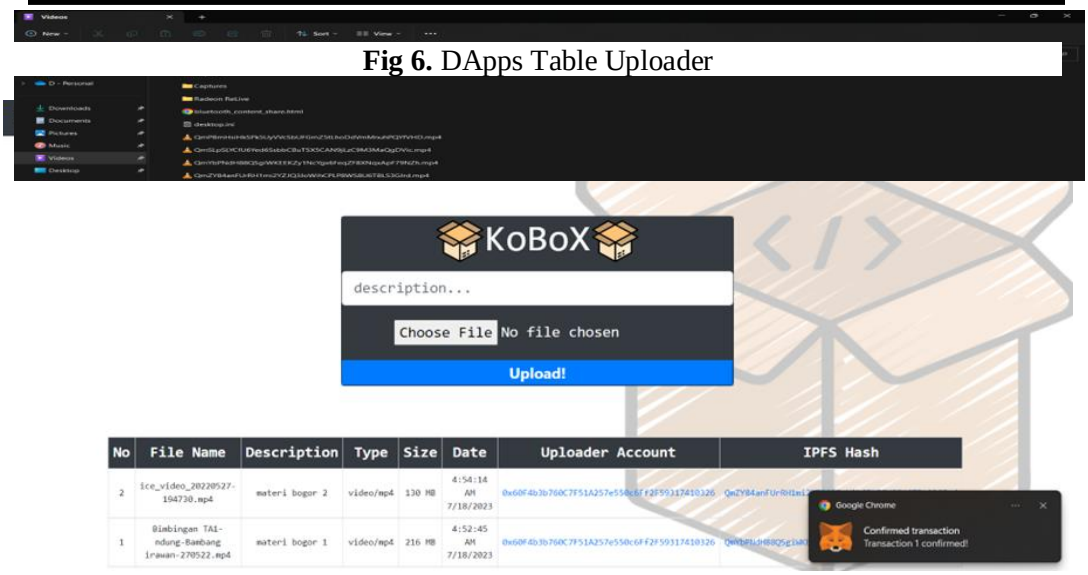


Fig 7. Preview and File Download

Figure 1.8 shows the hash search mode of IPFS, and contents of CID opened in browser, and shows file downloaded from IPFS.

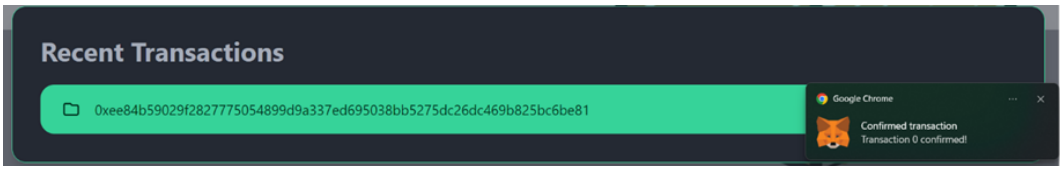


Fig 8 Korlip Wallet DApps

Figure 1.9 shows the information and confirmation of a transaction on Metamask of 1ETH from the Corlip account to Contributor 1's account, as well as the successful transaction proof notification and recording to DApps on the blockchain network.

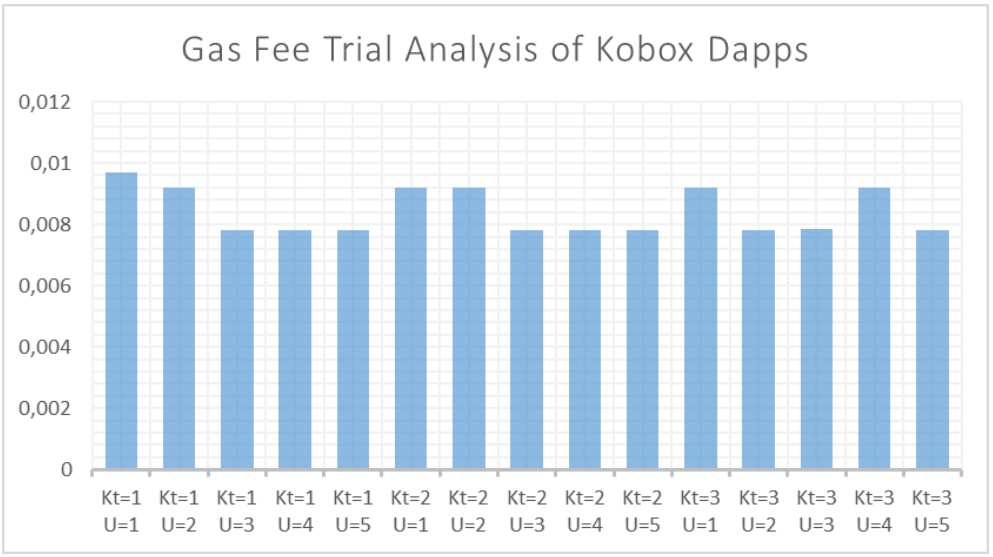


Fig 9. Analysis of Gas Fee Trial against upload phase

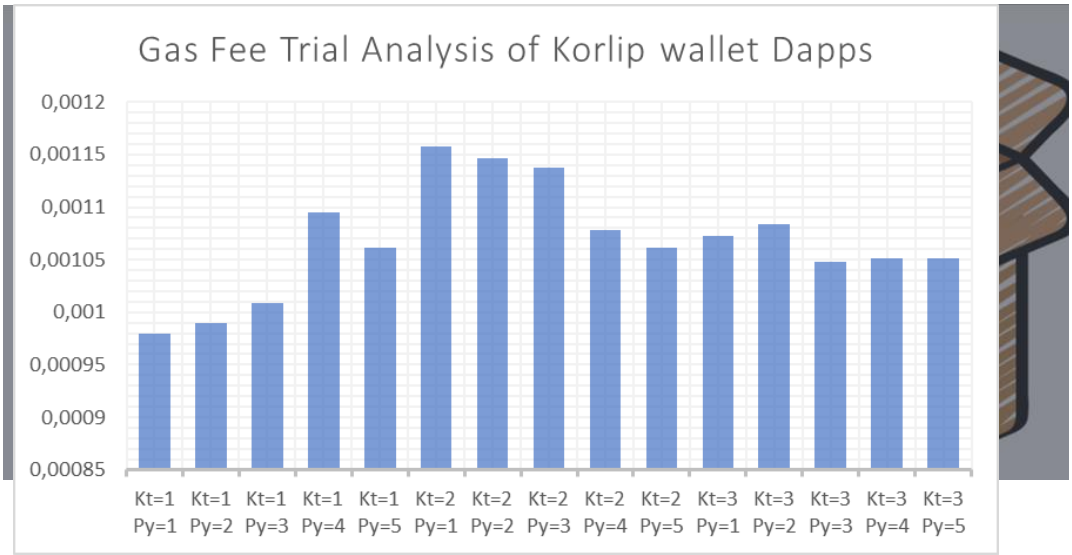


Fig 10. Gas Fee Trial Analysis of the payment phase

Description:

Kt = Contributor Account.
U = Upload Phase.
Py = Payment Phase.

In Figure 1.10, based on the results of the gas price test on DApps Kobox, in the graph from contributor account 1 and upload phase 5 to contributor account 3 and upload phase 5 with different file sizes, we can see the gas price values in the first and second transactions with higher gas price compared to the third transaction with the same relative gas price value.

In Figure 1.11, we can see that the chart from contributor account 1 and payment phase 5 with different payment values to contributor account 3 and payment phase 5, based on the results of the gas price test on the DApps Korlip wallet, uses relatively the same gas price value for each second payment transaction that uses a higher gas price compared to the first payment transaction. Phase.

IV. CONCLUSION

It is based on research results and discussions on reliable distributed storage of audio-video logs based on blockchain technology and ipfs. A web based DApp was used to test data integrity on IPFS using hashing parameters and passed bench test scenarios when renaming files in a way that IPFS maintains file content authenticity. If the content of the file changes, the hash obtained from IPFS will be different even if the filename is the same. From this we can conclude that using IPFS to maintain data integrity is reliable as no changes were made during testing. Therefore, these results meet the information security aspects of the CIA's three-fold model (confidentiality, integrity, and availability).

The analysis of the gas fee value testing trial on trusted decentralized storage for audio video logs based on Blockchain and IPFS technology. In this test, it is known that if the contributor uploads for the second time, there will be a change in the value of gas fee usage.

The entire process in the trusted decentralized storage system for audio video logs based on Blockchain and IPFS technology is recorded on the Blockchain network transparently, immutable, and automatically to avoid the existence of nonrepudiation tempering data carried out by irresponsible parties.

V. ACKNOWLEDGMENTS

The authors would like to extend their gratitude to the Department of Computer Science Informatics Engineering at Esa Unggul University for their support in this project. Special thanks are also given to Mr. Bambang Irawan, a lecturer, and Yudi L., Chief Technical Operation Center of Stasion TV x, for their valuable contributions. Furthermore, heartfelt thanks are conveyed to Family and Friends for their invaluable support.

REFERENCES

[1] Naughton, J.: Is Blockchain the most important IT invention of our age?.The Guardian, (2016).
[2] Mougayar, W. et al.: The Business Blockchain: Promise, Practice and Application of The Next Internet Technology. Wiley (2016).
[3] O'Dair, M., Beaven, et al.: "Music on the blockchain," Middx. Univ. (2016).
[4] Bogner, A., Chanson, M., Meeuw, A.: A decentralised sharing app running a smart contract on the ethereum blockchain. in ***Proceedings of the 6th International Conference on the Internet of Things, pp. 177–178, (2016).***
[5] S. Fujimura et al.: BRIGHT: A concept for a decentralized rights management system based on blockchain. in Consumer Electronics-Berlin, ***2015 IEEE 5th International Conference*** on.
[6] Rajalakshmi.: A Blockchain and IPFS based framework for secure Research record keeping. (2018).
[7] Whitten, J. L, et al. Metode Desain & Analisis Sistem Edisi 6 (2011).
[8] Dexin Zhu, et al. Nianfeng and Lijun Song, A Hybrid Encryption Scheme for Quantum Secure Video Conferencing Combined with Blockchain. (2022).
[9] Hsiao-Shan Huang, et al. A Secure File Sharing System Based on IPFS and Blockchain. (2020).
[10] Randhir Kumar, et al. A secured distributed detection system based on IPFS and Blockchain for industrial image and video data security. (2021).
[11] Suvadra Barua, et al. A Blockchain based Decentralized Video Streaming Platform with Content Protection System. (2020).
[12] Wan Yeon Lee, et al. Reliable Integrity Preservation Analysis of Video Contents with Support of Blockchain Systems. (2022).

[13] Tony Haryanto, et al. Secure Cybersecurity Information Sharing for Sectoral Organizations Using Ethereum Blockchain and IPFS. (2021).
[14] Muhammad Danil Muis, et al. Access Control and File Distribution Management for Electronic Diploma and Transcript using Ethereum Smart Contract and InterPlanetary File System. (2021).
[15] Ananda Rizky Duto Pamungkas, et al. Designing peer-to-peer inter-planetary file system (IPFS) based data storage system with blockchain architecture using ethereum. (2021).
[16] Bambang Irawan, Blockchain Technology as An Alternative Method of Payment Transaction Proof. (2021).
[17] Peng Kang, et al. ***Blockchain Private File Storage-Sharing Method Based on IPFS***. (2022)
[18] Revet et al.: The Intercompany Settlement Blockchain: Bene fi ts, Risks, and Internal IT-Controls. (2021).
[19] Wu, K. (2019). An Empirical Study of Blockchain-based Decentralized Applications.