Development of Blockchain-Based Digital Signature Platform

Ang Sandy Kristiawan[1], F Ridwan Sanjaya[2], FX Hendra Prasetya[3]
[1]Department of Game Technology, Soegijapranata Catholic University
[2,3]Departmen of Information System, Soegijapranata Catholic University
[1,2,3]Jl. Pawiyatan Luhur Sel. IV No.1, Bendan Duwur, Kota Semarang, Jawa Tengah 50234
[1]sandz9b@gmail.com
[2]ridwan@unika.ac.id
[3]hendra@unika.ac.id

Abstract— As technology develops, the Internet of Things (IOT) becomes a topic that is being mentioned over and over again. Many things can be done online. One of them is document signing activity. A company named "XYZ" wanted to build a prototype application using a framework that can build and develop a multiplatform app that can be used to sign a document and secure it with digital certificates, and the transaction activity is recorded and can be verified through a blockchain system. This study aims to find out how to apply blockchain system in a series of digital signing activities, how are the concept and how to verify a transaction that already recorded in a blockchain system, and also how to make a prototype that easy to develop further for other platforms. In the end, the application can be made easily using Expo, Node.Js, and the process for recording and verifying transactions can be done easily with the help of Hyperledger Iroha.

Keywords— Internet of Things, Blockchain, Verification, Application, Framework, Multiplatform, Digital Signature, Digital Certificate

I. INTRODUCTION

As Technology develops, most people can have access to technology easily. Most of them even make contact with technology since they were very young. There was a survey from "Katadata" titled "How many Internet users in Indonesia? Projection of Internet Users in Indonesia 2017-2023" that shows Indonesian internet users have been growing each year and will grow more until 2023 [1]. And also according to Hootsuite's survey taken in January 2020 can be seen that 64% of Indonesian are internet users, then 59% of them are social media users. The average time of them using the internet is 7 hours 59 minutes and the for using social media is 3 hours 26 minutes [2]. As January 2021 has been recorded that now the internet users become 79.5% of the Indonesian total population, and then the social media users become 65.3% [3].

Through this information, document falsification and plagiarism are among the things that can become a threat because so much information nowadays can be accessed openly, and some entities might be able to fake that information. There is a survey from "Katadata" titled "List of Cyber Crimes Most Reported to the Police" taken in 2020 that shows that data theft or identity theft is ranked sixth, and data manipulation ranked fifth. These two crimes are among the tenth most reported cybercrime [4]. Electronic signatures alone are not necessarily a guarantee that a document cannot be falsified. And it might be hard to prove or validate a plain signature attached in a document.

Ideas are born to design a prototype that can validate and prove that a document remains intact since it has been signed. It can also proves the signing transaction done through the blockchain system. This research is expected to fulfill the needs of a company named "XYZ" that wants to make digital signature products using a blockchain system.

II. LITERATURE REVIEW

2.1 Digital Signature

A digital signature is a type of signature attached to a document that contains

electronic information. The information attached such as writing, picture, or anything else is for verification or an authentication tool [5].

2.2 Public Key Infrastructure

Public Key Infrastructure (PKI) is a system that helps digital certificate creation and management. Public Key Infrastructure can bind a public key with its owner [7].

Public Key Infrastructure contains several components to do its jobs such as Request Authority (RA), Certificate Authority (CA), and Validation Authority (VA) [6].

2.3 Digital Certificate

A certificate that binds data of the relevant legal subject and contains an electronic signature which is then secured by encryption. Documents bound with digital signatures can be verified for its ownership and authenticity. The ownership status cannot be denied after its signed [8]. Digital certificates become invalid if there are changes to a document where the certificate is attached, as a sign that the document is no longer "intact" [9]. Electronic certificates are issued by electronic certification providers [5].

2.4 Cryptography

Cryptography is the study of ways to secure a message or information. The values of cryptography are, confidentiality, ciphertext or random text that cannot be read, keys to perform cryptography, and algorithms in carrying out the cryptographic process [10].

2.5 Blockchain

Blockchain is a database network system that is structured in a decentralized manner, not centralized in a single entity like in a database system in general but consists of many peers that store data in the form of interconnected blocks (blockchain). Each block has a timestamp and records the relationship with the previous blocks in the form of a hash of the previous block. The purpose is to keep records and the history of every transaction on the blockchain system. Each peer plays a role in a consensus process where the goal is to validate each block on the blockchain that is on the peer [11].

2.6 Node.Js

Node.js is software used to develop a server-side application using JavaScript. Node.js replaces browser in JavaScript processing. Node.js uses “V8 Engine” developed by “Chromium Project”.

2.7 Expo

Expo is a React-based framework. Expo can be used to create multi-platform applications easily, and faster because applications created using Expo by default can be directly accessed via Android and iOS smartphones as well as the Web.

2.8 MongoDb

MongoDB is one of the "NoSQL" based database systems, unlike conventional SQL databases that use tables and their relations which may be quite complicated to learn and develop [12]. MongoDb was chosen because it is easy to use and flexible in development. It is easy to customize and also the data structure can be changed according to the needs at any time if needed. The document is stored in BSON, which can be very dynamic in structure with dynamic schemas that can be changed whenever needed [13].

2.9 OpenXPKI

OpenxPKI is a PKI (Public Key Infrastructure) that can function as a Certificate Authority, Validation Authority, as well as a Request Authority. OpenXPKI can help with the certificate signing request (CSR) process, certificate validation process, and certificate revocation.

2.10 Hyperledger Iroha

Hyperledger Iroha is a blockchain infrastructure that uses distributed ledger technology (DLT), can assist in the process of asset management, small information storage for each user, identity management. In Iroha, some activities can be done and these activities are divided into three groups of commands, queries, and verification of transaction hashes [14].

There are several components of Hyperledger Iroha that can be discovered further in the Hyperledger Iroha documentation such as Toori, MSTP, PCS,

Ordering Gate, Ordering Service, Synchronizer, Block Creator, WSV, etc [16].

2.11 Docker

Docker is software that can virtualize the operating system and its programs which can then be wrapped in a docker container. Docker is quite reliable because it can wrap the system and applications needed and their dependencies with a fairly compact size into one docker container, and can be run on various other operating systems that have Docker installed. So it's as if Docker is like a Virtual Machine (VM) but the scale is very small [15] where the container can run with a fairly fast setup and with a relatively much smaller size compared to running the operating system and its contents through the Hypervisor.

III. APPLICATION DESIGN AND TESTING

4.1 Signing Up

The registration process begins by selecting the “Sign up” button on the application start page. Users can choose two types of user accounts, namely individual accounts or enterprise accounts.

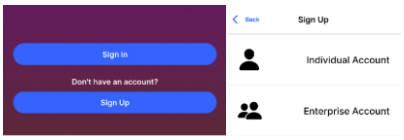

Figure: 4.1 The start page when the application is opened, and the selection page for the type of account user wants to register.

If a user chooses to register as an "Enterprise Account" there are two options, namely "New Account" if the user wants to register as a group admin (enterprise admin) or "Join Existing Group" to register as a member of an existing group.

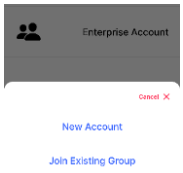

Figure: 4.2 Modal in the form of a drawer to choose a new account or join an existing group.

If the user wants to register as a member of an "enterprise group", the user needs a QR Code that can be viewed through the admin account of the "enterprise group".

Figure: 4.3 QR Code to register enterprise group members.

Figure: 4.4 Group members applicants scan the QR Code from the group admin to register as a member.

On the registration data page, some fields need to be filled in based on account type. If a user registers as an “enterprise account admin”, there are additional fields that must be filled in related to organization information which will later be used for asset management.

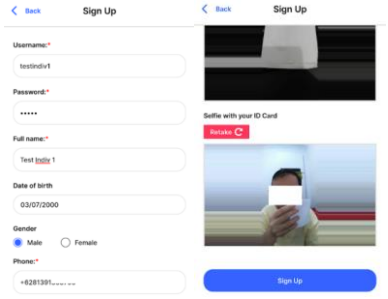

Figure: 4.5 Sign Up page sample.

If all data has been filled in, the user can press the “Sign Up” button to complete OTP verification.

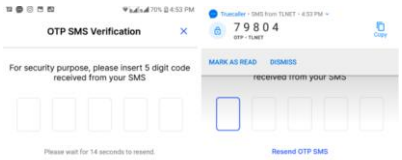

Figure: 4.6 Receive OTP Code via SMS.

If passed, the application will send the registrant information to an endpoint via POST request. A Certificate Signing Request will be generated to request a certificate generated by OpenXPKI then the registrant's data will be stored in the database.

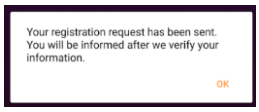

Figure: 4.7 Display when registration is successful.

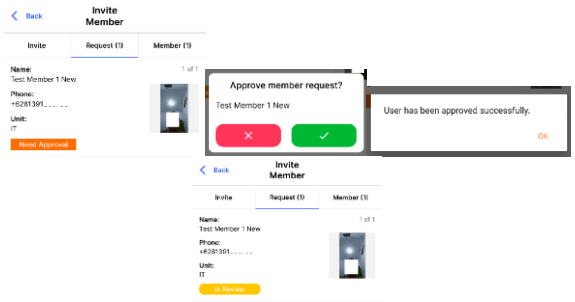

Figure: 4.8 Requests received by the admin group are approved and are waiting for the RA operator's admin approval.

The request will be received by the RA admin (operator) who handles user registration through a special web dashboard created to display incoming user registration requests. The operator must first check each incoming request with information displayed such as ID cards, and other information. The operator must accept the request through OpenxPKI before being able to approve through the web dashboard.

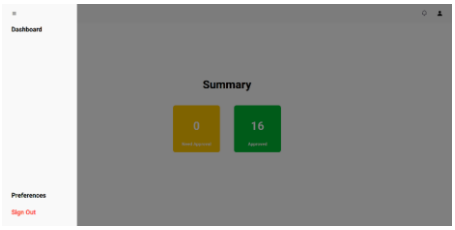

Figure: 4.9 Simple RA (request authority) admin dashboard website display which was also created using the Expo framework.

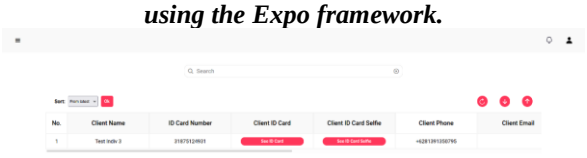

Figure: 4.10 RA admin dashboard display on the "Need Approval" page when receiving a user registration request.

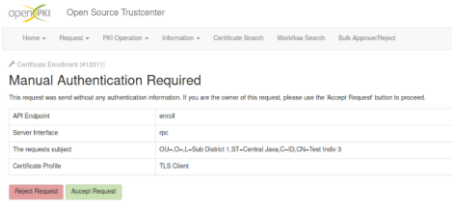

Figure: 4.11 Display request details and also the option to accept or reject the request.

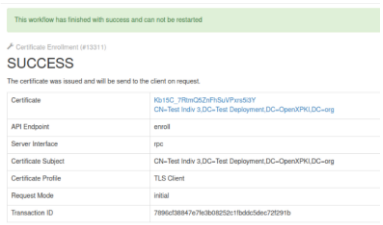

Figure: 4.12 Display if the enrollment request is approved.

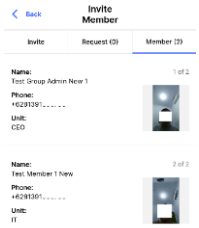

Figure: 4.13 Display on the list of group members if members of a group have been approved by the RA operator admin.

After the registration request is approved, the user can now use the application.

4.2 Sign In

To be able to enter the application, the user presses the "Sign in" button on the application's home page. Then the user will be asked to enter username and password. The user then presses the "Sign In" button. The application will send the request to an endpoint.

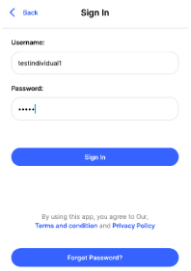

Figure: 4.14 The "Sign In" Page

There will be several data validation processes. The password sent by the user will be authenticated using the "bcrypt" library. If the process is successful, a JWT token will be generated and the refresh token is stored in the database. Then on the client application even though the API responds with a success status, the user still needs to complete OTP verification. If the user passes the verification, both token and refresh token will be saved to the device and then the user redirected to the main page of the app.

4.3 Individual Signing Process

For each signing process, the user must have a balance. The Hyperledger Iroha stores the user's balance as the user's asset that will be deducted for each signing transaction.

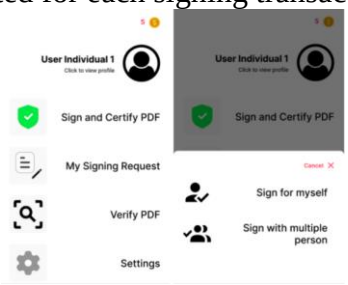

Figure: 4.15 Sign and Certify PDF menu option as a non-enterprise user.

The user can make a transaction by pressing the "Sign and Certify PDF" button, then "Sign for myself". To browse a PDF document the user press "Press to browse".

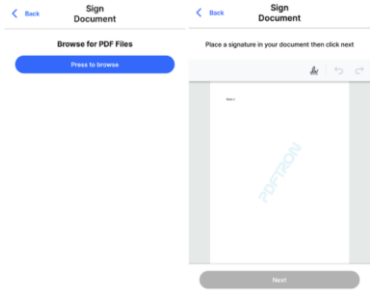

Figure: 4.16 The display before and after the document is selected.

After the document is selected, the user will be directed to the signing page. New users must first create a signature that will be saved to their device. After it's created and saved, the user can stamp the signature on every signing process. The user press "Next" to continue.

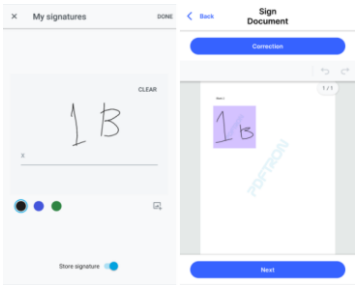

Figure: 4.17 The creation of a new signature and the display of the signature attached to the previously created container.

On the confirmation page, there is some information that needs to be filled in before the user presses the "Confirm" button. Then the user will be asked to complete the OTP verification. If the verification is successful, the application will send the information to the individual signing endpoint.

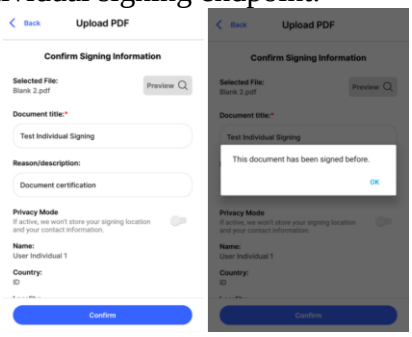

Figure: 4.18 Confirmation page on the "individual signing" process and the display if the document that has been through the certification process is found.

To be able to make a transaction, it will be checked first whether the user has a balance through the "getAccountAssets" query on Hyperledger Iroha. If the document has never been signed before and the user has a sufficient balance, the process of signing and embedding the user's digital certificate will run followed by the deduction of user's balance, and then recording the transactions to Hyperledger Iroha with certified PDF SHA-256 hash as the transaction description.

To create a certificate archive in PKCS#12 format, the "node-forge" library can be used by providing certificate chain information, private key, and password to lock the created PKCS#12 archive. QRCode will also be created to verify transactions that has been made if needed. The QRCode will store the hash of the unsigned PDF, which can be used to lookup the document data found in the database. The PDF processing such as certifying, stamping QRCode, and embedding info is done by the PDFTron library. The user's signature will also be stored in the database if there is no same signature found. After processes are completed, all these activities are also recorded in the database. Then the API will send responses containing a success code and a certified PDF buffer.

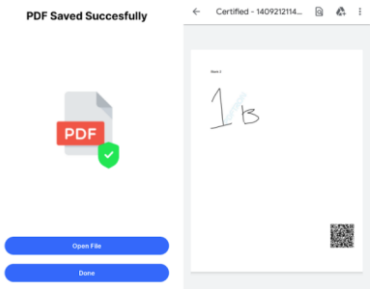

Figure: 4.19 Pop-up if the transaction has been completed by the last signer and the display of documents that have been opened.

The client application will display a modal (pop-up) if the process has been done successfully. Users can also view their transaction history and then download their documents on the “My Signing Request” menu on the “Finished” tab.

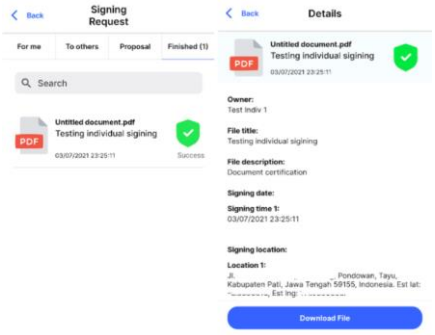

Figure: 4.20 Signing process completed.

4.4 Multiple Signing Activity

In this type of transaction, the number of signings must be carried out by more than one user, and each user must have sufficient balance to be able to sign as an evidence that the user have made a signing transaction.

There are two ways in the group signing process. The first is that the user first signs a document, then on the confirmation page the user selects another user who can sign the document. Then the user presses the "Upload" button. The application will send all information through the “multiple signing” endpoint. If there is no existing document found, the system will carry out activities as before, namely embedding the user's signature and certificate into the PDF, but the first time the PDF will not be locked with permissions so that the next user can sign. Then the transaction will be recorded into the blockchain system and also at the same time deducting the user’s balance. Then the system will record these activities into the database but with the transaction status with the status "On process" because there are still other users who haven’t to sign the document. Users who act as initiators can see the status of their transactions on the "My Signing Request" menu and on the "To others" tab, but when all processes are completed the user can view the completed documents on the "Finished" tab.

The next user can view the signing request on the "My Signing Request" menu on the "For me" tab. To sign the document the user selects the request, then the app will redirect to the signing page. On the confirmation page the “non-initiator” user can’t change the pre-filled data, but can choose whether to include the signing location and contact info. Then when the user presses the “Upload” button the app sends all the information to the same endpoint. The same signing activity will be carried out with the difference that if the user is the last user who hasn’t signed, the system will embed the QRCode, and then lock the document so that it cannot be modified anymore. If it is found that more than one person has not been signed the document, the document won’t be locked. If all signers have signed the document, then all of the participants can download the certified document.

Users can also send signing requests to multiple users without having to sign the document first by leaving the document unsigned, but the user must also include information on who must sign the document. The fee is only charged to the user who did the signing and in the database history still recorded who is the initiator.

4.5 Group Signing as Enterprise Admin

The admin user must have a balance in every enterprise signing. The user selects the “Sign and Certify PDF” menu, then selects “Sign with multiple persons”. The user can sign the document first or just press the "Next" button leaving the document unsigned to send a signing request for its members. The user can then press “Upload” to send the document. The signing request will be sent to the selected user.

Keep in mind that in enterprise transactions, there is a cash flow that is

different from non-enterprise transactions. Only the admin balance is used for payment. If the account used by the user is an “admin” type, then the admin balance will be deducted immediately and sent to the “Iroha admin” account as a record. But if the type of user used is an enterprise “member”, some steps are needed in the background. The system will transfer the required balance from the enterprise admin account to its member, then the system will transfer the member’s balance to the "Iroha admin” account as records of enterprise transactions.

4.6 Group Signing as Enterprise Member

The enterprise cash flow also applies to this transaction. First, the members press the "Sign and Certify PDF" menu on the main page, then select "Make signing request". The user will be asked to enter the document to be signed. At least there must be one signer to be set. Then the user presses the “Confirm” button to do SMS OTP verification. If successful, the proposal will be send through an endpoint.

The enterprise admin account can find the proposal at the "My Signing Request" menu on the "Proposal" tab. Then the admin must choose to reject or accept proposals from members. If the admin accepts, all requests for signing will be forwarded to the selected user that must sign the document.

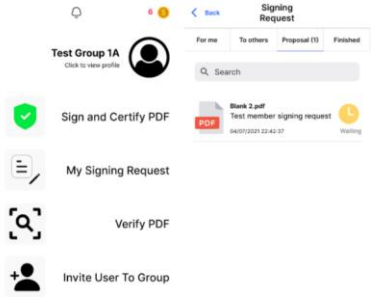

Figure: 4.21 The display of the home page for the admin group users and the display of proposals that have been sent by members.

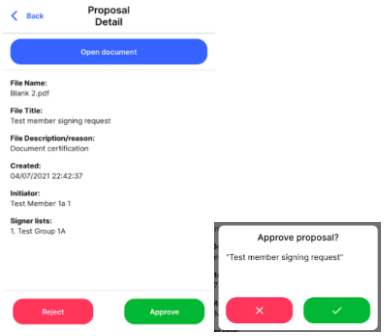

Figure: 4.22 The "proposal detail" page.

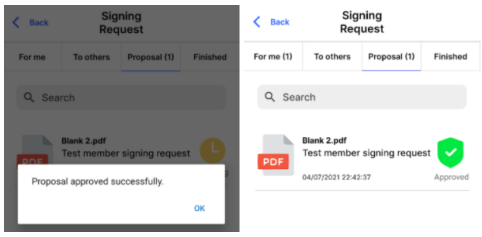

Figure: 4.23 Proposal has been approved.

If the admin has granted permission to sign the document, the user set that can sign the document can look at the "My Signing Request" menu on the "For me" tab. The signing process proceeds as before. If all signer listed have signed the document, they can download the document.

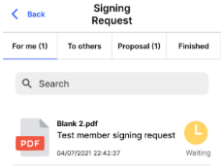

Figure: 4.42 Incoming signing request.

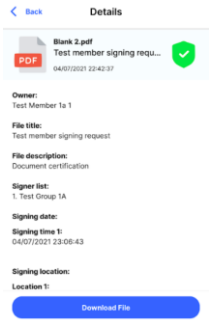

Figure: 4.24 Certified document details.

4.7 Signing Transaction Verification

Verification process can be done in several ways. The first is to search for unsigned document hashes found in QRCode, then retrieve the transaction hashes generated when making transactions through Hyperledger Iroha then querying it via “getTransactions” query.

The second way is to upload the document to be verified. With the document uploaded, further checking can be done. It is even possible to identify, for example, an user uploads a document that has signed from another platform, or even displays transaction data when uploading a document file before it is signed (there is document file data after it is signed).

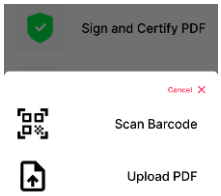

Figure: 4.25 "Verify PDF" menu in the application.

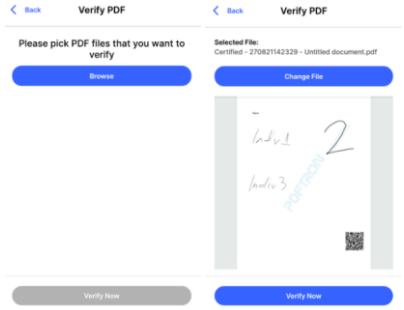

Figure: 4.26 Manual verification (via file)

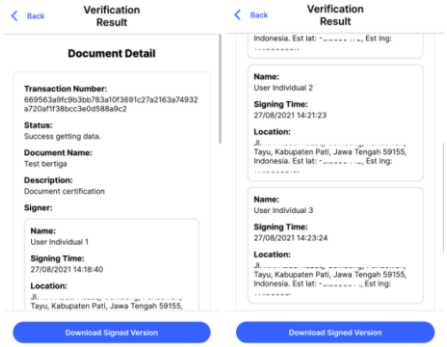

Figure: 4.27 Details of document verification by uploading documents.

Figure: 4.28 Verifying a signing transaction by scanning the QR Code.

4.8 Signing Out

To carry out the "signing out" process is by deleting user data and all JWT tokens stored in the client application. The refresh token is also removed from the database.

4.9 Hyperledger Iroha Block store and WSV Experiment

A simple Hyperledger Iroha security test was also done to find out how Hyperledger Iroha version 1.2.1 can handle when an attack occurs against one or more peers.

4.9.1 Simulation if a peer losing a block with an unordered block

If a peer loses a block with the block store state being unordered, the peer can still receive a new block. But when the peer restarted it won't be able to run as expected. The block conditions in the "blockstore" directory must be in order so that synchronization process will occur by downloading the missing block from the peer that still has a complete block.

4.9.2 Simulation if one of the blocks in a peer's "blockstore" is changed

If one block is removed from a block store, Hyperledger Iroha peer doesn't immediately do a disk synchronization. Synchronization activity will occur when the peer is restarted.

4.9.3 Simulation if several peers have different "blockstore" conditions

If changes are made to almost all peers, then when the peer is restarted the block synchronization process for each peer will be carried out by taking a number of blocks from the peer that still has a complete and sequential number of blocks.

4.9.4 Simulation of all the data on the peer's "blockstore" in the blockchain network is equalized

If block store's block deletion is made by treating all block stores condition the same, it's treated as if nothing happened, and as a result, the missing blocks have been lost forever.

4.9.5 Simulation of data changes in "World State View"

In this simulation, it is assumed that the attacker has access to the database. The first experiment is to make changes to "account details" on an account on the blockchain system via World State View on each peer. The result is that the query

data changed when accessed through the "Get Account Details" query.

The second experiment is if the attacker deletes some vital data such as all of account data. Then the deleted information on the attacked peer cannot be accessed, thus making it become a problematic peer.

4.10 Certified document security testing

Testing is simply done by making changes to documents that have finished certification processes.

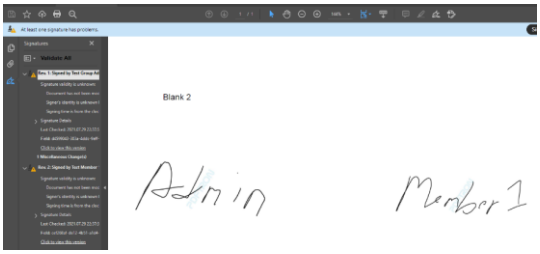

Figure: 4.29 Display of documents that have been completed through the signing process and have also been embedded with digital certificates from each signer.

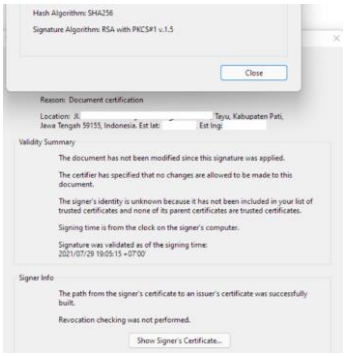

Figure: 4.30 A detailed view of one of the signatures when clicked.

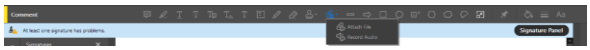

Figure: 4.31 The annotation or comment tool does not work because the permission when saving PDF is set to "no change allowed".

Figure: 4.32 Annotation tool or comment tool with unsecured PDF with no permissions at all can be accessed.

Figure: 4.33 Certificates became invalid due to changes to documents.

Figure 4.33 shows that the certificate is invalid due to document changes because of "no change allowed" settings.

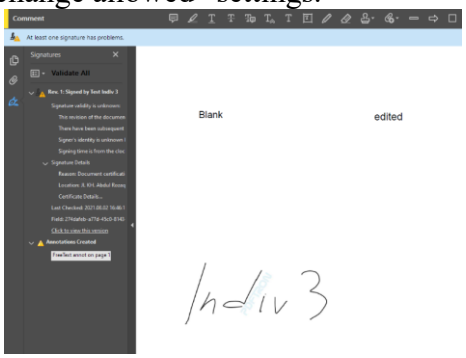

Figure: 4.62 Result if the document is not locked with permissions.

If the document is not locked with permissions, the annotation/comment menu can be displayed in Adobe Reader. And also if someone makes changes to the PDF file and then saves it, the attached certificate and signature won't become invalid, but the user who opens the document will see a warning that says if a change has been made

IV. CONCLUSIONS

The implementation of blockchain can be applied to the process of recording signing activities by embedding the hash of the certified file as a transaction description.

The verification process for documents that have gone through the "transaction" process can be done not only with database but also checked directly through Hyperledger Iroha by searching for the hash of transactions that have been completed on Hyperledger Iroha.

Application development can be done easily and quickly by using Expo for making front-end application, and Node.Js for creating the back-end application. Management of user digital certificates using OpenXPKI and certificate processing using the "node-forge" library. The PDF processing can be done with PDFTron library. Each signing activity is always recorded on the blockchain system. The document verification can be done via file upload or by scanning the QR code that has been displayed on the document page that has passed certification processes.

REFERENCES

[1] "Berapa Pengguna Internet di Indonesia? | Databoks." https://databoks.katadata.co.id/datapublish/2019/09/09/berapa-pengguna-internet-di-indonesia (accessed Apr. 21, 2021).

[2] "Hootsuite (We are Social): Indonesian Digital Report 2020 – Andi Dwi Riyanto, Dosen, Praktisi, Konsultan, Pembicara: E-bisnis/Digital Marketing/Promotion/Internet marketing, SEO, Technopreneur, Fasilitator Google Gapura Digital yogyakarta." https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2020/ (accessed Apr. 21, 2021).

[3] "Digital in Indonesia: All the Statistics You Need in 2021 — DataReportal – Global Digital Insights." https://datareportal.com/reports/digital-2021-indonesia (accessed Apr. 21, 2021).

[4] "Daftar Kejahatan Siber yang Paling Banyak Dilaporkan ke Polisi | Databoks." https://databoks.katadata.co.id/datapublish/2020/09/08/daftar-kejahatan-siber-yang-paling-banyak-dilaporkan-ke-polisi (accessed Apr. 21, 2021).

[5] "Peraturan Pemerintah Nomor 63 Tahun 2019 - Pusat Data HukumOnline.com," 2019. https://www.hukumonline.com/pusatdata/detail/lt5dad2315ee51a (accessed Apr. 13, 2021).

[6] J. Harsono and R. M. No, "Penentuan Model Kepercayaan Infrastruktur Kunci Publik Di Indonesia Dengan Pendekatan," 2016.

[7] A. I. Fatra, R. R. Isnanto, and E. W. Sinuraya, "Perancangan Infrastruktur Kunci Publik Dengan Implementasi Pembuatan Kuitansi Digital Pembayaran Kursus Bahasa Inggris," *Transient*, vol. 2, no. 3, pp. 799–804, 2013, [Online]. Available: https://ejournal3.undip.ac.id/index.php/transient/article/view/3977.

[8] "Perbedaan antara tanda tangan digital dan tanda tangan elektronik | Tanda Tangan Digital vs Tanda Tangan Elektronik 2021." https://id.esdifferent.com/difference-between-digital-signature-and-electronic-signature (accessed Apr. 13, 2021).

[9] "Apa Perbedaan Antara Tanda Tangan Elektronik dan Digital? - SSL.com." https://www.ssl.com/id/faqs/faq-tanda-tangan-digital-dan-penandatanganan-dokumen/ (accessed Apr. 13, 2021).

[10] A. Hidayatullah, Entik Insanudin, MT, "PENGENALAN KRIPTOGRAFI DAN PEMAKAIANYA SEHARI-HARI," *Kriptografi*, no. May, pp. 1–7, 2016.

[11] L. Arief and T. A. Sundara, "Studi atas Pemanfaatan Blockchain bagi Internet of Things (IoT)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 1, p. 70, 2017, doi: 10.29207/resti.v1i1.26.

[12] "What Is MongoDB? | MongoDB," *MongoDB*, 2019. https://www.mongodb.com/what-is-mongodb (accessed May 04, 2021).

[13] C. Győrödi, R. Gyorodi, G. Pecherle, and A. Olah, "A Comparative Study: MongoDB vs. MySQL Energetical sustainability of a local community using air flows View project Convergence of university practical training for integration with success in the labor market View project," 2015, doi: 10.13140/RG.2.1.1226.7685.

[14] "iroha/README.md at master · hyperledger/iroha." https://github.com/hyperledger/iroha/blob/master/README.md (accessed May 04, 2021).

[15] C. Anderson, "Docker," *IEEE Softw.*, vol. 32, no. 3, pp. 102–105, 2015, doi: 10.1109/MS.2015.62.

[16] "2. Concepts and Architecture — Hyperledger Iroha documentation."

https://iroha.readthedocs.io/en/develop
/concepts_architecture/index.html
(accessed Oct. 12, 2021).