Chapter 16

A Decentralized File Storage for Effective E-Government

Ahmad Fajar, Rahmat Trialih, & Fitria Wulandari Ramlan

A. Overview of Decentralized File for Goverment

Countries with fast population growth will lead to various problems related to population. The most central is the issue of data security. The theft of personal data is becoming more common. Even in 2021, President Joko Widodo's vaccination certificate is circulating on social media. This certificate is allegedly derived from the PeduliLindungi application by obtaining an Identity Number from the General Election Commission.

Apart from the president's data, there have also been leaks before. Around 279 million BPJS Health participant data are traded on RaidForums. Also, about 91 million Tokopedia users, then 1.2 million users of Bhineka.com, and 2.3 million voter data from the

A. Fajar, R. Trialih, & F. W. Ramlan
King Abdulaziz University, Saudi Arabia, e-mail: ahmad.fajar@outlook.co.id

Fajar, A., Trialih, R., & Ramlan, F. W. (2022). A decentralized filestorage for effective e-government. In R. Trialih, F. E. Wardiani, R. Anggriawan, C. D. Putra, & A. Said (Eds.), *Indonesia post-pandemic outlook: Environment and technology role for Indonesia development* (279–295). DOI: 10.55981/brin.538.c497 ISBN: 978-623-7425-85-4
E-ISBN: 978-623-7425-89-2

General Election Commission have been traded on the internet. This fact indicates that the protection of personal data still needs to be a concern by the government.

Personal data protection is increasingly important, especially during a pandemic when transactions begin to switch to digital or online due to restrictions on people's mobility. The cyber police recorded that the public reported 182 cases of data theft. This figure increased by 27.3% compared to the previous year, with 143 reports. Over the last five years, the increase in reports of data theft increased by 810% from 20 reports in 2016 (Jayani, 2021). The public must also protect personal data by not spreading personal and confidential information. In addition, the public needs to read the privacy policy when accessing social media to avoid unwanted incidents.

Those things can happen because the data storage system is still centered in one location or server. This term is called the centralized server. Storing and accessing files containing sensitive data such as medical records, financial history, personal information, and legal papers is difficult since it involves file system administration and authorization of those data. We have gone far from the inflexible and unreliable paper-file storage method to today's digital alternatives. Cloud-based centralized storage technology has outperformed local physical storage devices such as hard drives and servers during the last decade. About 94% of all enterprises now adopt centralized cloud solutions for data storage. Users may store data over the internet and access it remotely using centralized storage systems everywhere. Major organizations centrally hold data in a cloud storage system.

Cyberattacks and other security issues are made possible by such data. Decentralized storage solutions rely on a peer-to-peer network of users who individually store tiny, encrypted chunks of the actual data. Consequently, a reliable data storage and sharing system have been created. It might be built on a blockchain or any other peer-to-peer network. Enabling this technology for government or other sensitive data can minimize stealing those data.

B. The Blockchain

1. Technology behind Decentralization

We need to explain this term thoroughly. Before we go through it in detail, let us know each part related to the blockchain.

In daily life, people use computers to read and change data. It is possible to buy a computer of many different types. These types include laptops, desktop computers, tablets, and smartphones. Data is information in various forms, from videos and photos to text. In the past, we kept things like paper or film. Our computer can keep this data digitally. It has a lot of different parts that work together to make it easy for us to get and change all that data quickly and easily in a digital format.

If our data is saved on a local computer, it means no connection to the internet. Suppose we keep our data on the internet. The computer is called a server. Servers host websites, databases, files, or other services. It comes physically, but only authorized person or organization can access it directly. When we want access to a website, we access the server that stores it. For instance, when we want to send a message on Facebook Messenger, we access a Facebook server providing the messenger's service.

Every computer has an IP address (internet protocol address), effectively its mailing address. A website's name is just an IP address code. When you enter Facebook into your browser search box, it sends you to the Facebook server.

The next question is where we store our data? A database is a place that can keep our data saved. The database is on servers that can be easily accessed, managed, and updated. A small system only needs a small database on its server. On the other hand, big companies like Google and Facebook use massive servers to run or store their applications and users' data. It consists of many servers called data centers. Only those companies can manage the data center. Therefore, the user's data will depend on the company. Because of fires and hacks,

data could be lost or leaked at the data center. Hackers will find places to attack because the system is in one place. Because of this, some databases are distributed across servers in different areas; this kind of database is called distributed databases.

Distributed databases are databases that are stored on several servers with different locations. If one server goes down, it can continue running to serve the application or request. From this checkpoint, we can get the rough meaning of distribution. We are almost to the blockchain.

The main things that make them different are what kind of data, how it is stored, who can access it, and who can see it. Once data is created on a blockchain, it cannot be changed or deleted.

A blockchain is a database shared by all the computers in a computer network. As a database, a blockchain stores information digitally in a form that can be read and used. Blockchain is best known for its important role in cryptocurrency systems, such as Bitcoin, where they keep a record of secure and independent transactions. A new thing about a blockchain is that it makes people trust each other without needing a third party.

In the blockchain, data is stored in blocks linked together via cryptography. It is one transaction. Another case is when there are too many transactions for a block. It will be added to a long chain of transactions called "blockchain". Besides, when you do this, you will get a chronological record of transactions, like a ledger. This situation goes from the first transaction in the first block to the last transaction in the most recent block. The blockchain stores these blocks in a way that allows us to see a perfectly-recorded history of the Bitcoin transactions that took place over the past year (Conway, 2021).

C. Usage Ideas and Examples of Blockchain

However, blockchain technology has a lot of potential applications than merely serving as the fuel for Bitcoin. The "business intelligence"

article highlighted some of its emerging uses in banking, business, government, and other fields below (Intelligence, 2022).

(1) Blockchain in Banking and Finance

(a) **International Payments**

Blockchain technology enables the secure and rapid development of a tamper-proof record of sensitive activity. As a consequence, it is well-suited for international payments and money transfers.

(b) **Regulatory Compliance and Audit**

Blockchain is very safe, making it a good tool for accounting and auditing because it reduces the risk of human error and ensures the integrity of the records. When the account records are locked in with blockchain technology, no one can change them, even those who own them. In this case, the trade-off is that blockchain technology could eventually do away with the need for auditors and cut down on the number of jobs.

(c) **Money Laundering Protection**

Again, the encryption so important to the blockchain makes it very good at stopping money laundering. The technology that allows businesses to keep track of their customers' identities is "Know Your Customer (KYC)." Companies use this process to discover their customers and verify their identities.

(d) **Insurance**

Smart contracts are most likely the best approach to leverage Blockchain in insurance. These contracts enable consumers and insurers to process claims simply and securely. All contracts and claims may be stored on the blockchain and authenticated by the network, preventing anyone from making fraudulent claims. The blockchain would reject several claims for the same accident since it would not allow more than one.

(e) **Peer-to-Peer Transaction**

Venmo and other P2P payment services are easy to use but have limitations. Some services do not allow transactions based on where

you live. For other people, you must pay a fee to use them. Many of them can be hacked, which is unsuitable for people who put their personal financial information. Blockchain technology could also solve these problems with all the benefits it has.

(2) Blockchain Application in Business

(a) **Supply Chain Management**

Blockchain is a good choice for tasks like real-time tracking of goods as they move and change hands through the supply chain. Using a blockchain gives companies a lot of different ways to move these goods. A blockchain can put events in a supply chain in order. For example, when goods arrive at a port, they can be put into different shipping containers. Blockchain is a new way to organize and use data. It is a way to keep track of things and use them.

(b) **Healthcare**

Health data that can be used on the blockchain includes general information like your age and gender and essential medical history data, like your immunization history or vital signs. On its own, none of this information would be able to identify any person, which is why it can be stored on a shared blockchain that many people can access without worrying about privacy.

If you have many specialized medical devices connected to your health record, blockchain can help you link those devices to your record. There will be a way for devices to store the data made on a healthcare blockchain and add it to people's medical records. Connected medical devices have a big problem because the data they produce is split up into different places. Blockchain could be the link that connects those other places.

(c) **Real Estate**

Most people will move about 12 times throughout their lives. The average home is sold by a homeowner every five to seven years. Using

blockchain could benefit the real estate market because it moves so often. It would speed up home sales by quickly verifying finances, reducing fraud thanks to encryption, and making the selling and buying process more transparent.

(3) Blockchain Applications in Government

(a) **Record Management**

The government keeps people's birth and death dates, marriage status, and property transfers. However, keeping track of all this information can be challenging, and some of these records are still on paper. Sometimes, people must go to their town hall to make changes, which is time-consuming, unnecessary, and frustrating. Using blockchain technology could make this record-keeping a lot easier and safer.

(b) **Identity Management**

Blockchain technology can be useful if it has enough information, especially in identity management cases. It will help people's activity by showing or providing their special authentication code. For example, The World Food Programme used a similar Blockchain-guided approach for their biometric ID and digital payments. It allows refugees in a Jordanian camp to reserve funds and purchase goods without physical documents or valets. Furthermore, with the advent of Schengen II, the European Union (EU) is considering digital identity and working on the mobility of identity-related credentials in its member states through the eIDAS Directive (EU Regulation No 910/2014). A trend is shifting "control" of identity away from governmental institutions and corporate actors and toward "self-sovereign individuals" who can now manage their digital selves autonomously.

(c) **Voting**

Blockchain technology can make it easier for people to vote while also being more secure. Because even if someone were to get into the terminal, they would not be able to do anything to other nodes. Each

vote would be linked to a single ID, and with the ability to make a fake ID impossible, government officials would be able to count votes more quickly and effectively.

(d) **Taxes**

Experts in technology and tax from the private and public sectors join forces to investigate the potential of blockchain. Much information could be stored on the blockchain to make the time-consuming and prone to human error process of filing taxes much more efficient.

(e) **Non-Profit Agencies**

Blockchain could help charities fight antitrust by making them more transparent. The technology can show donors that NPOs use their money the way they say they are. Blockchain technology could also help those NPOs give those funds more quickly, manage their resources better, and improve their ability to track them.

(4) Blockchain Applications in Information, Communication, and Technology (ICT)

(a) **Record Management**

As previously stated, encryption based on blockchain makes it very effective for record management by preventing duplicates, false entries, and other errors.

(b) **Cybersecurity**

Blockchain is a big help in cybersecurity because it does not have a single point of failure. Another benefit of blockchain technology is that it can be used to keep your information safe and secure from start to finish.

(c) **Big Data**

Because the information on the blockchain cannot be changed, and every computer on the network continuously checks its information, blockchain is a great way to store big data.

D. Interplanetary Filesystem (IPFS): Advance Technology for Sharing File

Blockchain uses smart contracts running on a decentralized virtual machine. Users might create a decentralized application (dApps) using this second generation of technology (Wood, 2022). Additionally, the Interplanetary File System (IPFS), a peer-to-peer distributed file system, is an intriguing architecture to consider in conjunction with blockchain. It combines various previously successful methods that use a content-addressed block storage paradigm to store data. IPFS aims to enhance HTTP, the most widely used file-sharing protocol (Hsiao-Shan et al., 2020).

It allows us to learn more about IPFS. Assume we wish to download a photograph from the internet. We instruct the computer where to look for the picture when we do this. In this example, the picture's location is an IP address or domain name, such as *http://websitename.com/tiger.jpg*. This method is known as "Location-Based Addressing." We tell the computer where to retrieve the information, but you will not get the picture if the location is inaccessible, or the server is unavailable. However, if this occurs, there is a good probability that someone else has already downloaded that image and still has a copy. The computer will be unable to get a copy from that person. To overcome this, IPFS switches from "location-based" to "content-based" addressing (Drake, 2015). Instead of mentioning/where/to look for the resources, you say/what/we need.

There is a hash for every file. This hash is like a fingerprint. To get a file, we ask the network: "Who has the file with this hash?" Someone in the IPFS network will give it to us, and we will use it. They might ask how we know that person has not changed the file. Because we used a hash to ask for the file, we can check to see what we got. We ask for a file with a certain hash. When we get the file, we check to see if the hash is the same as we asked. It is safer than before now. Use hashes to find content that does not have to be repeated. When many people put the same file on IPFS, it will only be made once, making the network easier to use.

How does IPFS work? Files are kept within IPFS objects, which may hold up to 256kb and include connections to other IPFS objects. For example, we save a "Hello World" text file that is relatively short and is saved in a single IPFS object. But what about files greater than 256kb? As an example, consider a photograph or video. Those are divided into numerous IPFS objects of 256kb each, and the system then creates an empty IPFS object that connects to the other parts of the file. IPFS's data architecture is simple, yet it may be quite powerful. This design enables us to utilize it as a filesystem. For example, we have a basic directory structure with a few files. We can transform this into IPFS objects and construct one for each file and directory. IPFS employs content-based addressing. Once anything is introduced, it cannot be removed. It is an immutable data repository, similar to a blockchain.

How do we edit things on that file if modified or updated? IPFS supports the versioning of files. We are working on a critical document that will be shared with everyone through IPFS. IPFS will generate a new commit object for us. This object is critical since it informs IPFS which commit came before it and relates to our file's IPFS object. After a time, we would like to update this file. We upload our changed file to the IPFS network, and the program generates a new commit object for us. This commit object now refers to the previous commit. This method may be repeated indefinitely. IPFS will ensure that our file and its history are available to all network nodes.

The most challenging issue that IPFS confronts is keeping files accessible. Every node on the network maintains a cache of downloaded files and helps others distribute them if needed. However, if these four nodes host a certain file - and those nodes go down, that file becomes inaccessible, and no one can get a copy of it.

This dilemma may be solved in two ways. We can either incentivize individuals to keep files and make them accessible or proactively distribute files and ensure that there are always a specific number of copies available on the network.

In this case, the government has many institutions and should have at least one data center. We can use those data centers as nodes or use other people's spaces on their computers and pay for that space.

E. Decentralized Storage for Sensitive File

Data breaches and loss usually become the real deal, and the most common problem happens in many organizations, including countries. Today's data can be accessed on the internet quickly, and there is no perfect protection in protecting data, especially for sensitive files that may contain important information. This situation allows the data to be transferred freely in the business network, cloud, and devices, raising the risks of data breaches. Data breaches were mentioned as severe threats to organizations, which may cause great harm, including significant reputational damage and financial losses (Long et al., 2017). By referring to IBM and the Ponemon Institute's recent studies, many companies and organizations have suffered data breaches more than 17,000 times annually. It is possible if sensitive data related to the government is in it (IBM, 2021).

Most of these breaches resulted in a significant data leak that may have caused a loss in productivity, decreased public confidence, trust, and increased costs associated with government response (Waind, 2020). Due to the growing number of security threats, data loss and data leakage in government have become significant concerns because public data are secret and not allowed to be disseminated freely. In general, the process of sharing data for business-related activities, both internally and externally requires good safety. The possibility of data theft and misuse is rising, and the government should prevent their action. Therefore, the government can utilize distributed ledger technology known as blockchain to prevent and secure sensitive organizations' data (de Haro-Olmo et al., 2020).

F. Utilizing Blockchain to Protect Sensitive Data

We must understand that governments need to save and share sensitive data with their underlings' departments internally and externally. When this action is taken, it may be shared through email or cloud service. Based on this situation, we can suggest that the data is usually unprotected and leaked to unsupervised people. It will be dangerous if such action is taken using the stolen data. For example, it is used to deceive an easily fooled person. Blockchain technology can prevent this situation from happening because it uses a peer-to-peer method that allows all participants in the network to have an identical copy of the ledger. When any changes happen to the ledger, it will also reflect in all copies in minutes or some cases, seconds. We argue that distributed ledger technologies can help the government protect sensitive data and ensure the integrity of data records.

G. Implementation for the Government

The main problem we would like to solve is securing personal data. Many companies or the government try to protect the users' data. Nevertheless, their system can still be hacked. Therefore, it is not enough to only protect the algorithm in code. Also, the storage of these data is still centered in one place. The system is easily penetrated and even more dangerous if the government does not have a backup.

We want to emphasize that blockchain applications are still in their infancy and represent an incredibly fast-paced subject with no established theory, few recognized specialists, and no clear solutions. Scholarly discussion on this topic is still in its infancy, with the majority of attention focused on Bitcoin's technological, financial, and legal aspects. As a result, a thorough examination of the influence of blockchain technology on political governance and democracy, in general, is sorely missing at the moment (Atzori, 2017).

The combination between Blockchain and IPFS could be the best solution for this matter (Hsiao-Shan et al., 2020). Previous research

has already adopted this approach. They proposed a design model for a permission-less sharing system. The member in the system could create a group or join an existing group and send the file to it. Otherwise, the member can also request a file from that group. Sending and receiving the file needs a key generated in the IPFS proxy, Shah et al (2020). also proposed a similar solution for securing the storage. The IPFS protocol is then used to distribute and store encrypted data across network peers.

To make our sensitive data well protected. We can use this technology to secure our data, especially in Indonesia, with many institutions spread over several areas. We are trying to specify the implementation. For instance, we want to apply IPFS and Blockchain in Social Security Administrator for Health (BPJS Kesehatan). The people who want to open a new account in BPJS Kesehatan usually need to come to the office. The office here is a branch office or smaller office. Staff will input the personal data using his computer, then store it in the database through software.

However, the software will store that data in a database using a relational database management system (RDBMS) stored on one server. Could you imagine we changed how the software puts the applicant data? As we mentioned before, we can use the benefits of Blockchain and IPFS. The data will not be saved in the central database but distributed to the network nodes.

We can implement this matter in real life. We can make it a node for the computer used by the front liner staff. For instance, five staffs are in one branch office, so we have five nodes. Then, multiply by the total branch office that BPJS Kesehatan has. Do not worry about data security in one computer; a key protects the data from IPFS proxy. Furthermore, the user or staff who need that data should request a decrypt key through the network security builds in.

How about the trend that people no longer need to come to the office, just use their smartphones? The basic idea is the same; we only change how to save and access the data. From centralized storing and

accessing, it becomes decentralized. Not limited to storing or accessing the files, it also tracks the file's history. Who was the creator? Who is trying to access that file and all updated versions?

H. Recommendations

1. Involving Stakeholders

Consider the objectives: What technology feature gives the essential advantage or benefit to a specific technical architecture product, service, or component? Examine whether distributed ledgers are the best vehicle for your objectives.

Collaborate with all internal stakeholders; Decentralized blockchain technology should not be confined to the innovation laboratory or the technical team. Collaborate immediately with the many stakeholders within your company to ensure that the solution is planned from the start to satisfy the regulatory, commercial, and technological issues that will undoubtedly occur.

Obtain executive approval; Board-level buy-in would be required to meet aggressive targets. Educate to close technological gaps and make the realm of public blockchains less intimidating.

Deal with legal issues head-on; Certain use of distributed ledger technology will undoubtedly generate legal concerns. According to some experience, regulators are becoming more pragmatic when evaluating innovation and regulation that predates certain technology.

We advocate starting early with regulators and educating them about the solution and its benefits. It is critical to ensure that you have evaluated the potential legal challenges before proceeding.

2. Government

We want to see a government working group define key investigation areas and, potentially, controlled pilots. It is not about attempting to solve everything at once but about taking small steps that, over time, may make a difference.

A decentralized record of transactions will enable anything of worth and decide whether it includes trade securely, straightforwardly, and without the threat of trying to interfere. This situation could have been what society has been looking for exactly. It can deliver real-time, reliable information to many people and create a system, for example, in which taxpayers and tax authorities have equal trust in the factuality of the data obtained. It may make it easier to pay taxes and for governments to close the tax gap.

3. Society

Recommendations for society could be divided into several fields:

(a) On Research:

We can encourage collaboration and collaborative work among specialists from different fields of the research world. This action will increase the value and interest in Indonesian language competence. In addition, it can increase Indonesia's research efforts on privacy. In addition, we can concentrate on the part of the software engineering capabilities on the blockchain infrastructure and application difficulties. Then, we need to investigate the establishment of an international interdisciplinary Blockchain Institute.

(b) On the Digital Trust:

Begin a certification reflection using blockchain to develop new certification skills for products and services. Begin work on a project to create a scalable, modular digital identification service for individuals and businesses.

(c) On the Public Policy Support:

Create a public research advisory council to advise the state on blockchain-related technology concerns.

4. Academic

Establish master's level specialist training, specialized R&D engineers, and application engineers by higher education organizations. Encour-

age work-study programs at the field's research and development facilities.

Design a MOOC (Massive Open Online Courses) to offer and support current efforts on the subject, for example, offer hosted on the platform, and create specific technologies that allow for a high level of learner involvement.

I. Conclusion

We know that blockchain technology gives benefits, and previous research has already discussed how this technology can be used in governments and other countries' sectors. However, we are sure that this technology should be implemented carefully. We see this as an opportunity, and by considering the risk, we ought to recommend a top-down approach to implementing blockchain in government. Moreover, we should remember that implement blockchain is not an easy task. Besides using the government or representative council to create the policy, it will be wiser to involve other stakeholders. We can use the triple helix approach of government, society, and academia. We are sure that if the communication between these three stakeholders runs smoothly, it will help Indonesia create a better government environment with good safety.

References

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

Cheng et al. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. In *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5)*. Wiley-Blackwell. https://doi.org/10.1002/widm.1211

Conway, L. (2021). What is a blockchain? The simple explanation - The street crypto: Bitcoin and cryptocurrency news, advice, analysis and more. *The Street*. https://www.thestreet.com/crypto/bitcoin/what-is-a-blockchain-the-simple-explanation

de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymization: A systematic literature review. *Sensors (Switzerland)*, *20*(24), 1–21. https://doi.org/10.3390/s20247171

Drake, K. (2015). HTTP is obsolete. It's time for the distributed, permanent web. *IPFS.IO*. https://ipfs.io/ipfs/QmNhFJjGcMPqpuYfxL62VVB9528NXqDNMFXiqN5bgFYiZ1/its-time-for-the-permanent-web.html

Huang et al. (2020). A secure file sharing system based on IPFS and blockchain. In *Proceedings of the 2020 2nd International Electronics Communication Conference,* 96–100. Association for Computing Machinery. https://doi.org/10.1145/3409934.3409948

International Business Machines Corporation (IBM). (2021). Cost of a data breach report 2021. https://www.ibm.com/security/data-breach

Intelligence, I. (2022). The growing list of applications and use cases of blockchain technology in business and life. Business Insider. https://www.businessinsider.com/blockchain-technology-applications-use-cases?r=US&IR=T

Jayani, D. H. (2021). Pencurian data pribadi makin marak kala pandemi. *Databoks*. https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi

Shah, M., Shaikh, M.Z., Mishra, V., & Tuscano, G. (2020). Decentralized Cloud Storage Using Blockchain. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 384-389.

Waind, E. (2020). Trust, security and public interest: Striking the balance a narrative review of previous literature on public attitudes towards the sharing, linking and use of administrative data for research. *International Journal of Population Data Science, 5(3).* Swansea University. https://doi.org/10.23889/IJPDS.V5I3.1368

Wood, G. (2022). Ethereum: A secure decentralized generalized transaction ledger eip-150 revision. https://gavwood.com/paper.pdf