Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain

Andi[1*], Carles Juliandy[2], Robet[3], and Octara Pribadi[4]
[1−4]Informatics Engineering Department, STMIK TIME
Medan 20212, Indonesia
Email: [1]andi@stmik-time.ac.id, [2]carlesjuliandy@stmik-time.ac.id, [3]robet@stmik-time.ac.id,
[4]octarapribadi@stmik-time.ac.id

***Abstract*—The rapid and dangerous spread of COVID-19 has forced governments in various countries to provide information on patients' medical records to the public in the context of prevention. Meanwhile, patients' medical records are vital and confidential because they contain patients' privacy. Changing and falsifying a patient's medical record leads to various dangerous consequences, such as mishandling which results in the patient's death. From these problems, the research introduces a new model with a combination of blockchain technology and the Elliptic Curve Digital Signature Algorithm (ECDSA) to secure the medical records of COVID-19 patients. This model is an improvement from the model and framework proposed by previous researchers. The proposed model consists of two big parts (front and back end). Then, the simulations are carried out to measure and prove the level of security of blockchain technology in securing patient medical records. The research results show that the ECDSA algorithm can protect patients' medical records from being opened by unauthorized parties. Then, blockchain technology can prevent changes or manipulation of patient medical records because the information recorded on the blockchain network is impossible to change and will be immutable. The research has successfully introduced a new model in securing patient medical records.**

***Index Terms*—Medical Records, COVID-19, Elliptic Curve Digital Signature Algorithm (ECDSA), Blockchain Technology**

I. Introduction

THE COVID-19 is an infectious disease that its outbreak first appeared in 2019 and has spread to all countries in the world [1]. Based on data from Worldometer on February 24th, 2022, COVID-19 disease infected 430,230,124 people worldwide and caused the death of 5,936,969 people [2]. The rapid and dangerous spread of the COVID-19 disease has forced governments in various countries to provide information on patients' medical records to the public in the context of prevention so that people who come into contact with patients can immediately self-isolate and stop the chain of spreading the virus [3]. However, the patients' medical records are very important and confidential because it contains patient privacy. If the information is spread to the public, it is certainly very dangerous because irresponsible parties can use or manipulate it [4, 5]. Although many institutions have changed the way of storing patients' medical records from paper-based to electronic, this method still has weaknesses, such as patients' medical records that can be accessed by unauthorized institutions and threats in the form of hacking and falsification of patients' medical records [6–8]. Changing and falsifying the patients' medical records is very dangerous because it can cause mishandling from the doctor to the patient. For example, the doctor gives medicines that the patient should not consume because the patient has allergies and particular medical history. The mistake is fatal and can lead to the patient's death [8].

Blockchain technology can be used to secure the medical records of COVID-19 patients. This technology is a decentralized ledger that stores or provides recording and tracking processes on the network without involving third parties. Every data stored in the Blockchain network will be encrypted using cryptographic functions and stored in a block. Therefore, with the help of cryptography, these blocks are linked together so that no modifications can be made. If there is a change in data in one block, it will affect the hash value of the following blocks. It means that hackers must resolve the hash values of all blockchain networks if they want to make data changes. This condition is

Received: Dec. 08, 2021; received in revised form: March 08, 2022; accepted: March 08, 2022; available online: March 31, 2022.
*Corresponding Author

undoubtedly impossible to do because it takes a very long time [9–11]. Blockchains can be classified into three categories: permissionless blockchain, public permissioned blockchain, and permissioned blockchain. The blockchain used in the research is permissionless because this type of blockchain has the characteristics of being decentralized, transparent, and immutable. In addition to its advantages, permissionless blockchain has the disadvantage of slow transaction speeds and requiring high computing power [12]. Unlike the public permissioned blockchain and permissioned blockchain, both types have faster transaction speeds and are more energy-efficient. However, these two types of blockchain have a lower level of security, are not decentralized, are less transparent, have partial immutability, and are still restricted and controlled by specific parties [13, 14]. In the research, the priority is the security of patient medical records so that the permissionless blockchain is the right type of blockchain to be implemented [15].

Several previous studies discussed the application of blockchain technology in securing medical records of general patients or COVID-19 patients. One of the studies of using blockchain technology in securing patient medical records shows that blockchain technology can ensure that patient medical record data is not tampered with and increase the security of the data [16]. Furthermore, another previous research proposes a low-cost blockchain technology application model to store and view the medical records of COVID-19 patients in the form of patients' status and transaction history details related to their medical condition. The research results indicate that patients' medical records stored in the blockchain network will be stored securely, cannot be changed, and can only be seen by participants with access rights [4].

Moreover, previous studies mention that blockchain technology is very safe in securing patient medical records but has not directly carried out simulations in measuring the security of the technology in their proposed model. In addition, the mechanism for maintaining access rights from the proposed model still has shortcomings. It is still possible for the patients' medical records stored in the network to be hacked and accessed by unauthorized parties. Thus, it requires increased security in ensuring that only interested parties with access rights can view the patients' medical records [17].

The contribution of the research is to introduce a new model in securing patient medical records. The proposed model combines blockchain technology with a digital signature scheme algorithm, namely the Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA algorithm is chosen because it has advantages over other digital signature algorithms, such as Rivest Shamir Adleman (RSA) and ElGamal algorithms. Moreover, the ECDSA algorithm can provide the same level of security with less key size and overhead than other digital signature algorithms [18–20]. Blockchain technology ensures that the medical records of COVID-19 patients are stored securely and cannot be altered or manipulated. Then, the ECDSA algorithm ensures that only interested and identified parties can view the patients' medical records. In addition, in the research, simulations are carried out to measure and prove the level of security of blockchain technology in securing patient medical records.

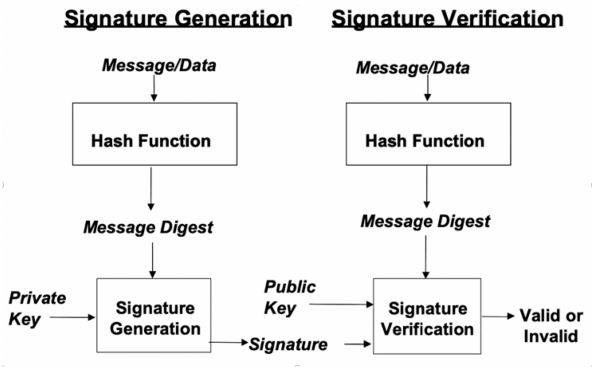

Fig. 1. Digital signature scheme.

II. Literature Review

A. Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) is an electronic analog of a written signature that uses a mathematical scheme by relying on the content of the message and the sender of the message to prove the authenticity of a message or document. This scheme is carried out to guarantee that the data and information come from the correct source. DSA has two main functions, namely signature creation and signature validity checking, developed from the ElGamal algorithm. DSA uses two keys: the public key and the private key. The formation of a signature uses a private key, while digital signature verification has a public key, as illustrated in Fig. 1 [21].

In the first step of digital signature generation, the data messages are compressed by subjecting them to a hash function, resulting in a fixed-size message digest. Then, hash algorithms provide another level of security as they are designed so that it is impossible for two messages that are not similar to be assigned the same hash value. On the other hand, it is impossible to determine the contents (message) by reverse-engineering the message digest. Message-Digest 5 (MD5) and

Secure Hash Algorithm (SHA) are some of the hash functions in common use today. FIPS 180 specifies SHA-2 as the current hashing standard for encryption. In the second stage of digital signature generation, the resulting message digest is signed using the signatory's private key. Consequently, the digitally signed message is sent to the receiver. Finally, on the receiving end, the signature is verified by using the signatory's public key. If the hash values are equal, the signature is valid. It means that the integrity of the message is intact and authentic. If a hacker alters even a single bit in the message, the hash values will not be equal. So, it invalidates the signature [22].

B. Elliptic Curve (EC)

Before discussing ECDSA, the structure of the elliptic curve is discussed. The basic facts of elliptic curves over a finite field of F_p. Let E be an elliptic curve over F_p. In this section, it is assumed $p \neq 2,3$. Then, E may be described in terms of the Weierstraß equation as follows:

$$\begin{aligned} &y = x^2 + ax + b, \\ &a, b \epsilon \mathbb{F}_p, \\ &4a^3 + 27b^2 \neq 0. \end{aligned} \tag{1}$$

The requirement of $4a^3+27b^2 \neq 0$ ensures that E is non-singular. It means, in particular, that one may compute the tangent at every point on the curve. Several different representations for elliptic curves exist. Only the affine representation (cf. Eq (2)) is used within this guideline. The set of rational points in E over F_p denoted by $E(F_p)$ is

$$E(\mathbb{F}_p) = \{(x, y) \epsilon \mathbb{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \tag{2}$$

where O is the point at infinity. It is the projective closure of the equation of $y^2 = x^3 + ax + b$ and may not be described in terms of two coordinates in F_p.

$E(F_p)$ carries a group structure with the point at infinity acting as the identity element. The binary operation of rational points in $E(F_p)$ is commonly denoted as an addition. It turns out that the addition of points in $E(F_p)$ has a simple geometric interpretation, visualizing the operations on an elliptic curve defined over R.

Let $P \epsilon E(F_p)$ and $Q \epsilon E(F_p)$ be points on the elliptic curve. The addition law uses the chord-tangent process where the following different cases have to be distinguished:

- Let $P + O = O + P = P$ for all $P \epsilon E(F_p)$. Thus, O acts as the identity element in the group $E(F_p)$.
- Let $P \neq O$ and $P = (xp, yp)$. The point $(xp, -yp)$ is an element of $E(F_p) \setminus \{O\}$ and one defines $-P = (xp, -yp)$. Additionally, one sets $-O = O$. The identity $P + (-P) = O$ holds for all $P \epsilon E(F_p)$.
- Let $P \neq O$, and $Q \neq O$ such that $P \neq \pm Q$, i.e., P and Q have different x-coordinates. The line through P and Q intersects $E(F_p)$ in a third point $R \epsilon E(F_p) \setminus \{O\}$. One sets $P+Q = -R$. This definition leads to the following addition rule: Set $\lambda = (yQ - yp)/(xQ - xp)$ and $P+Q = (xR, yR)$ (the denominator is different from zero, as $xP \neq xQ$). Then, xR and yR may be computed by the following formula.

$$xR = \lambda^2 - xP - xQ, yR = \lambda(xP - xR) - yP. \tag{3}$$

- Let $P \neq O, P \neq -P$. The tangent to $E(F_p)$ in P intersects $E(F_p)$ in $R \epsilon E(F_p) \setminus \{O\}$, and it is set to $[2]P = -R$.
- This description leads to the following doubling rule: Set $\lambda = (3x^2P + a)/(2yP)$ and $[2]P = (xR, yR)$. Then, xR and yR may be computed by the following formula.

$$xR = \lambda^2 - 2xP, yR = \lambda(xP - xR) - yP. \tag{4}$$

The chord-tangent process for an elliptic curve over real numbers has the above $(E(F_p), +)$ is an Abelian group. The order of $E(F_p)$ may be estimated due to a theorem of Hasse. Hasse's theorem shows that $\#E(F_p) \approx p$, i.e., p and $\#E(F_p)$, is the same order of magnitude. The equation is as follows.

$$p + 1 - \sqrt[2]{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + \sqrt[2]{p}. \tag{5}$$

C. Elliptic Curve Digital Signature Algorithm (ECDSA)

Scott Vanstone proposed ECDSA in 1992 to ensure data integrity and prevent data tampering. It was in response to the National Institute of Standards and Technology (NIST) request for public comments on its first proposal for DSS. It was accepted in 1998 as an International Standards Organization (ISO) standard (ISO 14888-3), accepted in 1999 as an American National Standards Institute (ANSI) standard (ANSI X9.62), and accepted in 2000 as an Institute of Electrical and Electronics Engineers (IEEE) standard (IEEE 1363-2000) and a Federal Information Processing Standard (FIPS) (FIPS 186-2) [23]. After that, FIPS 186 version 2009 introduced a new digital signature technique based on elliptic curves, known as Elliptic Curve Digital Signature Algorithm (ECDSA) [24]. This algorithm is a development of DSA, in which both algorithms rely on Discrete Logarithm (DPL) problems. However, the ECDSA algorithm uses a set of points on the curve,

and the generating key is small [23]. This algorithm consists of three procedures [23].

- Key generation:
  1) Select a random or pseudorandom integer d in the interval $[1, n–1]$.
  2) Compute $Q = dG$
  3) Public key is Q, private key is d.
- Signature generation:
  1) Select a random or pseudorandom integer $k, 1 \leq k \leq 1$.
  2) Compute $kG = (x1, y1)$ and convert $x1$ to an integer $\bar{x}$.
  3) Compute $r = x1 \bmod n$. If $r = 0$, go to step 1.
  4) Compute $k^{-1} \bmod n$.
  5) Compute SHA-1(m) and convert this bit string to an integer e.
  6) Compute $s = k^{-1}(e + dr) \bmod n$. If $s = 0$, go to step 1.
  7) Signature for the message m is (r, s).
- Signature verification:
  1) Verify that r and s are integers in the interval $[1, n - 1]$.
  2) Compute SHA-1(m) and convert this bit string to an integer e.
  3) Compute $w = s^{-1} \bmod n$.
  4) Compute $u1 = ew \bmod n$ and $u2 = rw \bmod n$.
  5) Compute $X = u1G + u2Q$.
  6) If $X = \Theta$, reject the signature. Otherwise, convert the x-coordinate, $x1$ of X, to an integer $\bar{x1}$, and compute $v = \bar{x1} \bmod n$.

D. Blockchain Technology

Blockchain was first created by Satoshi Nakamoto in 2008 and used as a ledger for public transactions of the cryptocurrency Bitcoin [25]. After this discovery, blockchain has become a technology in great demand and continued to evolve from Blockchain 1.0 to Blockchain 4.0. Blockchain 1.0 refers to digital currencies. Blockchain 2.0 is associated with smart contracts. Blockchain 3.0 is used for digital society, such as new technologies that are still under development, which can be applied in various fields, such as health [10], the food sector [26], electronic voting [27], and education [9]. The latest version is Blockchain 4.0, which is a real implementation of blockchain in business to fulfil the daily useable requirements [28]. Figure 2 shows the use of blockchain technology in various fields.

The research focuses on the application of blockchain in the health sector, especially to secure patients' medical records. The implementation of blockchain in securing patients' medical records was carried out in 2019 by presenting MedBloc, a blockchain-based in securing Electronic Health Record (EHR) system that allows patients and health care providers to access and share medical health records while maintaining privacy [29]. Later in the same year, a combination of secure file transfer tools and blockchain technology was introduced as a solution for recording patient medical records to quickly and securely present all patients' medical records when a patient transferred to another hospital [30].

In 2020, an electronic medical record system based on the "hyperledger" permissioned blockchain was introduced. In the same year, blockchain technology architecture was also introduced to the Electronic Medical Record (EMR) system in Peruvian private healthcare organizations to address their EMR security and interoperability issues. Their proposed architecture was proven to provide security for their EMR and prevent changes or duplication of patient medical records [31]. Then, subsequent research in 2021 proposed a low-cost blockchain technology application model to store and view COVID-19 patient medical records in the form of patient status and detailed transaction history related to the patient's medical condition. Patients' medical records stored in the blockchain network were stored securely, could not be changed, and could only be seen by participants in the network who have access rights [4].

Blockchain technology is also implemented in their Electronic Health Record (EHR) to secure the patients' medical records from being changed, deleted, or sent to other unauthorized parties [32]. Furthermore, previous research proposes a more secure framework with blockchain technology. The proposed framework is multi-level authentication to protect the block of records among different communities of people in the cloud from phishing attacks, wallet attacks, dictionary-based attacks, and co-resistance attacks [32]. Then, recent research proposes a patient healthcare framework that provides greater security, reliability, and authentication than existing blockchain-based access controls [33]. The application of blockchain technology ensures privacy, security, and ease of accessibility of patients' medical records [34].

III. Research Method

The research proposes a new model with a combination of blockchain technology and the ECDSA algorithm in securing medical records of COVID-19 patients. This model is an improvement from the model and framework proposed by previous researchers. The proposed model consisted of two big parts. Figure 3 shows the architecture of the new model.

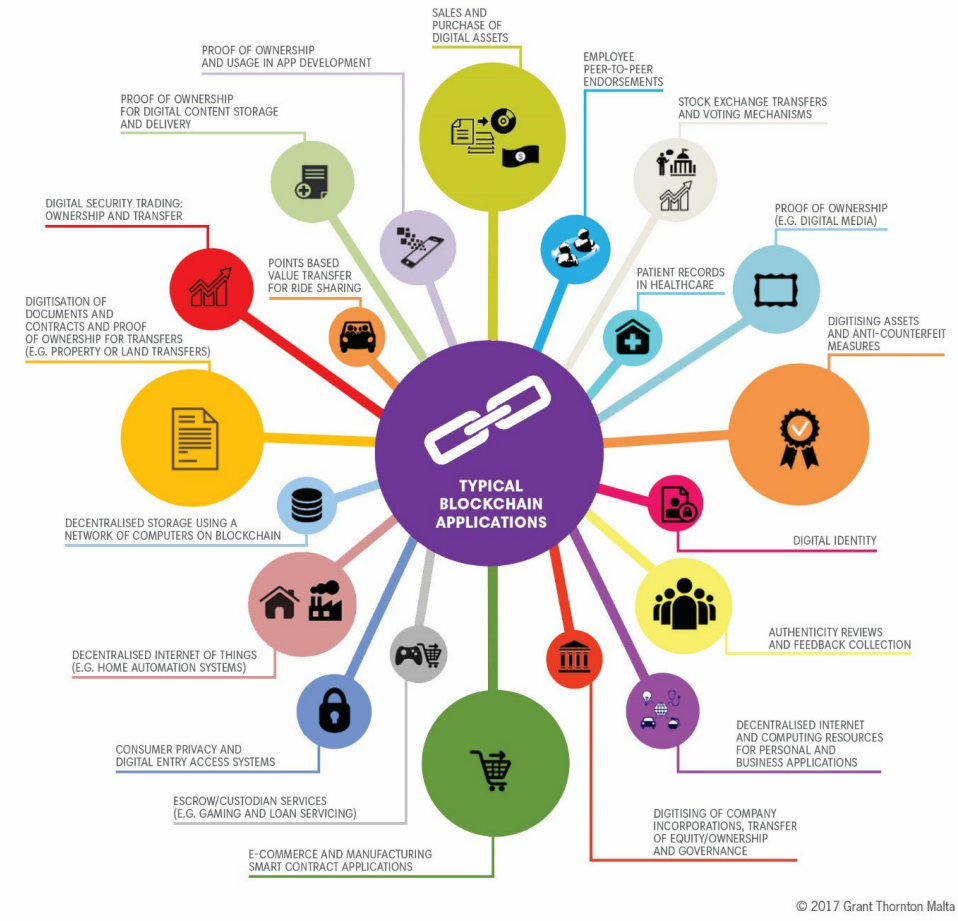

Fig. 2. The use of blockchain technology in various fields.

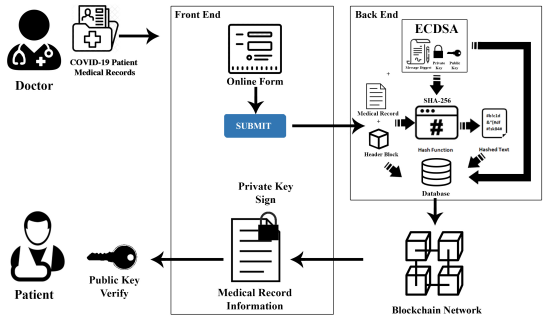

Fig. 3. The proposed model architecture in securing medical records of COVID-19 patients.

1) Front End:
In the front end, a form is provided for doctors to fill in the information on the medical records of COVID-19 patients. If the patients' medical records have been filled in, the doctor simply presses the submit button to continue the back end process. After going through the back end process, in this section, the patients are given output in the form of their medical record, which is encrypted with a private key. This information can only be unlocked using the patient's public key.
2) Back End:
In the back end, the medical record information of COVID-19 patients is protected by digital signatures using a public key and a private key. The doctor stores the private key, and the public key will be given to the patient who has the medical record. So, the information can only be opened by the patient. Participants in the blockchain network who do not have the public key cannot open the patients' medical records. After going through the encryption process with ECDSA and SHA-256, patients' medical records are stored in the blockchain network, where each block contains one patient's medical record. If a new patient's

medical record is entered, it will be added to the next block.

Then, the research performs simulations to show the proposed model in securing patient medical records. Figure 4 illustrates the simulation stages.

Based on the flowchart in Fig. 4, it can be explained step by step the stages of the simulation carried out are:

- The Input of Dataset to Blockchain Network:
  The dataset used in the research is the COVID-19 Symptoms Checkers available at Kaggle.
- ECDSA Algorithm Simulation:
  At this stage, it simulates how the ECDSA algorithm protects the patients' medical records so that they can only be opened by the patients (the owner of the public key).
- Blockchain Technology Simulation:
  At this stage, a simulation is carried out to measure the security level of blockchain technology in securing patient medical records. Tests are carried out to find the relationship between the number of blocks and difficulty targets to the security level, which is indicated by mining time if there is a change in the block. This testing process is known as Proof of Work (POW). Based on the flowchart in Fig. 5, the length of the mining process for a block is calculated. Then, the mining time is also simulated when the target difficulty is changed. The old mining calculation process does not use formula because it only counts how many milliseconds of the mining process to change the hash value so that it can be accepted on the blockchain network [35].
- Conclusion:
  Conclusions based on the simulation results that have been carried out are presented.

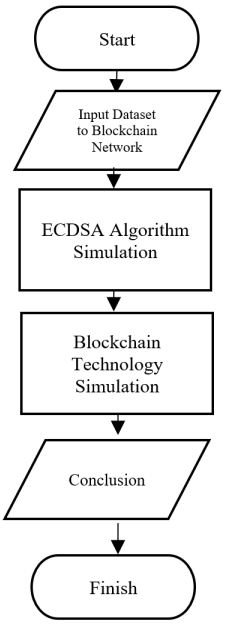

Fig. 4. Flowchart of simulation stages

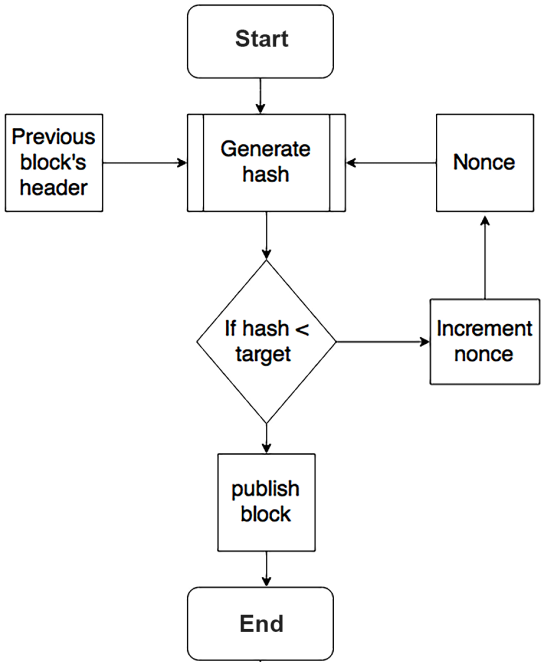

Fig. 5. Proof of Work (POW) algorithm flowchart.

IV. Results and Discussion

The researchers build a simulation website using node.js and test it with a laptop with the Intel® Core™ i5 @2.3 GHz processor specification. The number of datasets on the blockchain network is limited to 10,000 medical records of COVID-19 patients. It means there are 10,000 blocks on the blockchain network.

A. Elliptic Curve Digital Signature Algorithm (ECDSA) Algorithm Simulation

The first simulation stage presents the implementation of the ECDSA algorithm in protecting patient medical records. The researchers build an ECDSA simulation form which consists of a textbox containing a private key that has been signed with the ECDSA algorithm and a textbox to fill in the public key. Next, the empty public key textbox must be filled in with the appropriate public key to open the information on the medical record data of the COVID-19 patient to prove the simulation of the ECDSA algorithm. After the public key is filled in, the user can press the

Cite this article as: Andi, C. Juliandy, Robet, and O. Pribadi, “Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain”, CommIT Journal 16(1), 87–96, 2022.

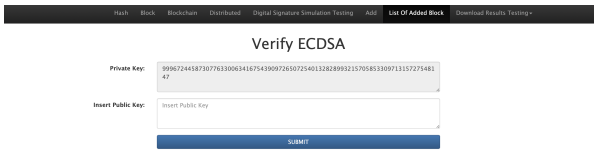

Fig. 6. Elliptic Curve Digital Signature Algorithm (ECDSA) verification simulation form.

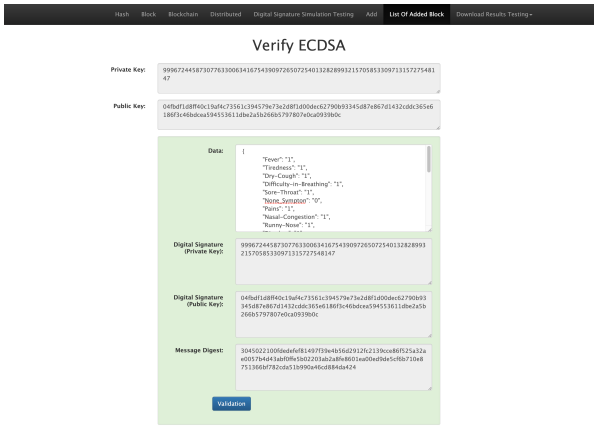

Fig. 7. Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm verification results if public key matches.

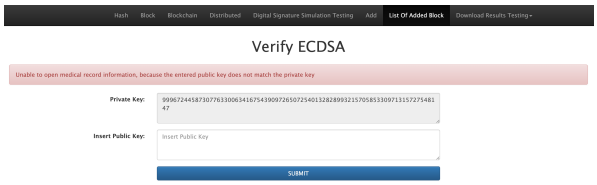

Fig. 8. Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm verification results if the public key does not match.

submit button to perform the simulation. The ECDSA simulation form can be seen in Fig. 6. Only patients or participants with a public key can read and open patient medical records. If the public key is appropriate, the patient’s medical record information appears as shown in Fig. 7.

The patients’ medical records can be opened and read if the public key is correct, as shown in Fig. 7. However, if the entered public key is incorrect, the patients’ medical records cannot be opened or read, as shown in Fig. 8. With the implementation of the ECDSA algorithm, it can guarantee that only those who have the authority can open the patient’s medical records, because the private key is only owned by the doctor and the public key is only owned by the patient. Without the pair of these two keys, it is impossible to open the patient’s medical record.

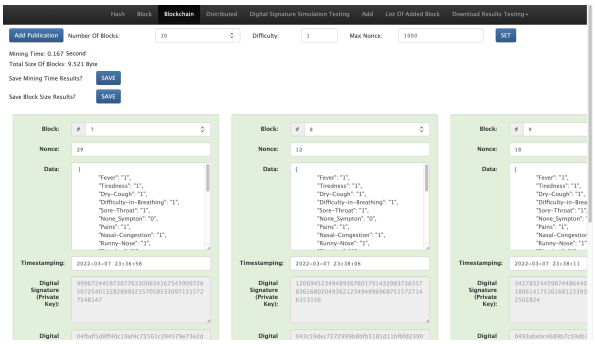

Fig. 9. Simulation application design with blockchain technology implementation.

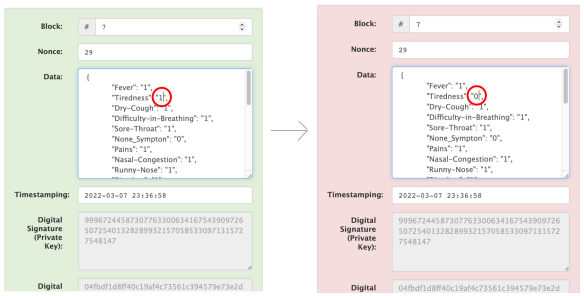

Fig. 10. Simulation of changes in medical record information on one of the blocks in the blockchain network.

B. Blockchain Technology Simulation

Furthermore, the following simulation proves the level of security of blockchain technology in securing patient medical records. So, they are not changed or manipulated. The researchers build a simulation application to show how blockchain technology works in securing medical records of COVID-19 patients. Figure 9 shows the simulation.

Figure 9 shows a collection of blocks in the blockchain network that is still safe (blocks are still green). Assume that in block number 9, there is a change by the hacker in one of the patient data attributes, the tiredness attribute, which has a value of 1, is then changed to 0. Figure 10 shows the changes.

As shown in Fig. 10, block number 7 turns red. It means that there is a change to the COVID-19 patient data in the block. It will affect other blocks in the blockchain network because the hash value of each block has changed and does not meet the requirements of the consensus POW algorithm. Figure 11 shows the effects of changing one block on other blocks in the blockchain network.

The mining process must be carried out against these blocks to make the blocks to be valid. The mining process is certainly not easy because it requires very

Cite this article as: Andi, C. Juliandy, Robet, and O. Pribadi, “Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain”, CommIT Journal 16(1), 87–96, 2022.

TABLE I
TESTING RESULTS OF MINING TIME.

Number of Blocks	Mining Time (Seconds)				
	DT=1	DT=2	DT=3	DT=4	DT=5
1	0.01	0.12	0.28	3.17	26.84
10	0.04	0.38	2.46	29.32	551.15
50	0.29	1.17	12.45	194.26	4,213.34
100	0.96	2.18	22.82	460.45	9,781.02
250	3.81	6.89	57.09	1,304.13	25,031.22
500	14.81	17.57	118.97	2,903.66	61,321.41
1,000	38.27	53.72	251.87	7,483.93	140,561.13
2,500	225.94	254.94	880.81	30,031.41	340,321.61
5,000	721.43	928.92	3,721.31	73,113.51	900,123.41
10,000	1,653.41	1,832.41	15,553.21	1,736,579.08	11,081,702.31

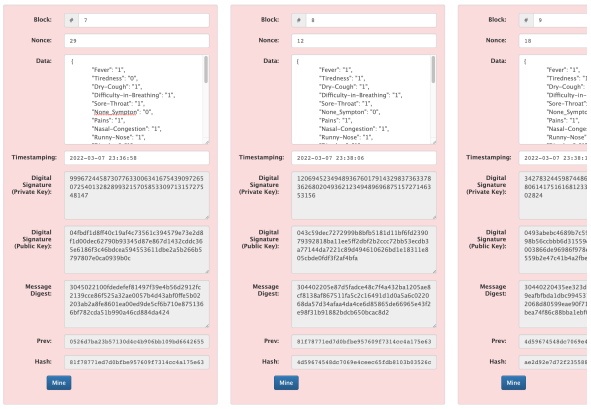

Fig. 11. The effect of changing one block on other blocks in the blockchain network.

expensive computing equipment and takes a very long time to mine. The more blocks are found on the blockchain networks, the longer time will be taken to do the mining process for the entire block. Mining time testing in the blockchain network is carried out to prove the security of the proposed model. The researchers perform tests with the several Numbers of Blocks (NB) = 1, 10, 50, 100, 250, 500, 1,000, 2,500, 5,000, and 10,000. Meanwhile, for Difficulty Targets (DT), the research uses DT = 1 to DT = 5. Each different NB and DT produces different mining times, as shown in Table I.

Table I shows that the more the number of blocks is contained in the blockchain network, the longer the mining time is required. In addition, the value of the greater difficulty target also increases the level of difficulty in changing block information on the blockchain network. Each additional difficulty target makes the mining time increase even more. This increase in time indicates that it is difficult to make slight changes to the block information recorded in the blockchain network. The test results show that the number of blocks of 10,000 with a target difficulty of 5 requires a mining time of up to 11,081,703.31 seconds.

The total datasets used in the research, namely the COVID-19 Symptoms Checkers, amount to 316,801 records (rounded to 300,000). It is impossible to make all blocks on the blockchain network valid in case of changes. If there is an action of change or manipulation in one of the blocks, the validation for the change requires a mining time of about 332,451,069.3 seconds (approximately 3,847 days). The results also show that the proposed model is very safe because the mining time required is very long.

V. CONCLUSION

Based on the research results, it can be concluded that blockchain technology is the right solution in securing patient medical records. The combination of the models is also proven. The application of the ECDSA algorithm is appropriate to protect the medical records of COVID-19 patients so that only interested parties can access them. Then, blockchain technology can prevent changes or manipulation of the medical records of COVID-19 patients. The experimental results show that it is not possible to make changes to the information on the blocks that have been recorded on the blockchain network because it takes a very long time to make all the blocks in the blockchain network valid.

The research still has limitations on the number of patient datasets used because the specifications of the research tools used are still not so high so that the number of datasets used is also not so large. Future research is expected to to perform simulations with larger datasets. In addition, it is proposed that a hospital stores medical records of COVID-19 patients to carry out an actual implementation based on the model. Then, it can see what challenges may be faced by implementing blockchain technology. In addition, future researchers can further develop the proposed model to record and secure information about the COVID-19 vaccine distribution supply chain.

Cite this article as: Andi, C. Juliandy, Robet, and O. Pribadi, "Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain", CommIT Journal 16(1), 87–96, 2022.

REFERENCES

[1] J. F. Almadani, A. P. Putera, and Yulianto, "Legal liability of doctors on the disclosure medical secrecy for COVID-19 patients in the pandemic era," *Jurnal Hukum Prasada*, vol. 8, no. 1, pp. 8–20, 2021.

[2] Worldometer, "COVID-19 coronavirus pandemic," 2022. [Online]. Available: https://www.worldometers.info/coronavirus/

[3] Suherman, "Dilemma between the disclosure of COVID-19 patients' medical records and transparency of public information according to law in Indonesia," *International Journal of Business, Economics and Law*, vol. 22, no. 1, pp. 133–139, 2020.

[4] P. Harris, "Blockchain for COVID-19 patient health record," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*. Erode, India: IEEE, April 8–10, 2021, pp. 534–538.

[5] M. Azhagiri, R. Amrita, R. Aparna, and B. Jashmitha, "Secured electronic health record management system," in *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*. Coimbatore, India: IEEE, Oct. 15–16, 2018, pp. 915–919.

[6] D. B. Santoso, A. Fuad, G. B. Herwanto, and A. W. Maula, "Blockchain technology implementation on medical records data management: A review of recent studies," *Jurnal Riset Kesehatan*, vol. 9, no. 2, pp. 107–112, 2020.

[7] W. K. Yang, J. S. Chen, and Y. S. Chen, "An electronic medical record management system based on smart contracts," in *2019 Twelfth International Conference on Ubi-Media Computing (Ubi-Media)*. Bali, Indonesia: IEEE, Aug. 5–8, 2019, pp. 220–223.

[8] V. Shukla, A. Mishra, and A. Yadav, "An authenticated and secure electronic health record system," in *2019 IEEE Conference on Information and Communication Technology*. Allahabad, India: IEEE, Dec. 6–8, 2019, pp. 1–5.

[9] Andi, R. Purba, and R. Yunis, "Application of blockchain technology to prevent the potential of plagiarism in scientific publication," in *2019 Fourth International Conference on Informatics and Computing (ICIC)*. Semarang, Indonesia: IEEE, Oct. 16–17, 2019, pp. 1–5.

[10] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, pp. 1–22, 2018.

[11] Andi, C. Juliandy, Robet, O. Pribadi, and R. Wijaya, "Image authentication application with blockchain to prevent and detect image plagiarism," in *2021 Sixth International Conference on Informatics and Computing (ICIC)*. Jakarta, Indonesia: IEEE, Nov. 3–4, 2021, pp. 1–6.

[12] D. D. Taralunga and B. C. Florea, "A blockchain-enabled framework for mhealth systems," *Sensors*, vol. 21, no. 8, pp. 1–24, 2021.

[13] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere, and F. Antonelli, "A decentralized peer-to-peer remote health monitoring system," *Sensors*, vol. 20, no. 6, pp. 1–18, 2020.

[14] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, 2021.

[15] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and IPFS: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, pp. 1–16, 2021.

[16] T. F. Lee, I. P. Chang, and T. S. Kung, "Blockchain-based healthcare information preservation using extended chaotic maps for HIPAA privacy/security regulations," *Applied Sciences*, vol. 11, no. 22, pp. 1–16, 2021.

[17] C. Juliandy, R. Purba, R. Yunis, and Darwin, "Modeling of image copyright protection using discrete cosine transform hash and blockchain," in *Proceedings of the International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies - CESIT*, INSTICC. Medan, Indonesia: SciTePress, Sept. 16–18, 2020, pp. 128–134.

[18] X. Wang, "Research on ECDSA-based signature algorithm in blockchain," *Finance and Market*, vol. 4, no. 2, pp. 55–58, 2019.

[19] D. Toradmalle, R. Singh, H. Shastri, N. Naik, and V. Panchidi, "Prominence of ECDSA over RSA digital signature algorithm," in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. Palladam, India: IEEE, Aug. 30–31, 2018, pp. 253–257.

[20] Y. Genç and E. Afacan, "Design and implementation of an efficient Elliptic Curve Digital Signature Algorithm (ECDSA)," in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. Toronto, ON, Canada: IEEE, April 21–24, 2021, pp. 1–6.

[21] A. Saepulrohman and A. Ismangil, "Data integrity and security of digital signatures on electronic systems using the Digital Signature Algo-

rithm (DSA)," *International Journal of Electronics and Communications Systems*, vol. 1, no. 1, pp. 11–15, 2021.

[22] R. Kasodhan and N. Gupta, "A new approach of digital signature verification based on BioGamal algorithm," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*. Erode, India: IEEE, March 27–29, 2019, pp. 10–15.

[23] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and secure ECDSA algorithm and its applications: A survey," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 11, no. 1, pp. 7–35, 2019.

[24] P. Sangeetha, "Preventing fake page from Blackhat's in mobile web browsers using enhanced ECDSA algorithm," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 4, pp. 5066–5071, 2019.

[25] C. S. Wright, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://ssrn.com/abstract=3440802

[26] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20 698–20 707, 2019.

[27] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24 477–24 488, 2019.

[28] A. G. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz, and T. M. Alam, "A journey of web and blockchain towards the Industry 4.0: An overview," in *2019 International Conference on Innovative Computing (ICIC)*. Lahore, Pakistan: IEEE, Nov. 1–2, 2019, pp. 1–7.

[29] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. C. Tu, "Medbloc: a blockchain-based secure ehr system for sharing and accessing medical data," in *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. Rotorua, New Zealand: IEEE, Aug. 5–8, 2019, pp. 594–601.

[30] S. Hasavari and Y. T. Song, "A secure and scalable data source for emergency medical care using blockchain technology," in *2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA)*. Honolulu, HI, USA: IEEE, May 29–31, 2019, pp. 71–75.

[31] A. Martínez, C. Molina, and D. Subauste, "Electronic medical records management in health organizations using a technology architecture based on blockchain," in *2020 IEEE ANDESCON*. Quito, Ecuador: IEEE, Oct. 13–16, 2020, pp. 1–6.

[32] B. Vardhini, S. N. Dass, R. Sahana, and R. Chinnaiyan, "A blockchain based electronic medical health records framework using smart contracts," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*. Coimbatore, India: IEEE, Jan. 27–29, 2021, pp. 1–4.

[33] A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud, J. Ali, and M. Baz, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, pp. 1–27, 2021.

[34] M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," *Procedia Computer Science*, vol. 174, pp. 321–327, 2020.

[35] S. Ghimire and H. Selvaraj, "A survey on bitcoin cryptocurrency and its mining," in *2018 26th International Conference on Systems Engineering (ICSEng)*. Sydney, NSW, Australia: IEEE, Dec. 18–20, 2018, pp. 1–6.