**IJCCS (Indonesian Journal of Computing and Cybernetics Systems)**
Vol.18, No.4, October 2024, pp. 429~440
ISSN (print): 1978-1520, ISSN (online): 2460-7258
DOI: https://doi.org/10.22146/ijccs.100953


# Feasibility Study of Using Blockchain Technology for Criminal Records in Central Java

**Puspa Ira Dewi Candra Wulan*[1], Rofiq Fauzi[2], Danis Putra Perdana[3] , Muhamad Eko Alfianto[4], Clarissa Monique Maharani[5], Yudha Satria Abdi Susila[6]**
[1,2,3,4,5,6]Cyber Security; Politeknik Bhakti Semesta, Salatiga, Indonesia
e-mail: ***[1]puspa@bhaktisemesta.ac.id** , [2]Rf@bhaktisemesta.ac.id , [3]danis@bhaktisemesta.ac.id , [3] clarissamonique02@gmail.com, [3] ekoalfianto19@gmail.com, [3] ysatria212@gmail.com

***Abstrak***

*Catatan kriminal merupakan dokumen resmi yang diarsipkan di kepolisian yang berisi riwayat kriminal masyarakat.Terdapat tantangan kompleks dalam pengolahan data catatan kriminal yaitu risiko manipulasi data. Salah satu tujuan manipulasi data yaitu perubahan catatan kriminal untuk kebutuhan tertentu. Meningkatnya kejahatan cyber di Indonesia tidak menutup kemungkinan bahwa peretasan data akan terjadi pada data catatan kriminal. Teknologi Blockchain melalui smart contract, merupakan solusi inovatif untuk mengatasi permasalahan manipulasi data. Blockchain sebagai buku besar digital terdistribusi yang tidak dapat diubah, memberikan jaminan keamanan dan integritas data. Dengan mengadopsi smart contract dalam pendataan catatan kriminal, dapat meningkatkan kecepatan akses informasi, mengurangi risiko manipulasi dan memberikan tingkat transparansi yang tinggi. Feasiblility study atau studi kelayakan tentang pentingnya penerapan teknologi Blockchain untuk penyimpanan catatan kriminal perlu dilakukan sebelum memutuskan untuk merealisasikan teknologi blockchain. Tujuan dalam penelitian ini yaitu untuk menganalisis seberapa penting data catatan kriminal harus diamankan menggunakan teknologi Blockchain di Jawa Tengah. Metode kualitatif digunakan dalam penelitian ini, pengumpulan data dilakukan dengan teknik wawancara kepada narasumber yang sudah ditentukan. Hasil dari penelitian ini menunjukan bahwa teknologi blockchain relevan sebagai solusi untuk melindungi data catatan kriminal, namun diperlukan persiapan Sumber Daya Manusia yang memahami implementasi teknologi ini sebelum blockchain digunakan untuk penyimpanan catatan kriminal di Jawa Tengah.*

***Kata kunci****— Blockchain; Catatan kriminal; Kejahatan Siber; Smart contract; Keamanan Data*

***Abstract***

*Criminal records are official documents archived by the police that contain people's criminal history. There are complex challenges in processing criminal record data, namely the risk of data manipulation. One of the purposes of data manipulation is to change criminal records for certain needs. The increase in cybercrime in Indonesia does not rule out the possibility that data hacking will occur in criminal record data. Blockchain technology, through smart contracts, is an innovative solution to overcome the problem of data manipulation. Blockchain as an immutable distributed digital ledger, provides guarantees of data security and integrity. Adopting smart contracts in criminal record data collection, can increase the speed of access to information, reduce the risk of manipulation, and provide a high level of transparency. A feasibility study regarding the importance of implementing Blockchain technology for storing criminal records must be conducted before deciding to realize blockchain technology. This research aims to analyze how important it is that criminal record data must be secured using Blockchain technology in Central Java. Qualitative methods were*

*Received October 23th,2024; Revised October 29th, 2024; Accepted October 31th, 2024*

*used in this research, data collection was carried out using interview techniques with predetermined sources. The results of this research show that blockchain technology is relevant as a solution for protecting criminal record data, but it requires the preparation of Human Resources who understand the implementation of this technology before blockchain is used for storing criminal records in Central Java.*

***Keywords—*** *Blockchain; Criminal record; Cyber Crime; Smart contracts; Data Security*

## 1. INTRODUCTION

The police is one of the government institutions that plays the role of maintaining security and public order [1]**.** The police is one of the functions of the state government in the field of maintaining security and public order, law enforcement, protection, protection, and service to the community [2]. The police manage data related to roles and functions, one of which is criminal registration data. Criminal record data collection is a vital component of the legal system, including in Indonesia.

Criminal records are official documents filed by the police that contain the criminal history of the community. Criminal records contain data on the criminal history of a person who commits a criminal act, not only when a guilty verdict is imposed by the court, but criminal records start from arrest even if the complaint is withdrawn, the prosecution is delayed, or the verdict is handed down [3]**.** In practice, it is not easy to manage criminal record data, a complex challenge that must be realized is the risk of data manipulation. Data manipulation is carried out for various purposes, one of which is the deletion or change of criminal records for certain needs. *Cybercrime* has experienced a significant increase, Cybercrime *is a* crime against network systems that use computer facilities [4]. Data from the E-MP Robinopsnal Bareskrim of the National Police shows that the police cracked down on 8,831 cases of cybercrime from January 1 to December 22, 2022 [5]. The increase in *cybercrime* in Indonesia does not rule out the possibility that *cybercrime* will occur in police data, one of which is criminal records in Central Java.

Central Java experienced an increase in the number of crime cases by 2.6 percent in 2023 with a total of 277 crime cases based on data from the Central Java Police Directorate of Criminal Investigation in 2024. The increase in cases that occur automatically increases the amount of criminal record data owned by the police.

Significant challenges related to data security, privacy, and interoperability of police records are matters that require consideration of how they are stored. Centralized storage makes it difficult to adequately address these challenges, giving rise to growing concerns about data breaches and misuse.

*Blockchain* technology through *smart contracts*, is an innovative solution to overcome the problem of data manipulation in police records in Indonesia. *Blockchain* as an immutable distributed digital ledger, providing guarantees of data security and integrity, is known as the fifth evolution, namely the development of computers that have data structures that can make offline books digital [6], By adopting *smart contracts* in the collection of criminal records, it can increase the speed of information access, reduce the risk of manipulation and provide a high level of transparency. *Smart contracts* will use cryptographic methods to protect data from the risk of data manipulation [7]**.**

The benefits that blockchain technology offers in terms of security, transparency, and decentralization are strong reasons why this technology is an innovative solution [8]**.** Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes, this reduces the risk of failure and empowers users by eliminating the need for third-party intermediaries, Cryptographic algorithms are used to secure transactions in blockchain technology, making it very difficult to change records. Once data is added to the blockchain, it

cannot be easily changed or tampered with, providing a high level of security against possible fraud and hacking. Every transaction in the blockchain is recorded on a public ledger, which is visible to all participants in the network. This transparency helps increase trust, making blockchain ideal for industries that prioritize transparency including the police in Central Java.

*A feasibility study* on the importance of applying *Blockchain* technology for criminal record keeping must be done before deciding to realize the technology. *The Feasibility Study* is carried out to facilitate planning, and implementation, minimize risks, and facilitate the supervision and control process.

Forum Group Discussion was carried out as a problem-solving approach in this research. The security of criminal records is related to 2 parties, namely law enforcement and hackers. The step taken after preparation and identification of needs was data collection by conducting a Forum Group Discussion with law enforcers in Central Java regarding records. Criminals including the Central Java Regional Police's Ditreskrimsus and the Central Java Province High Prosecutor's Office. The second discussion was held with the hacker community in Central Java to obtain relevant data related to the application of this technology. Triangulation is used to analyze Forum Group Discussion data so that relevant conclusions can be drawn.

Research on the importance of securing criminal record data and the use of *Blockchain* in criminal record data processing has never been conducted. Related research on police data was conducted by Eky Saputra in 2019 with the title "SKCK security information system using barcodes at the Riau Police Intelligence Directorate" The result of the research is that the system built can provide security for SKCK data and it easier for admins in the process of making SKCK [9], Research related to police data was also carried out by eka chandra in 2021 with the title "SIPEKA (SKCK Service Information System) at the Kotabaru Police Station, Karawang Regency" in the research a system was designed to facilitate the work of the Kotabaru Police in serving the Community in making SKCK as well as facilitating the processing of data on people who are involved or not involved in criminal activities [10]**.** The third research related to police data was conducted by Galih Ashari in 2020 with the title "Kajas Application as a Web-based Crime Report Management Information System" The study produced a prototype of the Kajas admin side application operated by the police to receive and make crime reports [11], from the three studies, it is known that the research was carried out to build an information system to facilitate police performance so that the research is not a research that contains how to secure police record data.

The results of research on this feasibility study will later contribute as a basis for implementing blockchain technology to store criminal records in Central Java. With the results of this feasibility study, it is known how important this technology can be applied. By implementing this technology, it is hoped that jurisdictions can improve data integrity, enable cross-institutional collaboration, and build public trust in the handling of criminal record data in Central Java.

## 2. METHODS

The conceptual model was prepared after reviewing the literature on the issues raised. The purpose of preparing a conceptual model is so that the research carried out can focus on the problems of the research object. The conceptual model developed in this research is depicted in Figure 1.

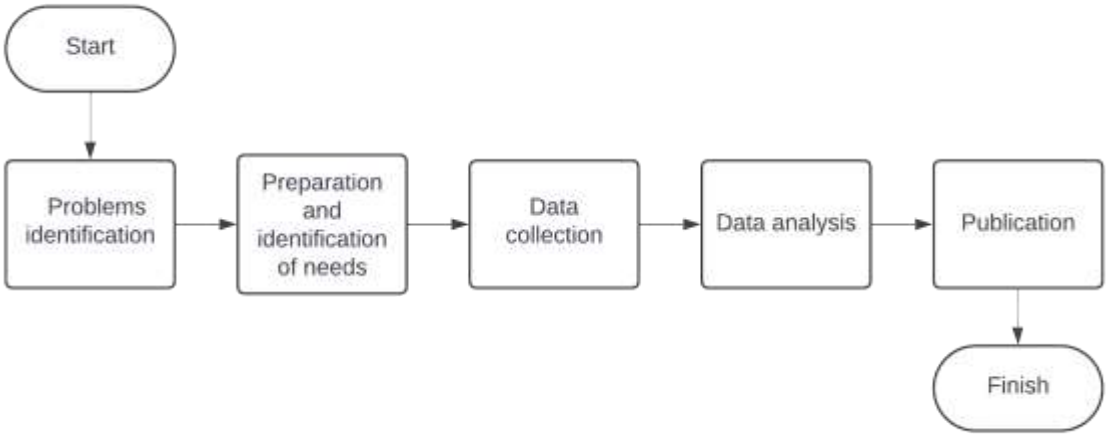


Figure 1 Conceptual Model

Problem identification is based on the results of pre-research, literature review, previous research, and interviews. After the process is complete, preparation and identification of needs are carried out. The results of problem identification become material for consideration in making instruments and determining research samples. The third stage in this research is data collection. The data was carried out by conducting focus group discussions to explore information and the essence of the answers, then data analysis was carried out to discuss the data findings and collect the essence by triangulating the data from the interview answers, the last was the research publication.

*2.1 Blockchain Technology*

*Blockchain* is a distributed *ledger* technology that cannot be traced and offers opportunities for digital certification and information exchange through computer networks [12]**.** *Blockchain* as an immutable distributed digital ledger, providing a guarantee of data security and integrity, is known as the fifth evolution, namely the development of computers that have data structures that can make offline books digital [6].

The popularity of *Blockchain* technology has been widely used in various aspects of life in various fields and industries, *Blockchain* is also an innovation that is growing in data security systems according to the times. This technology is used as an effective tool in performance development because the data storage is in a *cloud* system. Intervention by any third party is easily blocked by the presence of advanced algorithms in this technology.

*Blockchain* is divided into three parts, including public *Blockchain* which is a technology with wide distribution and native tokens used in the *Blockchain* process, *Blockchain* primitive which is a condition for developing a system by the integrity of *the blockchain* technology and *Private Blockchain* which is a technology that does not require a native token but hasa small use and is a favorite use for consortium participants [6].

*2. 2 Smart Contract*

*Smart contracts* are programs stored in the *Blockchain* system that run automatically when conditions are determined previously fulfilled. *Smart contracts* carry out *if-then* checks so that transactions can be completed [13]**.**

*Smart contracts* are contracts created to facilitate agreements between multiple *nodes* based on the type of consensus algorithm. The contract is in the form of a *source code* that uses *the solidity* language. *Smart contracts* can define rules and generate code to be applied to

the *Blockchain* network. *Smart contracts* cannot be deleted by default, and interactions with *smart contracts* cannot be eliminated.

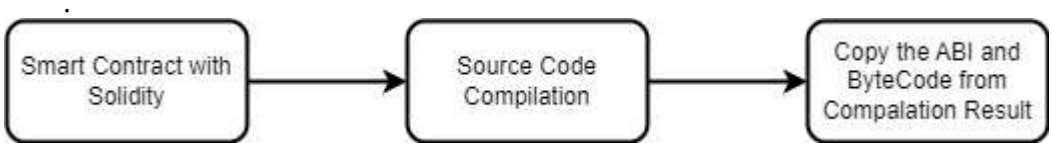


Figure 2 Smart Contract Workflow

*Solidity* is a programming language that is almost the same as C++, *solidity* has a .sol file extension. *Solidity* is object-oriented programming that is used to design *smart contracts* on *Blockchain* technology so that they can run on *Ethereum virtual machines*. Compilation is done to generate *bytecode* that is used for function reference and contracts to be executed on *the Ethereum virtual machine* [13].

*2. 3 Triangulation*

Triangulation in qualitative methods is used to find more perspectives related to the data found [1].

Triangulation has three model systems, including Theoretical Triangulation which is a method used to compare information from different theoretical perspectives, Data Source Triangulation which is a method used to validate data from various sources and Triangulation. A method that is a method used to check the completeness of data and ensure that the data obtained *is valid*, such as interviews, *surveys*, or *observations*.

In this study, the triangulation method of data sources is used, using various data sources to ensure the consistency of findings and increase the validity of the analysis results. The application of Triangulation in qualitative methods is used to find more perspectives related to the data that was found [6]. Figure 2 is the research flow using the theoretical triangulation method.

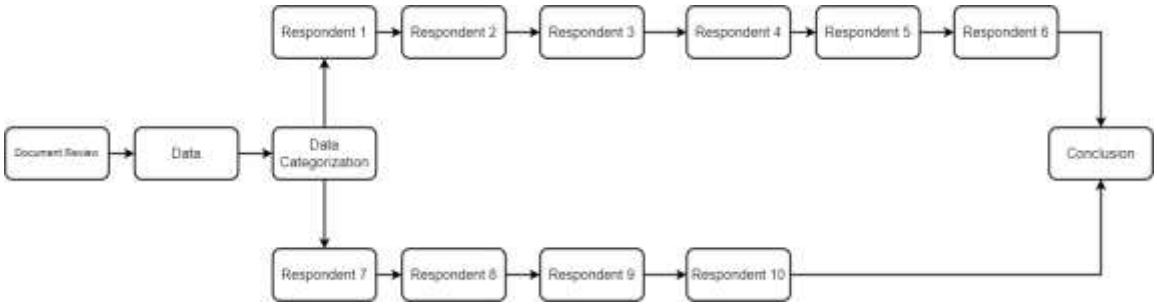


Figure 3. Triangulation Research Flow

In the figure above, it is explained that the research begins with the study of documents, collecting documents that will be used as a reference in data collection, data categorization is carried out to distinguish the instruments prepared, by the side of law enforcement and the side of users or actors. Data collection was carried out by interview techniques with 10 sources which were divided into 6 sources from the law enforcement side and 4 sources from the *hacker* community side. Conclusions were drawn by coding each question and answer from the results of data collection.

The triangulation method of data sources in criminal records research helps strengthen the reliability of data through inter-source verification, the use of multiple sources of information or perspectives to confirm and strengthen research findings, and data from various sources can provide a more comprehensive picture to reduce bias and provide a more comprehensive view. Comprehensive. In addition, triangulation of data sources strengthens the validity of the data which influences the validity of research findings. The use of coding techniques helps analyze data from various sources systematically, to find consistent and in-depth themes that support the validity of the research. The combination of triangulation and coding creates research results that are more reliable, accurate, and able to make a significant contribution to this research.

*2.4 Population and Sample*

The target population in this research is the Ditreskrimsus Polda Central Java, the Prosecutor's Office Central Java, and the Hacker Community in Central Java.

The Special Criminal Investigation Directorate (Ditreskrimsus) has an important role in storing and managing criminal records, especially those related to special crimes such as economic crimes, corruption, and cyber. Responsible for ensuring criminal record data maintained is accurate and unbiased. Ditreskrimsus Polda has high credibility in collecting, storing, and disseminating criminal record data, ensuring the data management process can be audited by other authorities to prevent misuse or manipulation of data, Ditreskrimsus implements security procedures, including data encryption and access restrictions by meeting the criteria above, Ditreskrimsus Polda was chosen as the source for this research.

The Prosecutor's Office (Kejati) has an important role in the law enforcement process, especially in the process of prosecuting and managing criminal data, the Prosecutor's Office maintains accountability in managing criminal data, ensures that the data stored is accessed by the authorities by regulations, the Prosecutor's Office provides criminal data and is responsible for ensuring that The data stored has high integrity, is free from manipulation, and reflects the actual legal situation, based on these criteria, the High Prosecutor's Office is one of the sources in the research.

The third resource person is a hacker in the Central Java province. Hackers with the right skills and a good reputation can offer valuable insight into system security and potential loopholes in the implementation of blockchain for criminal record keeping in Central Java.

## 3. RESULTS AND DISCUSSION

*3.1 Research Resource Persons*

There are three groups of resource persons as data sources in this study, the resource persons are divided into 2 aspects related to criminal records and 1 aspect of users or communities that are closely related to *Blockchain* security.

The first resource person from the police, the Police is one of the government institutions that plays a role in maintaining public security and order [13]. The police is one of the functions of the state government in the field of maintaining security and public order, law enforcement, protection, protection, and service to the community [2]. The police manage data related to roles and functions, one of which is criminal registration data. Criminal record data collection is a vital component of the legal system, including in Indonesia.

Resource person 2 came from members of the district high prosecutor's office, the district high prosecutor's office is very close to criminal records, and the high prosecutor's office has the task of collecting data and information, receiving reports, processing, and analyzing information obtained by themselves as well as reports from the police.

The third resource person is the *cyber* security community, where this community is a community that can work from the security side and can also work from the hacker side. The *cyber* security community is a community that carries out its activities using the

internet world [14]**.** It can be seen in Table 1 which is the complete data of the sources in this study.

Table 1 Data Source

| No | Narasumber | Asal |
|---|---|---|
| 1 | Kanit 1 Unit IV Sub-Directorate 5 Cyber Directorate of the Central Java Police AKP Endro Prabowo and his staff | Jl. Sukun Raya No.46, Srondol Wetan, Banyumanik District, Semarang City, Central Java 50263 |
| 2 | Assistant for the Development of the Central Java High Prosecutor's Office, the Chief Prosecutor Pratama Sugiyanta, S.H., M.H., and staff. | Jl. Pahlawan No.14, Pleburan, Kec. Semarang Sel., Semarang City, Central Java 50241 |
| 3 | *Cyber* Security Expert Tri Febrianto and community members. | Jl. Turus Asri IV No.6, Bulusan, Tembalang District, Semarang City, Central Java 50277 |

Table 1 synthesizes insights from the Central Java Police, the High Prosecutor's Office, and cybersecurity experts to evaluate blockchain's feasibility for managing criminal records. Law enforcement officials underscore the need for secure, immutable records to prevent manipulation, highlighting vulnerabilities in current centralized systems. Complementing this, cybersecurity experts affirm blockchain's resilience against tampering while addressing technical hurdles, such as resource demands and required expertise for implementation [7]. This triangulated approach validates blockchain's potential as a robust solution, provided that necessary adaptations in infrastructure and specialized knowledge are in place, thus supporting the study's conclusion that blockchain can enhance the security and integrity of criminal record management in Central Java.

*4.2 Research Instruments*

There are 2 research instruments for the data collection process in this study, the first instrument is used for data collection on the side related to criminal records. The research instrument is seen in Table 2.

Table 2 Research Instrument 1

| No | Questionnaire |
|---|---|
| 1 | Does the Agency keep criminal record data? |
| 2 | Where is criminal record data stored? |
| 3 | How important is a criminal record? |
| 4 | Is there a system in place to secure records criminal? |
| 5 | Are there any possible vulnerabilities? |
| 6 | What happens if a criminal record can be manipulated or deleted? |
| 7 | Is Blockchain technology needed for criminal record keeping? |
| 8 | Are there any regulations that will collide with the use of Blockchain technology? |

Table 2 functions as a targeted instrument for gathering data from law enforcement officials, structured to assess both their current practices in criminal record security and their perspectives on blockchain as a viable solution. Questions in this table focus on operational aspects, such as existing security protocols, identified vulnerabilities, and potential regulatory barriers to adopting blockchain. This data mining approach is critical as it captures insights into the institutional requirements and limitations within the criminal justice system, laying the groundwork for understanding how blockchain could enhance security, streamline access, and address specific weaknesses in record management practices.

The research instrument is adjusted to the resource person used in the research, the third resource person is the *cyber security* community, where this community is a community that can work from the security side and can also work from the hacker side. The *cyber security* community is a community that carries out its activities using the internet world. Table 3 is the second research instrument in this study.

Table 3 Research Instrument 2

| No | Questionnaire |
|---|---|
| 1 | Do you think *Blockchain* technology can improve the security of criminal records compared to traditional systems? |
| 2 | What are the potential drawbacks of using *Blockchain* in criminal record management, especially from a security perspective? |
| 3 | As a hacker, to what extent does *Blockchain* make criminal records more difficult to access or manipulate? |
| 4 | Can you explain how the characteristics of *Blockchain* play a role in protecting the integrity of criminal record data? |
| 5 | Do you see any exploitable loopholes in *Blockchain* implementations for criminal records, and how will you try to exploit them? |
| 6 | Do you think the encryption and hashing on *the Blockchain* are strong enough to protect sensitive data in criminal records from cyber threats? |
| 7 | In a scenario where criminal records are managed with *Blockchain*, do you think there are any new hacking techniques or tools that need to be developed to penetrate those systems? |
| 8 | What do you think about the possibility of unauthorized third parties accessing criminal records stored on the *Blockchain*, given the transparent nature of this technology? |

Table 3 is used to obtain expert input from the cybersecurity community, specifically regarding the technical feasibility and security implications of implementing blockchain for criminal record storage. Questions in this table probe into blockchain's resilience against manipulation, the adequacy of its cryptographic measures, and any possible technical vulnerabilities. By focusing on an expert analysis of blockchain's security capabilities and potential risks, Table 3 will provide valuable insights that can confirm the technical soundness of blockchain while identifying challenges that may need to be addressed in deployment. Together, these instruments ensure a balanced exploration of blockchain's feasibility, integrating both operational and technical evaluations.

*4.3 Data Codification*

Coding was carried out on the interview instrument to make it easier to conclude this study. Table 4 is the codification in his study.

Table 4 Data Codification

| No | Questionnaire | Description |
|---|---|---|
| BC1 | Criminal Record Keeping | Views on the importance of criminal record retention and how criminal records are stored in Police Agencies and District Attorneys in Indonesia |
| BC2 | Knowledge of Blockchain Usage | User's views and knowledge about *Blockchain* Technology in criminal record keeping |
| BC3 | Challenges and Implementation | Technical challenges, operational challenges, challenges in the availability and readiness of human resources, or regulations faced in implementing *blockchain* technology |
| BC4 | Benefits of Blockchain Implementation | Potential long-term benefits of *blockchain* adoption |
| BC5 | Data Security | Systems and properties of blockchain technology for data storage and security |

The data is coded according to the theme of concluding, 5 codes are initialized with codes BC 1 to BC 5 with the main theme of criminal record-keeping, Blockchain usage views, Challenges and Implementation, Benefits of blockchain implementation, and data security.

*3.4 Thematization*

After the data codification process, data is emphasized based on the data codification that has been carried out previously, table 5 is the research thematicization.

Table 5 Data Optimization

| No | Questionnaire | Description |
|---|---|---|
| BC1 | Criminal Record Keeping | • String using the app<br>• Verify using email authentication<br>• Placement of servers in one building |
| BC2 | Knowledge of Blockchain Usage | • Blockchain has the right capabilities to secure important data<br>• Blockchain is needed to secure sensitive data |
| BC3 | Challenges and Implementation | • It does not have adequate facilities and infrastructure<br>• Lack of availability of human resources<br>• Lack of knowledge about data security<br>• Regulations that collide with the techniques and nature of blockchain |
| BC4 | Benefits of Blockchain Implementation | • Difficult to access by just anyone<br>• Better security |
| BC5 | Data Security | • Decentralized server location<br>• Chain-like and interconnected data storage patterns<br>• Easy tracking of data changes |

Thematization is used to identify the main themes and sub-themes based on data coding, this serves to make it easier when collecting data so that the questions presented are by the themes and codes that have been prepared, and conclusions are drawn based on the themes and codes that have been prepared.

3.5 *Thematic Analysis*

The storage of criminal records carried out through the application allows for efficiency in data management. This application can be designed to manage, access, and process criminal records more quickly and accurately. However, the use of applications in criminal data storage also requires strict supervision in terms of security, especially since this data is very sensitive and important. The application storage system must be equipped with various layers of encryption to prevent unauthorized access. In addition, the existence of features such as automatic backups and disaster recovery plans is very important to ensure that this data remains safe in various situations. However, the use of applications in general is very easy to hack, so data theft is very likely to occur.

Using email authentication to verify access to criminal records represents a concern for data access security. However, email authentication systems alone may not be enough to protect sensitive data. This system is vulnerable to phishing or email hacking threats. Therefore, other better security methods such as blockchain are needed. This will ensure that only truly authorized individuals can access criminal records.

Storing servers that manage criminal records in one physical location can be a major risk in terms of physical security and data availability. If a natural disaster, fire, or other security incident damages the facility, all data could be at risk of being lost or damaged. This is one of the disadvantages of infrastructure centralization. This is the function of blockchain, where the server is decentralized so that its location is not limited to one server in one building.

Taking these aspects into account, it is clear that although current technologies and systems offer basic efficiency and security, there is still a need for improvements and strengthening of security and storage models to ensure that criminal records are protected from a variety of threats, both digital and physical.

Blockchain is known for its ability to be very suitable for securing important data. This is due to the blockchain architecture being decentralized and resistant to data changes without the consent of the entire network. This technology is very effective in protecting data from manipulation and attacks, especially for data that must remain safe and intact, such as criminal records.

Data stored in blockchain is broken down into interconnected blocks and encrypted with strong cryptographic algorithms. Each block contains information from the previous block, creating a chain that cannot be changed without affecting the entire chain. Additionally, any changes that occur in the blockchain can be easily tracked and verified by all parties participating in the network. This transparency makes it more difficult for parties with bad intentions to commit fraud or change data without being detected. This characteristic of transparency and integrity is very relevant when it comes to storing important data because maintaining the integrity and correctness of data is a top priority.

One of the main advantages of blockchain in securing sensitive data is its ability to eliminate the need for vulnerable third parties to become security weak points. In traditional systems, data is often processed and stored by a central server that can be the target of attacks. However, with blockchain, data is spread across the network so that no single entity has complete control over the data. This makes data more difficult to access by unauthorized parties and better protected from cyberattacks, including hacking, data leaks, and unauthorized access.

No weaknesses were found in blockchain technology from a technical perspective, however, with a lack of understanding about digital security, especially the use of blockchain, users can

exploit it by irresponsible people to create loopholes in taking over data stored on the blockchain.

Overall, blockchain provides a solid solution for securing important and sensitive data and is able to overcome many of the weaknesses that exist in traditional storage systems. Its change-resistant, transparent, and decentralized nature provides a guarantee that data will remain safe, intact, and protected from growing threats in the digital world.

## 4. CONCLUSIONS

Blockchain technology offers a powerful solution for securing important and sensitive data, especially in the context of criminal record keeping. Its decentralized architecture and strong encryption make the blockchain resistant to manipulation and attacks, ensuring that data remains safe and intact. However, the main challenge is not the technical aspect, but rather the lack of human resources who have a deep understanding of this technology. Blockchain implementation can also help overcome weaknesses in traditional systems such as weak authentication and server centralization, which can increase security risks. Therefore, blockchain is becoming increasingly relevant as a solution to protect sensitive data in this digital era, offering greater security, transparency, and integrity.

The feedback gathered from the police, prosecutors, and cybersecurity experts reflects a strong consensus on blockchain's potential to enhance security for criminal records. Police respondents emphasized blockchain’s immutability, viewing it as a crucial asset for preventing unauthorized data alterations, which are prevalent risks in centralized systems. Prosecutors highlighted the transparency and traceability benefits of blockchain, noting that these features could support effective audits and reduce the risk of illegal processes. The cybersecurity community, with a practical understanding of security vulnerabilities, affirmed blockchain’s resilience to cyber-attacks due to its cryptographic structure and decentralized design, which reduces single points of failure.

To support sustainable adoption, we recommend targeted training for staff, phased integration with current systems, regular security assessments, and standardized policies across institutions. These steps will ensure a smooth transition and maintain data integrity in criminal record management.

## REFERENCES

[1] R. I. Afriani, N. Handayani, T. Apriani, M. Husni, and U. Bina Bangsa, “Volume 4 Nomor 1 Tahun 2023”, doi: 10.46306/rev.v4i1.

[2] P. Kedudukan Dan Kewenangan Kepolisian Perbandingan Kedudukan Dan Kewenangan Kepolisian, F. Eden Surbakti, A. Abdilah, F. Eden, and P. Kedudukan Dan Kewenangan, “PERBANDINGAN KEDUDUKAN DAN KEWENANGAN KEPOLISIAN DALAM KONSTITUSI YANG PERNAH BERLAKU DI INDONESIA,” *J. Huk. Pembang.*, vol. 51, no. 1, p. 9, doi: 10.21143/jhp.vol51.no1.3012.

[3] N. K. Sa’diyah and U. Enggarsasi, “Social Structure as the Root of Improving Criminality in the Era of Pandemic Covid-19,” *Int. J. Criminol. Sociol.*, vol. 10, pp. 1202–1211, Jul. 2021, doi: 10.6000/1929-4409.2021.10.140.

[4] M. A. Aldriano and M. A. Priyambodo, “CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA,” *J. Kewarganegaraan*, vol. 6, no. 1, 2022.

[5] S. Jaya Lesmana and I. Sofia Latif, “Law Enforcement in Efforts to Combat Cyber Crime in Indonesia: Building Future Digital Security.”

[6] P. A. Sunarya, “Penerapan Sertifikat pada Sistem Keamanan menggunakan Teknologi Blockchain,” vol. 1, no. 1, pp. 58–67, 2022, [Online]. Available: https://journal.pandawan.id/mentari/article/view/139

[7] T. K. Agrawal, J. Angelis, W. A. Khilji, R. Kalaiarasan, and M. Wiktorsson,

"Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration," *Int. J. Prod. Res.*, vol. 61, no. 5, pp. 1497–1516, 2023, doi: 10.1080/00207543.2022.2039413.

[8] V. M.-J. of H. A. and ML, U. 2023, and V. L. P. Molli, "Blockchain Technology for Secure and Transparent Health Data Management: Opportunities and Challenges," *J. Healthc. AI ML*, vol. 10, no. 10, pp. 1–15, 2023, [Online]. Available: https://journalpublication.wrcouncil.org/index.php/JHAM/article/view/9

[9] E. Saputra and D. Fitri, "SISTEM INFORMASI PENGAMANAN SKCK MENGGUNAKAN BARCODE PADA DIT INTELKAM POLDA RIAU," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 5, no. 1, pp. 1–7, 2019.

[10] E. Chandra Ramdhani, D. Indah Permatasari, J. Eka Sapitri, S. Informasi, and T. Informasi, "Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional. SIPEKA (SISTEM INFORMASI PELAYANAN SKCK) PADA POLSESK KOTABARU KAB. KARAWANG," *J. Inf. Syst. Applied, Manag. Account. Res. ( Printed)*, vol. 5, no. 1, 2021, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/jisamar,

[11] P. P. Bandung, G. A. Rakhmat, and G. Alexis, "APLIKASI KAJAS SEBAGAI SISTEM INFORMASI PENGELOLA LAPORAN KRIMINALITAS BERBASIS WEB."

[12] Hendriyati Haryani, S. M. Wahid, A. Fitriani, and M. faris Ariq, "Analisa Peluang Penerapan Teknologi Blockchain dan Gamifikasi pada Pendidikan," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 1, no. 2, pp. 163–174, Jan. 2023, doi: 10.34306/mentari.v1i2.250.

[13] A. M. Mabruroh, F. Dewanta, and A. A. Wardana, "Implementasi Ethereum Blockchain dan Smart Contract Pada Jaringan Smart Energy Meter," *MULTINETICS*, vol. 7, no. 1, pp. 82–91, Oct. 2021, doi: 10.32722/multinetics.v7i1.4122.

[14] R. Balai, B. Pengembangan, S. Dan, P. Kominfo, K. Medan, and J. Tombak, "KAJIAN NETNOGRAFI TERHADAP KOMUNITAS CYBER DBC NETWORK ETNOGRAPHY STUDY ON COMMUNITY CYBER DBC NETWORK," 2018.