Al-Kharaj: Journal of Islamic Economics and Business
Volume 8 (2), 2026
P-ISSN: 2686-262X; E-ISSN: 2685-9300

Use of Biometric Data on Crypto Platforms in the Perspective of Islamic Economics

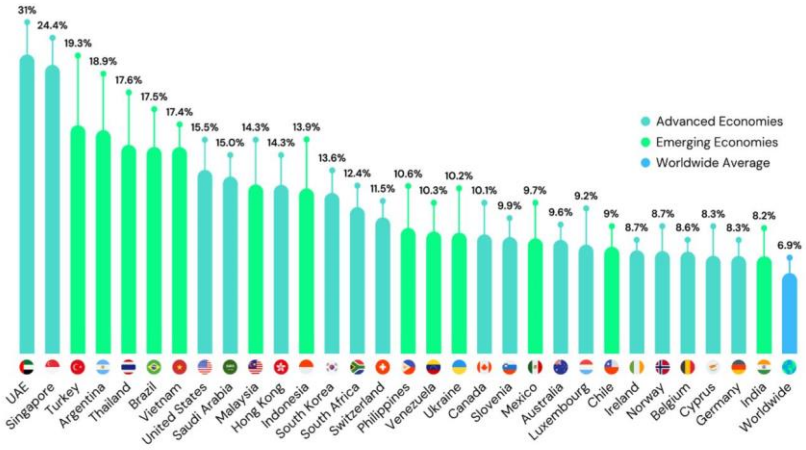
Dea Amanda Wulandari[1], Sukron Mamun[2], Kisanda Midisen[3], Sakum[4], , MH Ainulyaqin[5]
[12345]Sharia Economics Study Program, Faculty of Economics and Business, Pelita Bangsa University, Bekasi
E-mail:deaamandawulandarii@gmail.com,sukron@pelitabangsa.ac.id,kisandamidisen@pelitabangsa.ac.id sakum@pelitabangsa.ac.id,hamdanainulyaqien@pelitabangsa.ac.id

Keywords:
Biometric Data, Cryptocurrency, Islamic Economics.

Abstract: *Advances in digital technology, particularly in blockchain-based financial systems, have driven the increasingly widespread use of cryptocurrency in society. As the use of crypto platforms grows, security has become a primary concern, leading many platforms to adopt biometric authentication technologies such as fingerprint and facial recognition. This study aims to analyze the use of biometric data on crypto platforms and assess its suitability from an Islamic economic perspective. From an Islamic economic perspective, the use of biometric data on crypto platforms is fundamentally permissible because it does not involve elements of gharar, maysir, or usury; however, its use must adhere to the principle of benefit, protect privacy, and not cause harm to users. Thus, biometric technology is acceptable within the Islamic economy provided it is managed securely, transparently, and in accordance with Sharia principles.*

INTRODUCTION

Advances in digital technology have brought about various innovations in the global financial system. One of the most notable innovations is the emergence of cryptocurrencies based on blockchain technology. Cryptocurrencies, such as Bitcoin, Ethereum, and others, offer a decentralized, fast, and efficient financial system that does not require third-party intermediaries such as banks or traditional financial institutions. Global trends in cryptocurrency ownership and usage have shown a significant increase in recent years. This is driven by advancements in blockchain technology, rising digital literacy among the public, and a shift in preference toward more decentralized financial systems. This phenomenon indicates that cryptocurrency is no longer a niche phenomenon but has become an integral part of the dynamics of the global financial system.



Gambar 1. 1 *The State of Global Cryptocurrency Ownership in 2024*

Sumber: (Triple-A., 2024)

Figure 1.1, "The State of Global Cryptocurrency Ownership in 2024," shows that the number of cryptocurrency owners worldwide has reached 562 million people, an increase of 34% from 420 million in 2023. This figure is equivalent to approximately 6.8% of the world's population. This trend indicates that digital assets are gaining increasing popularity among the public, particularly among younger generations who are more open to technological innovation (Triple-A., 2024).
In Indonesia, the trend of cryptocurrency asset usage has shown a significant increase. According to data from Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI), the number of crypto investors in Indonesia reached 21.6 million people as of October 2024, increasing from 17.91 million in the previous year. This figure indicates that more people, especially the younger generation, are entering the crypto space, and along with this growth, the risk of cybersecurity threats, including the misuse of personal data, is also rising.

Amid the increasing use of crypto platforms, various security threats such as identity theft, hacking, and the misuse of digital accounts are becoming more prevalent, thus requiring stronger security systems to protect user data and assets. One solution that has begun to be implemented is the use of biometric data, such as fingerprints, facial recognition, and iris scans, as methods of authentication and identity verification, which are considered more reliable due to their unique characteristics and difficulty to be forged (Jain, Ross, 2024). Therefore, the application of biometrics is considered capable of enhancing the security and integrity of transactions compared to conventional authentication methods (Jain, Ross, 2024).

In Indonesia, regulations regarding personal data are governed under Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Personal Data Protection Law), which classifies biometric data as specific and sensitive data, although its implementation and supervision in the financial sector, particularly in crypto assets, are still limited. Therefore, it is important to ensure that the use of biometric technology remains aligned with sharia principles, especially in safeguarding privacy and individual rights, so that all financial activities can be conducted in a secure, fair, and trustworthy manner from the perspective of Islamic economics.

From the perspective of Islamic economics, every financial transaction must be free from elements of gharar, maysir, and usury. These principles serve as the foundation for assessing

various modern financial innovations, including cryptocurrency as part of digital technological developments. In this context, not only the transaction mechanisms need to be considered, but also supporting aspects such as security and user data protection. Therefore, the implementation of technology on crypto platforms, including the use of biometric-based authentication systems, must be carried out ethically with values of justice and honesty. In line with this, within Islamic economics, technologies that provide public benefit (benefit) and do not violate sharia principles are generally acceptable. Thus, examining the use of biometric data in crypto platforms becomes important in order to evaluate its compliance with sharia values (Karlan et al., 2020).

Several previous studies that form the basis of this research include the study conducted by Sirait et al., (2023), which shows that the use of biometric data in various business sectors in Indonesia has increased significantly, mainly because it is considered more secure and more difficult to forge compared to other types of personal data. A study by Muhammad Ridha, (2025) indicates that cryptocurrency has a high level of volatility and lacks a clear underlying asset, thereby potentially containing elements of uncertainty. However, under certain conditions, cryptocurrency may still be considered as a commodity as long as it does not violate sharia principles.
Furthermore, research by Kisanda et al. (2022) demonstrates that blockchain technology has advantages in enhancing the security of cryptocurrency transactions through its decentralized system and immutability (the property of data or objects that cannot be altered, edited, or deleted once created), making transaction data difficult to manipulate or change. A study conducted by Kamali, (2022) shows that new technologies must not only be evaluated from functional and security aspects but also must comply with ethical and moral values in Islam. This includes the obligation to ensure that the application of technology does not involve elements of gharar, maysir, and usury for its users. Subsequently, research by Arsyad, (2022), within the context of Islamic economics, emphasizes the importance of comprehensive studies to ensure that technology can be implemented safely, transparently, and in accordance with sharia principles. These findings indicate that the use of biometric data in various business sectors in Indonesia has increased because it is considered more secure and more difficult to forge compared to conventional data. However, these studies tend to focus primarily on technological and regulatory aspects in general.

However, these studies still tend to address technological, security, and legal aspects separately and have not specifically examined the use of biometric data on crypto platforms within an integrated analytical framework grounded in Islamic economics. Therefore, this study aims to fill this gap by analyzing the use of biometric data on crypto platforms based on Sharia principles. Considering all these aspects, this study is both relevant and important. It examines how biometric technology is applied within crypto platforms, what the risks and benefits are, and how these practices are evaluated from an Islamic economic perspective, as well as in light of the values of justice, honesty, and the protection of individual rights. This study is also expected to contribute to the formulation of policies and the development of technology that is ethical, secure, and in line with Islamic values. In this digital age, Muslims should not merely be consumers of technology but must also become key actors capable of evaluating and guiding technology in accordance with Islamic economics.

METHODS

Types and Design of Research

This research is qualitative with a normative-conceptual approach combined with a case study, ideal for exploring the phenomenon of biometric data use on crypto platforms and its alignment with Islamic economic principles in a natural setting (Sugiyono, 2022; Creswell & Poth, 2023). The qualitative approach allows the researcher, as the primary instrument, to collect descriptive data through source triangulation, analyzing inductively to understand the meaning, uniqueness, and building an understanding of phenomena related to data security and Sharia principles (Syahputra, 2020; Rijal, 2021). This flexible design utilizes primary and secondary data to address the research questions regarding biometric implementation and Sharia perspectives, focusing on a conceptual analysis of the DSN-MUI fatwa and the regulations of the PDP Law (Creswell & Poth, 2023; Emzir, 2023).

Data Collection Instruments and Techniques

The primary instrument was the researcher, supported by semi-structured interviews, participant observation, and documentation as primary and secondary data collection techniques (Sugiyono, 2022; Sudaryono, 2022). Interviews explored informants' perspectives on biometric authentication and hifdz al-mal, observations recorded the behavior of crypto platform users directly through the five senses, while documentation was collected from archives such as journals, fatwas, and regulations to strengthen the analysis (Emzir, 2023; Sudaryono, 2022). This technique ensured rich and credible data through triangulation, avoiding single-source bias, in accordance with Sharia fintech research practices (Syahputra, 2020; Rijal, 2021).

Population and Sample

The population included active crypto platform users in Indonesia, Islamic economics experts, sharia academics, and regulators such as Bappebti (Sugiyono, 2022; Creswell & Poth, 2023). The sample was purposively selected with relevance criteria: four informants (three active crypto users and one Islamic economics academic) to achieve data saturation for in-depth analysis of sharia compliance (Emzir, 2023; Sudaryono, 2022). This approach, consistent with qualitative case studies on Islamic crypto, ensures diverse representation without statistical generalization (Rijal, 2021; Syahputra, 2020).

Data Analysis Techniques

Data analysis follows the interactive model of Miles and Huberman: data reduction through selection and summary of focused biometric-sharia themes, data presentation in narratives, tables, or matrices for interaction patterns, and drawing preliminary conclusions via triangulation verification until a final conclusion answers the problem formulation (Sugiyono, 2022; Emzir, 2023). This iterative process is interpretive-inductive, with credibility validated through member checks and peer debriefing (Creswell & Poth, 2023; Sudaryono, 2022). The technique aligns with normative qualitative analysis on Islamic economic issues, ensuring objectivity and depth (Rijal, 2021; Syahputra, 2020).

Research Procedures

The procedure begins with ethical preparation and permits, parallel data collection (2-3 weeks of interviews, field observations, documentation), initial field reduction, interactive analysis until saturation, verification, and report preparation (Creswell & Poth, 2023; Sugiyono, 2022). Each stage is verified for validity, with researchers documenting reflections for transparency (Emzir, 2023; Sudaryono, 2022). A systematic, adaptive approach to crypto dynamics is oriented toward Sharia-compliant interests (Rijal, 2021; Syahputra, 2020).

RESULTS AND DISCUSSION

Description of the Use of Biometric Data on Crypto Platforms

This study aims to analyze the use of biometric data on crypto platforms from an Islamic economic perspective. Data were obtained through interviews with four informants: three active crypto platform users and one academic in the field of Islamic economics.

In this study, the author interviewed 4 informants, namely 3 active users of the crypto platform and 1 Islamic economics academy.

1. Use of biometric data on crypto platforms

The first interview focused on the use of biometric data on crypto platforms. The author conducted the first interview on January 20, 2026. The following are the results of the interview, which focused on the use of biometric data on crypto platforms:

Based on interviews and observations regarding the use of biometric data on the first phase of the crypto platform, on January 20, 2026, it was discovered that biometric data, such as fingerprints and facial recognition, had been implemented on the crypto platform they used. These features are typically used for logging into applications and for verification during transactions. According to Hafizh hugo harman the interviewee, the use of biometrics makes account access faster and more practical because it eliminates the need to manually enter passwords. Furthermore, the interviewee stated that the reason for using biometric authentication is because it is considered more secure and convenient. Fingerprints or facial recognition are considered difficult to imitate by others, thus providing additional protection for user accounts. Compared to passwords or OTPs, the interviewee considered biometrics more efficient because the process is faster and does not require additional codes.

Interviewees also experienced several issues when using biometric verification. For example, fingerprints couldn't be read when fingers were wet or dirty, and facial recognition sometimes failed in low lighting conditions. However, these issues were not considered to significantly impact the app's overall usability.

In terms of security, the source believes that biometric data can help improve account protection from hacking or identity theft. This is because biometric data is unique and difficult for third parties to fake. They acknowledge the risk of biometric data leaks if platform security systems are not properly managed.

Regarding biometric data storage, the source argued that crypto platforms should store such data with robust security systems, such as encryption and robust server protection. He added that platform managers must also ensure that user data is not misused by irresponsible parties.

Furthermore, the resource person also had general knowledge of the personal data protection policy in Indonesia, which is regulated by the Personal Data Protection Law (PDP Law). He stated that this regulation is crucial for ensuring that companies and digital platforms

maintain the confidentiality of users' personal data, including biometric data.

As a suggestion, the resource person hopes that crypto platform managers can continue to improve user data security systems, conduct regular system monitoring, and provide transparent information to users regarding how their biometric data is stored and used.

Based on interviews and observations regarding the use of biometric data on the first phase of the crypto platform, on January 11, 2026, it was discovered that, as a crypto platform user, biometric data was significantly helpful in improving account security. He stated that using fingerprints or facial recognition during login and KYC verification makes account access more practical and secure. He believes that with a biometric system, the possibility of an account being opened by a third party is reduced because only the original owner can access it.

In terms of security, Sabrina believes biometrics are more secure than password-based methods or OTP codes via SMS. She argues that passwords can be guessed or hacked, while OTPs are at risk of being intercepted. Meanwhile, biometrics are considered more difficult to forge, thus minimizing the risk of account hacking.

However, Sabrina also expressed concerns about the risk of biometric data leaks. She stated that facial or fingerprint data is highly personal and, if leaked, could be misused for fraud or other digital crimes. Therefore, she believes that crypto platform companies must have robust security systems and not carelessly share user data with third parties.

Regarding regulations, Sabrina stated that biometric data is classified as sensitive data and therefore must be strictly protected in accordance with the provisions of the Personal Data Protection Law (PDP Law 2022). She believes that the collection and use of biometric data should be carried out with the user's explicit consent and accompanied by guaranteed legal protection.

In general, Sabrina views the use of biometrics as an innovation that brings benefits in increasing account security, as long as it is managed transparently, is not misused, and still pays attention to protecting user rights.

Based on interviews and observations regarding the use of biometric data on the first phase of the crypto platform, on January 11, 2026, it was discovered that biometric data was used. Based on interviews, Adam, a user of the Indodax crypto platform, stated that biometric technologies such as fingerprints and facial recognition are very helpful in maintaining account security. She stated that biometric systems provide an additional layer of protection beyond usernames and passwords. She stated that even if someone knows her username and password, her account remains inaccessible without biometric verification.

In terms of effectiveness, Adam believes biometrics is quite secure and efficient because the authentication process is fast and minimizes the risk of digital identity theft. However, she still uses backup methods such as passwords as an alternative in case the biometric system is unusable, for example, due to technical issues with the device.

Regarding risks, Adam emphasized that biometric data is highly sensitive and must be stored in an encrypted system. She believes that companies should not provide access to this data to third parties without user consent. She believes that transparency regarding how data is collected, stored, and used is crucial for users to feel safe and trust the platform.

Regarding regulations, Adam stated that crypto service providers must comply with the provisions of the Personal Data Protection Law (PDP Law 2022). She believes that regulatory compliance represents a company's moral and legal responsibility to maintain the

confidentiality and security of user data.

Overall, Adam believes that the use of biometrics on crypto platforms offers significant benefits in enhancing account security, provided that data management is carried out professionally, transparently, and in accordance with applicable laws. Based on interviews, Adam, a user of the Indodax crypto platform, stated that biometric technologies such as fingerprint and facial recognition are very helpful in maintaining account security. She believes that biometric systems provide an additional layer of protection beyond a username and password. She explained that even if someone knows her username and password, her account remains inaccessible without biometric verification.

In terms of effectiveness, Adam believes biometrics is quite secure and efficient because the authentication process is fast and minimizes the risk of digital identity theft. However, she still uses backup methods such as passwords as an alternative in case the biometric system is unusable, for example, due to technical issues with the device.

Regarding risks, Adam emphasized that biometric data is highly sensitive and must be stored in an encrypted system. She believes that companies should not provide access to this data to third parties without user consent. She believes that transparency regarding how data is collected, stored, and used is crucial for users to feel safe and trust the platform.

Regarding regulations, Adam stated that crypto service providers must comply with the provisions of the Personal Data Protection Law (PDP Law 2022). She believes that regulatory compliance represents a company's moral and legal responsibility to maintain the confidentiality and security of user data.

Overall, Adam believes that the use of biometrics on crypto platforms offers significant benefits in enhancing account security, provided that data management is carried out professionally, transparently, and in accordance with applicable laws.

2. Islamic economist

The second source is an Islamic economist, the interview was conducted on January 18, 2026. The author conducted two interviews. The following are the results of the interview with the Islamic economist:

Based on the results of interviews and observations with Islamic economists in the first phase, on January 18, 2026, it was discovered that from an Islamic economic perspective, the use of biometric technology in crypto platforms is basically permitted as long as it does not contain elements prohibited in Islamic economics, namely gharar, maysir, and usury.

First, regarding the element of gharar, he stated that biometrics can actually minimize identity ambiguity in digital transactions. Verification systems using fingerprints or facial recognition can ensure that account holders are legitimate parties, thereby reducing the risk of fraud and account misuse. Therefore, from a security perspective, biometrics can reduce the potential for gharar by protecting user identity.

Second, regarding the element of maysir (gambling), he emphasized that it's not just the biometric technology itself that needs to be thoroughly examined, but also the transaction activities within the crypto platform. If transaction practices contain elements of excessive speculation and resemble gambling, then they could be considered maysir. However, the use of biometrics as an authentication and security tool does not contain elements of maysir because it is not related to speculation or chance.

Third, in the context of usury, Ust. Ahmad explained that usury is related to additional

requirements in debt or exchange transactions that are not in accordance with sharia provisions. The use of biometric technology is not directly related to usury practices. However, if the product or system on a crypto platform contains a mechanism that is usurious in nature, then this aspect needs to be studied legally, not the technology.

He also emphasized the importance of responsibility in managing biometric data. Data misuse, such as unauthorized distribution or harming users, is prohibited in Islam because it violates the principles of justice and the protection of individual rights.

Thus, based on the informant's view, the use of biometric data in crypto platforms is acceptable from an Islamic economic perspective as long as it does not contain elements of gharar, maysir, and usury and is not misused in practice.

DISCUSSION

Use of Biometric Data on Crypto Platforms

The development of digital technology has brought significant changes to various sectors, including technology-based financial systems. One emerging innovation is the use of biometric technology as an authentication method in various digital services. Biometric data is an identification system that utilizes an individual's biological characteristics, such as fingerprints, facial recognition, or iris recognition, to verify a user's identity. This technology is considered to have a higher level of security than conventional authentication methods such as passwords or PINs because biometric characteristics are unique to each individual.(Jain, Ross, 2024).

The use of biometric data is one way to improve user account security and protect identities during digital asset transactions. Crypto platforms are digital asset trading systems that utilize blockchain technology as their operational basis. This system allows users to conduct transactions directly without going through intermediaries like banks. However, the high transaction activity in digital systems also increases security risks such as account theft, identity fraud, and misuse of user data.

Based on the classification of general and specific data through the PDP Law, biometric data has been explicitly regulated in Article 4 paragraph (1) and paragraph (2) by emphasizing that biometric data is personal data of a specific nature. Thus, referring to the definition of specific data which has been clearly explained in the explanation of Article 4 paragraph (1) of the PDP Law, namely that specific personal data is personal data which, if processed, can have a greater impact on the personal data subject.(Sembiring, Ramli, 2024).

Crypto platforms implement a user identity verification system known as Know Your Customer (KYC). The KYC process is a procedure used by financial service providers to ensure that a user's identity matches their registered data. This process typically involves uploading identification documents such as an ID card or passport and performing facial verification using the device's camera. Facial recognition technology is then used to match the user's identity data with the uploaded documents, allowing the system to verify the user's authenticity.

The crypto trading ecosystem in Indonesia is also showing rapid development, with the presence of various digital asset trading platforms such as Indodax and Tokocrypto. These platforms operate under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti), which regulates crypto assets as tradable commodities in Indonesia.

One platform that provides crypto trading services is Tokocrypto. To trade on the Tokocrypto app, users must first download the app from the App Store or Play Store, then register an account by entering details such as an email address and password, and agreeing to the service's terms of

use. Once registration is complete, users will receive verification via email and will then be required to verify their identity through the KYC process. Without this verification, users will not be able to make transactions on the platform.

Once an account is verified, users can access the wallet menu in the app to view the various types of crypto assets available. Users can also deposit funds through a bank or digital wallet with a certain minimum amount before trading crypto assets in the marketplace menu. Furthermore, the platform offers a withdrawal feature to the user's bank account, subject to a minimum withdrawal limit and a specific administration fee.

Biometric data is also used in the authentication process when users access their accounts. Some crypto platforms allow users to log in using fingerprints or facial recognition via smartphone devices. Using biometrics allows users to access their accounts more quickly and conveniently without having to manually enter passwords. This also increases security because only the device owner has access to the biometric data.

Based on interviews conducted by researchers with three crypto platform users, it was discovered that the use of biometric technology facilitates account access. The first interviewee (N1) stated that the fingerprint or facial recognition login feature makes the app login process faster than using a password. Furthermore, the interviewee stated that the use of biometrics provides a sense of security because only the device owner can access the app.

A similar sentiment was echoed by the second source (N2), who stated that biometric technology helps improve account security from potential misuse by third parties. With a biometric verification system, users feel more protected from the risk of hacking or unauthorized access to their crypto accounts. Meanwhile, the third source (N3) also stated that the use of biometrics on crypto platforms provides convenience in using the application because the authentication process can be carried out more quickly and conveniently.

Based on the interview results, it can be concluded that the use of biometric technology on crypto platforms provides convenience and increases users' sense of security when accessing their accounts. Therefore, biometric technology is one solution used by crypto platforms to enhance digital security for their users. Biometric technology is increasingly used in various modern digital security systems.(Hartono, Rizaldi, 2022).

Islamic Economic Perspective

In Islamic economics, every economic activity must be carried out in accordance with sharia principles so that it does not contain prohibited elements such as gharar (uncertainty), maysir (speculation), and usury (unlawful additions to transactions).(Sahla, Nasution, 2023)Technological developments in digital financial systems, including the use of biometric technology in crypto platforms, need to be analyzed based on these principles.

*Cryptocurrency*is an innovation in digital financial systems that utilizes blockchain technology to record transactions transparently and decentralized. This technology offers several advantages, such as high transaction security, data transparency, and the potential to increase global financial inclusion. However, from an Islamic economic perspective, the existence of cryptocurrencies remains controversial due to the need to comply with Sharia principles in economic activities.

In Islamic economics, every transaction must be free from gharar (uncertainty), maysir (speculation or gambling), and usury (unfair interest). Therefore, the use of cryptocurrency needs to be analyzed based on these three principles.

1. Gharar

Gharar in Islamic economic law refers to the presence of uncertainty, ambiguity, or ambiguity in a transaction that could result in harm to one of the parties. Transactions containing excessive gharar are prohibited because they can lead to injustice and open up opportunities for exploitation.

The element of gharar is often associated with the high price volatility of crypto assets. The value of cryptocurrencies can fluctuate rapidly within a short period of time. For example, the price of Bitcoin can rise or fall drastically in a matter of hours or even minutes. This creates high uncertainty for users and investors. Some also argue that crypto lacks a clear underlying asset and is not regulated by a specific financial authority, such as a central bank.

However, some argue that not all cryptocurrencies contain excessive gharar. For example, stablecoins, whose value is pegged to a specific asset like the US dollar, lower price volatility, thus minimizing uncertainty.

2. Maysir

Maysir is a speculative activity similar to gambling, relying more on luck than effort or rational analysis. In Islamic teachings, all forms of gambling are prohibited because they provide no productive value and have the potential to cause harm to certain parties.

In practice, cryptocurrency trading is often associated with elements of maysir (gambling), particularly when conducted in short-term forms such as day trading or margin trading. In these activities, investors buy and sell crypto assets within a short period of time with the aim of profiting from rapid price fluctuations.

Many market participants engage in these transactions without a thorough understanding of the technology or fundamental value of the cryptocurrencies being traded. This activity is often based solely on speculation regarding market price movements. Not all cryptocurrency-related activities can be categorized as maysir (gambling). If someone invests in cryptocurrency with long-term goals and based on thorough analysis, the speculative element can be reduced. Therefore, some scholars argue that using cryptocurrency is still acceptable as long as it does not involve excessive speculation.

3. Usury

Usury is an unfair addition to a financial transaction. In conventional economic systems, usury typically appears in the form of interest charged on loans or deposits at financial institutions.

In the crypto ecosystem, elements of usury can arise in several mechanisms, such as crypto lending or staking, where users can earn returns on crypto assets they hold on a platform. If these returns are structured similarly to the interest system in conventional banking, then the practice can be categorized as usury. However, if the profits are derived from a profit-sharing system or a clearly defined investment activity, some scholars argue that such practices can still be considered within the framework of Islamic economics.

In Islamic jurisprudence, a currency generally must meet several criteria, including widespread acceptance as a medium of exchange, a relatively stable value, and a clear basis for value. In practice, cryptocurrencies like Bitcoin still face several limitations, including not being universally accepted as a means of payment, experiencing high price volatility, and not being backed by a central authority such as a central bank.

Based on an interview with Ustadz Ahmad Saekhu, the use of biometric data is part of a digital security system designed to protect user accounts. The use of biometric data, such as fingerprints or facial recognition, ensures that only the account owner can access the application or conduct transactions. The use of biometric technology is not directly related to the elements of gharar, maysir, or usury, as it serves solely as a tool for verifying user identity. With a biometric system in place, account security is better safeguarded, thereby minimizing the risk of misuse by third parties.

Based on an interview with Ustadz Ahmad Saekhu, the use of biometric data is part of a digital security system designed to protect user accounts. The use of biometric data, such as fingerprints or facial recognition, ensures that only the account owner can access the application or conduct transactions. The use of biometric technology is not directly related to the elements of gharar, maysir, or usury, as it serves solely as a tool for verifying user identity. With a biometric system in place, account security is better safeguarded, thereby minimizing the risk of misuse by third parties.

The use of biometric data on crypto platforms as a whole must still adhere to the principles of Islamic economics to ensure that transactions do not involve excessive speculation or practices that conflict with Sharia law.

Based on the research findings, the use of biometric data on crypto platforms is essentially part of a digital security system designed to protect user accounts. This technology is used for identity verification via fingerprints and facial recognition, thereby minimizing the risk of unauthorized account misuse.

From an Islamic economic perspective, the use of biometric technology is not directly associated with the elements of gharar, maysir, or usury. This technology serves solely as an authentication tool to ensure transaction security and protect users' digital assets. The use of biometrics can be viewed as an effort to enhance system security in digital transactions. The use of biometric data in crypto platforms is permissible under Islamic economics as long as it meets two main conditions.

4. First, it provides tangible benefits (maslahah), particularly in enhancing the security and efficiency of transactions. Second, it does not violate the principle of protecting individual rights, including safeguarding privacy and preventing data breaches. The high volatility of cryptocurrency prices has the potential to introduce elements of gharar, while speculative trading practices can lead to elements of maysir. Additionally, certain mechanisms within the crypto ecosystem, such as lending or staking, must be carefully examined to ensure they do not involve elements of usury.

CONCLUSION

This study concludes that the use of biometric data such as fingerprints, facial recognition, and iris recognition on crypto platforms like Indodax and Tokocrypto significantly enhances the security of authentication and KYC verification, making account access faster, more convenient, and harder to forge compared to passwords or OTPs (One-Time Password), as highlighted by three active users who emphasized these benefits, although minor technical issues such as wet fingers or poor lighting rarely cause disruptions.

From an Islamic economic perspective, experts state that this technology is permissible because it minimizes gharar through clear identity verification, is free from elements of maysir (gambling) and usury, and supports hifdz al-mal (the preservation of assets) provided there is consent, strong

encryption, and transparency in accordance with the Personal Data Protection Act (PDP) and DSN-MUI Fatwa No. 28/2021. This finding confirms that the use of biometric data aligns with Sharia principles in protecting users' assets and privacy within a crypto ecosystem vulnerable to cyber threats.

From the perspective of Islamic economics, biometric technology is not directly associated with the elements of gharar, maysir, or usury, as it serves solely as a means of securing the system. Therefore, the use of biometric data on crypto platforms is fundamentally permissible as long as it meets two main conditions: it must provide tangible benefits (benefit), particularly in enhancing transaction security and efficiency, and it must not violate the principles of individual rights protection, including safeguarding privacy and preventing the disclosure of confidential data.

Thus, the use of biometric data on crypto platforms is acceptable as a security system within the Islamic economy, provided that it serves the public interest, protects individual rights, and does not violate Sharia principles.

REFERENCE

Kamali, M. H. (2022). Maqasid al-Shariah Simplified. https://iiit.org/en/book/maqasid-al-shariah-made-simple/

Muhammad Ridha. (2025). Islamic Legal Review of Cryptocurrency: A Case Study of Bitcoin in the Category of Doubtful Wealth. Journal of Legal Research, Islamic Economics, Economics, Management and Accounting.https://doi.org/https://doi.org/10.61393/heiema.v4i2.331

Sakum. (2025). Gen Z's Consumptive Behavior and Digital Security Awareness in Indonesia's Digital Economyhttps://doi.org/https://doi.org/10.55123/jumintal.v4i2.6776

Arsyad, K. (2022). Fintech in Islamic finance: Theory and practice. UIN Alauddin Repository.https://repositori.uin-alauddin.ac.id/22775/

Coinvestasi. (2024). Triple-A Report: Crypto ownership in Indonesia is increasing.https://coinvestasi.com/berita/laporan-triple-a-38-juta-orang-di-indonesia-punya-kripto

Creswell, J. W., & Poth, C. N. (2023). Qualitative inquiry and research design: Choosing among five approaches (5th ed.). SAGE Publications.

Emzir. (2023). Qualitative research methodology: Data analysis. Rajawali Pers.

Foley, S., Karlsen, J., & Putniņš, T. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Ghafourian, M., Homayoun, S., & Dehghantanha, A. (2023). Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis. Journal of Cybersecurity Research.

Hartono, H., & Rizaldi, DL (2022). Literature study of biometric security systems for digital wallet verification and transactions. Journal of Information Technology.

Jain, A. K., & Ross, A. (2024). Introduction to biometric recognition. Springer.

Karlan, D., Osman, A. M., & Shammout, N. (2020). Enhancing financial inclusion in the Muslim world: Evidence from Islamic finance marketing experiments. World Bank Working Paper.

Indonesian Ulema Council. (2021). Law on crypto assets as commodities and a medium of exchange (DSN-MUI Fatwa No. 144/DSN-MUI/XI/2021).https://mui.or.id

Meriyati, M., Arifin, I., Arismanto, DFP, & Rizal, M. (2023). The law and existence of crypto trading for investment from an Islamic economic and social economic perspective. JUSTEKO, 7(2). https://doi.org/10.30651/justeko.v7i2.20456

Osman, M., Zawawi, N.A., & Muhammed, N. (2018). Privacy protection and cyber security policy for personal data protection. International Journal of Academic Research in Business and Social Sciences, 8(12).https://doi.org/10.6007/IJARBSS/v8-i12/5251

Prihatmoko, G. (2024). Islamic cryptocurrency: A Shariah principles' perspective study on current financial development. Journal of Islamic Financial Studies, 3.

Rijal, M. (2021). Understanding qualitative research method design. Humanities, 21(1).https://doi.org/10.21831/hum.v21i1.38075

Sahla, H., Nasution, M., & Siregar, S. (2023). Social justice and social welfare from an Islamic economic perspective. Scientific Journal of Islamic Economics, 9(3). https://doi.org/10.29040/jiei.v9i3.10500

Salleh, M.C.M., & Yaacob, H. (2020). Fintech and Islamic finance: Challenges and opportunities. Journal of Islamic Finance.

Sembiring, R., Ramli, T., & Rafianti, D. (2024). Implementation of privacy design as a protection for biometric data privacy. Veritas et Justitia, 10(1).https://doi.org/10.25123/vej.v10i1.7622

Sirait, RM, Ginting, RF, & Ginting, CDB (2023). Legal challenges of using biometric data for business purposes. JKPI: Journal of Islamic Educational Counseling, 4(2), 467–477.

Sudaryono. (2022). Research methodology: Quantitative, qualitative, and mixed methods. Rajawali Pers.

Sugiyono. (2022). Qualitative research methods. Alphabet.

Sufi', S., Putri, D., & Suhartini, S. (2023). Analysis of cybercrime threats and the role of biometric systems: Systematic literature review. Journal of Cyber Security.

Suryawijaya, TWE (2023). Strengthening data security through blockchain technology: Implementation in digital transformation in Indonesia. Journal of Public Policy Systems, 2, 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Syahputra, D. (2020). Quantitative and qualitative research methods. IMadeLaut.

Takahashi, D. (2022). Hackers steal $620M in Ethereum from Ronin Network. VentureBeat.https://venturebeat.com/games/hackers-steal-620m-in-ethereum-and-dollars-in-axie-infinity-maker-sky-mavis-ronin-network/

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.

Triple-A. (2024). Global cryptocurrency ownership data 2024.https://www.triple-a.io/cryptocurrency-ownership-data

Wijaya, DA (2016). Getting to know Bitcoin and cryptocurrency. Puspantara.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data. https://doi.org/10.1109/BigDataCongress.2017.85