Analysis of Blockchain Technology and Security Principles in Cryptocurrency Transactions according to the perspective of Islamic Economics. (Case study : Smart Contract on the Ethereum Blockchain Network)

Fahmi Sihabudin, Listian Indriyani Achmad,
Muhammad Hamdan 'Ainulyaqin, Kisanda Midisen, Sarwo Edy
listian.achmad@pelitabangsa.ac.id
Universitas Pelita Bangsa

Abstract: This study aims to understand the concept of security and privacy in blockchain technology through Islamic economics. Cryptocurrencies have been around for less than a decade, but they have caused divisions among religious scholars. Some Islamic scholars say that cryptocurrencies are haram or forbidden because they are based on speculation. Other scholars claim that cryptocurrencies are halal or permitted because they can be used for transactions that Islam considers legal. The debate over the legality of cryptocurrencies is complicated by the lack of a clear consensus among Islamic scholars. There is also disagreement over whether or not to allow investments in cryptocurrencies. This study uses a qualitative approach. Data collection was carried out using structured interviews with a number of respondents, including Islamic scholars and lecturers. The results of the study show that blockchain as a digital security transaction solution with its data decentralization is in line with the principles of Islamic Economics in the non-monetary field, but contradicts the principles of Islamic Economics in the monetary sector because of the obligation to follow the official Government in Monetary Policy.

Keywords: Security, Transactions, Blockchain, Cryptocurrencies, Smart contracts.

Abstrak: Penelitian ini bertujuan untuk memahami konsep keamanan dan privasi dalam teknologi blockchain melalui ekonomi Islam. Cryptocurrency telah ada selama kurang dari satu dekade, tetapi mereka telah menyebabkan perpecahan di antara para sarjana agama. Beberapa cendekiawan Islam mengatakan bahwa cryptocurrency adalah haram atau dilarang karena didasarkan pada spekulasi. Ulama lain mengklaim bahwa cryptocurrency adalah halal atau diizinkan karena dapat digunakan untuk transaksi yang dianggap legal oleh Islam. Perdebatan tentang legalitas cryptocurrency

diperumit oleh kurangnya konsensus yang jelas di antara para sarjana Islam. Ada juga ketidaksepakatan tentang apakah akan mengizinkan investasi dalam cryptocurrency atau tidak. Penelitian ini menggunakan pendekatan kualitatif. Pengumpulan data dilakukan dengan wawancara terstruktur dengan sejumlah responden, antara lain ulama dan dosen. Hasil penelitian menunjukkan bahwa blockchain sebagai solusi transaksi keamanan digital dengan desentralisasi datanya sejalan dengan prinsip Ekonomi Islam di bidang non-moneter, tetapi bertentangan dengan prinsip Ekonomi Islam di bidang moneter karena kewajiban untuk mengikuti Pemerintah resmi dalam Kebijakan Moneter
Kata kunci: Keamanan, Transaksi, Blockchain, Cryptocurrency, Kontrak pintar

Introduction

The era of the industrial revolution 4.0 has arrived. This has an impact on the economic system with the emergence of blockchain technology and the birth of a digital currency called cryptocurrency. In the long process of online and decentralized money exchange activities, there are miners who function as intermediaries to validate each transaction. Islamic economics must be able to adapt to the times, especially in the fields of technology and information. (Supplychain 4.0).

The Library of Congress (LOC) conducts periodic reviews of countries' attitudes towards Bitcoin and cryptocurrencies. In November 2021, the LOC identified 103 countries whose governments directed their financial regulatory bodies to develop regulations and priorities for financial institutions regarding cryptocurrencies and their use in AML/CFT. The LOC also identifies many countries that allow cryptocurrencies to be used including the United States, the European Union, Japan and others (Investopedia, 2021). Even in Islamic countries, cryptocurrencies are legalized and are starting to be adapted, such as in Bahrain, Kuwait, Iran, Lebanon and Palestine (Islamandbitcoin.com, 2021). On the other hand, the view of Islamic Economics regarding cryptocurrencies is not really clear. Up to this point, the discussion about cryptocurrencies is still concerned with the legitimacy of transactions and investments. As explained by the MUI (2021), "Cryptocurrency as a digital commodity/asset is not legal to be traded because it contains gharar, dharar, qimar and does not meet the sil'ah requirements according to syar'i, namely: there is a physical form, has value, the amount is known for certain, there are property rights and can be handed over to the buyer."

In digital transactions, there is an urgency to find solutions to security problems that often occur. This study uses a qualitative approach. Data collection was carried out using structured interviews with the Chancellor of the Muhammadiyah University of Surakarta, the Founder of The Great Coin Cryptocurrency, the CEO of Gaspack NFT Launchpad, and the Co-Founder of the Islamic Fintech Association, a Lecturer at the Faculty of Management and Sharia Business at the Tazkia Institute, a Lecturer at INISA, a Lecturer at IPAI UPI, a Lecturer of the Islamic Faculty at Universitas Pelita Bangsa, observations and documentation. The data obtained was then analyzed qualitatively through organizing the data, splitting it into units, compiling data collection, data reduction, displaying data into patterns, choosing which ones are important and what will be studied, describing them and then making conclusions. The results of the study show that blockchain as a digital security transaction

solution with its data decentralization is in line with the principles of Islamic Economics in the non-monetary field, but contradicts the principles of Islamic Economics in the monetary sector because of the obligation to follow the official Government in Monetary Policy.

There has been no further discussion regarding security in transactions that allow it to be adapted in the use of financial tech in the future. Even according to the DSN MUI fatwa, electronic money can be said to be legal if it meets the following elements: a) it is issued on the basis of the nominal amount of money deposited in advance to the issuer, b) the nominal amount of money is stored electronically in a registered media, and c) the nominal amount of electronic money managed by the the issuer is not a deposit as referred to in the law governing banking, and is used as a means of payment to merchants who are not the issuer of the electronic money. Problems with cryptocurrency transactions using blockchain technology are still not fully known, especially problems with security. There has been no deep discussion regarding the security of cryptocurrency transactions and adaptation to the development of blockchain technology in the perspective of Islamic economics. Therefore researchers are interested in analyzing the problems above with the title: "Analysis of the use of blockchain technology and security principles in cryptocurrency transactions according to Perspective Islamic Economics (Case study of smart contracts in the Ethereum blockchain network)."

Method

Based on the objectives to be achieved and the type of data required, this study uses a form of research that is descriptive qualitative by describing an empirical reality of the object being researched. As expressed by Mantra (2014), descriptive research aims to describe the complex social realities that exist in society. This research is a type of field research with an analytical descriptive approach to describe the data obtained in the field and then draw conclusions from the results of interviews.

After the data is collected, it is processed and analyzed by descriptive analysis. The analysis used is inductive analysis. After analyzing the cryptocurrency investment data, it is interpreted with a framework based on literature study. Finally, we will draw conclusions according to the research problem.

In qualitative research, the data collected through various different data collection techniques, such as interviews, observations, quotes, and suggestions from documents, notes through tape, can be described in words better than

numbers. Therefore, the data must be "processed" and analyzed before it can be used.

Result and Discussion

Decentralized blockchain technology allows each server to be connected to each other and have the same role. By establishing a kind of peer-to-peer network easier tracking of data is possible and if one server gets interrupted it can be backed up by another server, the problematic server can be temporarily removed from the blockchain network.

There is an urgency in the use of a decentralized system in the life of digital transactions because there are many dishonest parties in the process of recording transaction data that allow data corruption to occur. But it is necessary to build and maintain trust in order to counter the centralized systems. A centralized system that puts too much emphasis on approval and agreement from the authorized institution and that cannot provide freedom of transaction and should be considered obsolete.

Data decentralization in the perspective of Islamic economics refers to two things, the first from the monetary side. From a monetary point of view, decentralization of data is not an urgent problem for MUI, because according to their opinion, the only institution that has the right to create currency is the government. According to some, centralization of data in monetary principles is considered valid because trust has been achieved. More than that, they say that the demand for data decentralization in the monetary world is unnatural and the need does not exist.

In Islam itself, freedom is not fully given because in the principle of living life there are rules and norms that are applied. The true freedom that brings happiness and pleasure in life for humans cannot be achieved by abandoning religious norms. On the contrary, unbridled freedom is a life in shackles, as revealed in His word:

وَمَنْ أَعْرَضَ عَنْ ذِكْرِي فَإِنّ لَهُ مَعِيشَةً ضَنْكاً وَنَحْشُرُهُ يَوْمَ الْقِيَامَةِ أَعْمَى

"And whoever turns away from My warning, then indeed he (will taste) a narrow life (in this world), and We will gather him on the Day of Resurrection blind" (Surah Thaaha: 124). But from a non-monetary perspective, data decentralization can be implemented and perhaps more precisely, it should be implemented because there are trust issues. But if this blockchain is used in the

halal industry, for example. Well the dissatisfaction of data centralization is understandable.

Conclusion

Blockchain technology and cryptocurrencies should be investigated with their benefits and harms in mind. Those who criticize cryptocurrencies say that while these cryptocurrencies may have benefits, but they can cause more harm than these benefits. In this study, it was investigated whether this criticism is justified or not in terms of fiqh. Each cryptocurrency and Blockchain should be checked separately. The study of fiqh on blockchain returns to the concept of Islamic economics which emphasizes honesty with the limits of religious norms. So far, the fatwa on security from MUI, and studies on security in digital transactions have only been covered non-specifically in several DSN MUI fatwas, one of which is fatwa 117/DSN-MUI/II/2018. Those who put forward shariah rules still free individuals or institutions to create systems as long as they do not conflict with the shariah limits. The Blockchain Network provides a distributed database of records or public ledgers of all transactions that have been executed and shared among the participating parties, unlike conventional systems that record transactions as a central one. All parties verify every transaction in the system. When a transaction is recorded and confirmed on the blockchain, this record can no longer be changed or deleted (Crosby et al., 2016).

One of the important advantages of this technology is that all members or servers using the system have access to all transaction records. The immutability of this block prevents any changes to its contents. There is virtually no risk of cyber attacks because the same data is stored on thousands of users' computers (Crosby et al., 2016). In Islam, the concept of muamalah in society has been well and clearly regulated, as written and confirmed in the Qur'an and Hadith which implies a message about boundaries and maintaining one's privacy. As explained in QS An-Nur verse 27 which says that "O you who believe, do not enter a house that is not your house until you ask permission and greet its inhabitants. That is better for you, so that you (always) remember." "Yes, the argument or the rules in Islamic economics or fiqh muamalah maliyah in particular is that all transactions are allowed unless there is a proposition that prohibits and one of the prohibitions in transactions is decreased. Islamic economics is not allowed to do injustice. Thus, one of the injustices that I understand is not maintaining the security of data and transactions of the parties involved in the transaction. In other words, Islamic economics must maintain the security of data and transactions of the transacting parties. If the parties who do not transact do not maintain the security of their data and

transactions. It means that the document is personal data, especially if you intentionally leak data, then there will be injustice. Which injustice is once again avoided in transactions carried out by the parties in the corridor of Islamic economics.

The respondents in this study said that blockchain as a digital security transaction solution with its data decentralization is in line with the principles of Islamic Economics in the non-monetary field, however, when talking about monetary life, of course this is a separate prohibition, because in the process of making and distributing currency, the government has full power. In Islam, obeying the leader where he lives is an obligation.

Bibliography

Ali, S. T. (2015, March). Bitcoin: perils of an unregulated global P2P currency (Transcript of Discussion). In Cambridge International Workshop on Security Protocols (pp. 294-306). Springer, Cham.

Westin, A. F. (1972). Databanks in a free society: Computers, record-keeping and privacy. Report of the Project on Computer Databanks of the Computer Science and Engineering Board.

Anwar, N. S. (2019). Analisis Transaksi Digital Cryptocurrency Sebagai Investasi Global Dalam Perspektif Hukum Islam (Studi Kasus Dinar Dirham di Makassar). Gordon, JM (1998). Business Law: An Introduction. Business Law: An Introductionby TheBusinessProfessor. Com, 501, 428-431.

Barker, E., & Barker, E. (2016). Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. US Department of Commerce, National Institute of Standards and Technology.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE symposium on security and privacy (pp. 104-121). IEEE.

Bygrave, L. A. (2014). Data privacy law: an international perspective (Vol. 10). Oxford: Oxford University Press.

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. InProc. on Advances in Cryptology, ser. CRYPTO'88, Santa Barbara, CA.

Danial, K. (2019). Cryptocurrency Investing For Dummies. John Wiley & Sons

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy and the criminal law.

Dierks, T., & Rescorla, E. (2008). RFC 5246-the transport layer security (TLS) protocol version 1.2. The Internet Engineering Task Force (IETF).

Dr, P. (2008). Sugiyono, Metode Penelitian Kuantitatif Kualitatif dan R&D. CV. Alfabeta, Bandung.

Finney, H. (2004). Reusable proofs of work. Web Archives Homepage

Girasa, R. (2018). Regulation of cryptocurrencies and blockchain technologies: national and international perspectives. Springer.

Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering.

j Moleong, L. (2005). metodologi penelitian kualitatif, edisi revisi bandung: remaja Rosdakarya.

Judmayer, A., Stifter, N., Krombholz, K., & Weippl, E. (2017). Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms. Synthesis Lectures on Information Security, Privacy, & Trust, 9(1), 1-123.

Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.). (2017). Data protection and privacy:(In) visibilities and infrastructures. Springer International Publishing.

Liu, A. X., & Li, R. (2021). Algorithms for Data and Computation Privacy (pp. 3-404). Springer.

Luhmann, N. (1992). What is communication?. Communication theory.

Maulana, M. I., Kurnia, A. D., & Nurbaeti, A. (2021). Studi Kajian Bisnis Tambang Uang Digital (Cryptomining) Dalam Konteks Ijarah. EKSISBANK (Ekonomi Syariah Dan Bisnis Perbankan), 5(1), 35-56.

Mantra, I. B. (2004). Filsafat penelitian & metode penelitian sosial. Pustaka Pelajar.

Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., ... & Baird, M. (2016). Distributed ledger technology in payments, clearing, and settlement.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2017). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.

Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016, March). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 305-320). IEEE.

Purhantara, W. (2010). Metode Penelitian Kualitatif Kuantitatif Untuk Bisnis. Cet. I. Yogyakarta: Graha Ilmu.

Prusty, N. (2017). Building blockchain projects. Packt Publishing Ltd.

Quest, M. (2018). Cryptocurrency Foundation Success: The Beginners and Experts Guide to Understanding Basic and Advanced Concepts of Cryptocurrency, Bitcoin, Ethereum, and Altcoin Trading and Investing.

Sihombing, M. S. P., Nawir, J., & Mulyantini, S. (2020). CRYPTOCURRENCY, NILAI TUKAR DAN REAL ASSET TERHADAP HARGA SAHAM PADA PERBANKAN INDONESIA YANG TERDAFTAR DI BURSA EFEK INDONESIA. Ekonomi dan Bisnis, 7(2), 171-196.

Soediro, S. (2018). Prinsip Keamanan, Privasi, dan Etika dalam Undang-undang Informasi dan Transaksi Elektronik dalam Perspektif Hukum Islam. Kosmik Hukum, 18(2).

Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems, 36(1), 37-73.

Tamò-Larrieux, A., Tamò-Larrieux, & Seyfried. (2018). Designing for privacy and its legal framework. Cham: Springer.

Tavani, H. T. (2008). Floridi's ontological theory of informational privacy: Some implications and challenges. Ethics and Information Technology, 10(2-3), 155-166.

Wood, G. (2017). Ethereum: a secure decentralised generalised transaction ledger (2014).