LEGAL FRAMEWORK FOR PROTECTING BANKING TRANSACTIONS IN THE METAVERSE AGAINST DEEPFAKE TECHNOLOGY

Ifan Arsyad, Jamal Wiwoho

ABSTRACT

Background: In the virtual world of the metaverse, various activities such as banking transactions and blockchain, despite their positive impacts, are not immune to the risks of financial cybercrime, including the use of artificial intelligence deepfake technology. This technology can create seemingly authentic audiovisual content from individuals or customers, leading to data theft, money laundering, and other financial crimes. This research aims to analyze the legal framework governing banking transactions in the metaverse and blockchain, as well as the legal regulations addressing the protection against financial cybercrimes involving deepfake technology.

Methods: This research employs the doctrinal legal research method. The approach utilized includes the legislative approach (statute approach), conceptual approach, and comparative approach. It also utilizes primary data sources such as laws and secondary data sources like books, journals, and internet resources related to banking transactions in the metaverse and deepfake technology.

Results: The analysis results indicate that the Information and Electronic Transactions Law (UU ITE) and the Financial Services Authority (OJK) regulations in Indonesia do not specifically address banking transactions in the metaverse and blockchain. Additionally, the Personal Data Protection Law and regulations related to crimes involving deepfake artificial intelligence technology are also not specifically accommodated; they currently only have general coverage. This creates a legal vacuum in Indonesia regarding these issues.

Conclusion: There are differences in regulations in each country that govern banking transactions in the metaverse and crypto, as well as regulations on cyber financial crimes. Therefore, the government needs to review existing regulations and reconstruct them to govern banking transactions in the metaverse and blockchain. It is also essential to create specific regulations for the protection of personal data and regulations specifically addressing artificial intelligence.

Keywords: banking, blockchain, deepfake, legal protection, metaverse.

Received: 11/20/2023
Accepted: 02/12/2024
DOI: https://doi.org/10.55908/sdgs.v12i2.3199

a Master of Law Student, Faculty of Law, Universitas Sebelas Maret Surakarta, Central Java, Indonesia, E-mail: ifan.cpm@student.uns.ac.id, Orcid: https://orcid.org/0009-0002-5819-0815
b Professor in Law, Faculty of Law, Universitas Sebelas Maret Surakarta, Central Java, Indonesia, E-mail: jamalwiwoho@staff.uns.ac.id, Orcid: https://orcid.org/0000-0003-2931-8402
QUADRO JURÍDICO PARA PROTEGER AS TRANSAÇÕES BANCÁRIAS NO METAVERSO CONTRA A TECNOLOGIA PROFUNDA

RESUMO

Antecedentes: No mundo virtual do metaverso, várias atividades, como transações bancárias e blockchain, apesar de seus impactos positivos, não estão imunes aos riscos de cibercrime financeiro, incluindo o uso de inteligência artificial aprofundam a tecnologia. Esta tecnologia pode criar conteúdo audiovisual aparentemente autêntico de indivíduos ou clientes, levando ao roubo de dados, lavagem de dinheiro e outros crimes financeiros. Esta pesquisa tem como objetivo analisar o quadro legal que regem as transações bancárias no metaverso e blockchain, bem como os regulamentos legais que abordem a proteção contra os ciberdelitos financeiros envolvendo tecnologia deep fake.

Métodos: Esta pesquisa emprega o método de pesquisa legal doutrinal. A abordagem utilizada inclui a abordagem legislativa (abordagem estatutária), a abordagem concetual e a abordagem comparativa. Ele também utiliza fontes de dados primárias, como leis e fontes de dados secundárias, como livros, jornais e recursos da internet relacionados a transações bancárias no metaverso e tecnologia de falsificação profunda.

Resultados: Os resultados da análise indicam que a Lei de Informações e Transações Eletrónicas (UU ITE) e os regulamentos da Autoridade de Serviços Financeiros (OJK) na Indonésia não abordam especificamente as transações bancárias no metaverso e blockchain. Além disso, a Lei de Proteção de Dados Pessoais e regulamentos relacionados a crimes envolvendo tecnologia de inteligência artificial falsificada profunda também não são especificamente acomodados; eles atualmente têm apenas cobertura geral. Isso cria um vazio jurídico na Indonésia em relação a essas questões.

Conclusão: Há diferenças na regulamentação em cada país que regem as transações bancárias no metaverso e cripto, bem como na regulamentação sobre crimes financeiros cibernéticos. Portanto, o governo precisa rever os regulamentos existentes e reconstruí-los para governar as transações bancárias no metaverso e na cadeia de blocos. É também essencial criar regulamentos específicos para a proteção dos dados pessoais e regulamentos especificamente relacionados com a inteligência artificial.

Palavras-chave: bancário, blockchain, deep fake, proteção legal, metaverso.

MARCO JURÍDICO PARA PROTEGER LAS TRANSACCIONES BANCARIAS EN EL METAVERSO CONTRA LA TECNOLOGÍA FALSA

RESUMEN

Antecedentes: En el mundo virtual del metaverso, diversas actividades como las transacciones bancarias y la blockchain, a pesar de sus impactos positivos, no son inmunes a los riesgos de la ciberdelincuencia financiera, incluido el uso de la inteligencia artificial y la tecnología de profundidad. Esta tecnología puede crear contenido audiovisual aparentemente auténtico de individuos o clientes, lo que lleva al robo de datos, lavado de dinero y otros delitos financieros. Esta investigación tiene como objetivo analizar el marco legal que rige las transacciones bancarias en el metaverso y blockchain, así como las regulaciones legales que abordan la protección contra los ciberdelitos financieros que involucran tecnología deepfake.

Métodos: Esta investigación emplea el método de investigación doctrinal legal. El enfoque utilizado incluye el enfoque legislativo (enfoque estatutario), el enfoque conceptual y el enfoque comparativo. También utiliza fuentes de datos primarios como leyes y fuentes de datos secundarias como libros, revistas y recursos de Internet relacionados con transacciones bancarias en la tecnología metaverse y deepfake.
Resultados: Los resultados del análisis indican que la Ley de Información y Transacciones Electrónicas (UU ITE) y las regulaciones de la Autoridad de Servicios Financieros (OJK) en Indonesia no abordan específicamente las transacciones bancarias en el metaverso y la cadena de bloques. Además, la Ley de Protección de Datos Personales y las normas relativas a los delitos relacionados con la tecnología de inteligencia artificial profunda tampoco se tienen en cuenta específicamente; en la actualidad sólo tienen una cobertura general. Esto crea un vacío legal en Indonesia con respecto a estos temas.

Conclusión: Existen diferencias en las regulaciones de cada país que rigen las transacciones bancarias en el metaverso y cripto, así como las regulaciones sobre delitos financieros cibernéticos. Por lo tanto, el gobierno necesita revisar las regulaciones existentes y reconstruirlas para gobernar las transacciones bancarias en el metaverso y la cadena de bloques. También es esencial crear normas específicas para la protección de los datos personales y normas que aborden específicamente la inteligencia artificial.

Palabras clave: banca, blockchain, deepfake, protección legal, metaverso.

1 INTRODUCTION

"Metaverse" is a term formed by combining two words, namely "meta," meaning beyond, and "universe." Therefore, metaverse is interpreted as a post-reality universe that combines physical reality with the virtual digital world (Saad et al., 2023). This extraordinary technology, also known as internet advancement, encompasses various technologies that enable multisensory interaction with the virtual environment, humans, and digital objects such as virtual and augmented reality (Vakiti & S L, 2023).

Technically, the metaverse can be defined as a interconnected network of social environments that allows unlimited real-time communication and dynamic digital interaction among users.

Metaverse is typically used as a fully virtual interactive space, where users can create their avatars, interact with other users, and participate in various virtual activities such as real estate, gaming, shopping, attending academic events, professional meetings (Firmansyah & Umar, 2023) and even business and banking transactions. In the virtual world of the metaverse, big data also plays a role in contributing to the development of the fintech industry, especially in Indonesia. The utilization of big data and metaverse in the advancement of the fintech and banking industry provides many conveniences, facilitates more precise decision-making, and enhances profitability (Yathiraju & Dash, 2023). Millions of people worldwide have embraced digital and social media in recent years. This ongoing transformation in digital technology has changed the way individuals and organizations interact and operate, with significant consequences for global life.
A number of businesses in the financial banking sector, particularly those related to financial technology (fintech) and banking, are beginning to recognize and implement virtual reality and technology, especially by local digital companies. With the expanding development of the metaverse and its potential for direct engagement, businesses in the financial services industry, including fintech, are increasingly open to the opportunities and conveniences that arise. The advantages of the metaverse in enhancing customer engagement beyond physical boundaries and mobile applications, along with the utilization of computer technology, have become a major attraction for these business providers (Yathiraju & Dash, 2023).

In the realm of banking services for customers, the metaverse can provide a unique and immersive experience, ranging from virtual branches, augmented reality account management, virtual financial education, to virtual real estate tours and mixed-reality banking applications (Nguyen et al., 2023). These applications assist and facilitate customers in navigating and controlling the virtual world to access various banking services, interact with virtual tellers or advisors, and perform tasks such as fund transfers, bill payments, and account management with intuitive movements and visualizations. Several conventional banks and financial institutions have entered the metaverse banking arena to meet the growing consumer demand. With nearly half of bankers projecting that customers will use augmented reality (AR) and virtual reality (VR) as alternatives for transactions by 2030 (Dwivedi et al., 2021), the financial industry is eagerly exploring the advancements of this evolving technological trend (Nguyen et al., 2023).

Figure 1. How digital banking works in Metaverse

Source: Antier (Solution, 2023)
In Indonesia, one of the banking service providers, Bank Negara Indonesia (BNI), collaborates with Telkom University to create virtual banking services in the metaverse, aiming to enhance digital banking services for customers. The collaboration with BNI began in 2021 to develop BNI Metaverse (Anesti & Maulana, 2023). This development is part of the Computer Metaverse Avatar Creation and Interaction program of the BNI Virtual World, aiming to realize the BNI Virtual World on the Metaverse platform. The objectives of this platform include providing a more interactive and enjoyable banking experience for BNI customers (Anesti & Maulana, 2023).

In the virtual world of the metaverse, alongside its positive aspects in human life, there is also the negative aspect of cybercrime, including malware viruses, virtual online bullying, and fraudulent activities such as deepfake. The term "deepfake" itself is derived from the combination of "deep learning." Currently, there is no universally accepted definition for the term "deepfake" (Wu et al., 2023). Deepfake refers to manipulated media created using artificial intelligence and deep learning machine learning techniques. This process is carried out through neural networks with the aim of deceiving viewers, especially in the virtual world of the metaverse (Whittaker et al., 2020). In the United States, there is the "Deep Fake Prohibition Act of 2018," which defines "deep fake" as "an audiovisual recording that has been created or altered in a manner that would falsely appear to a reasonable observer or authentic expert to be an authentic recording of the actual person, whether or not such person existed, in a manner that mimics that person's likeness and voice." The term "audiovisual recording" refers to digital content such as images, videos, and sound. While deepfakes can be used for creative purposes like entertainment, education, and art, they also have the potential for illegal use, such as spreading fake news, defamation, or fraud, especially in banking transactions in the virtual world of the metaverse (Wu et al., 2023).

Due to the evolving nature of deepfake technology as a cybercrime, a significant portion of internet users cannot directly and specifically recognize this form of media (Stavola & Choi, 2023). The results of recent studies indicate that out of 93 respondents, 65% had no knowledge of deepfake at all. Only 13% were confident that the majority of internet users could identify deepfake, while the remaining 57% believed that the average internet user could not distinguish between deepfake and authentic media (Ahmed et al., 2021).
In Indonesia, the regulation of the metaverse is not specifically outlined at the moment, and virtual banking transactions in the metaverse are also not regulated. Currently, the Electronic Transaction Law (ITE Law) and the Financial Services Authority Regulation No. 12/POJK.03/2018 concerning digital banking serve as the general legal framework. Special attention is given to customer protection, particularly in banking transactions in the metaverse, as the virtual world of the metaverse is inherently global. The purpose of this writing is to analyze the existing legal regulations regarding the protection of banking transactions in the metaverse and how the law safeguards against the misuse of deepfake technology in banking transactions within the metaverse in Indonesia. It also aims to explore virtual banking transactions, various types of cybercrimes, and financial crimes on the blockchain, including deepfake, within the virtual world of the metaverse.

2 RESEARCH METHODS

The aim of this research is to examine how the law is applied to bank transactions in the metaverse and the challenges posed by deepfake technology crimes. This study utilizes normative legal research, also known as doctrinal legal research. In this type of research, the law is often considered as what is written in statutes (law in book) or as norms or principles that serve as the foundation for societal behavior based on what is deemed right. However, in reality, the law can also be seen as what happens in practice (law in action) (Efendi & Ibrahim, 2018). Law in book is a representation of the law that should be applied as expected, but it often differs from what is stipulated in statutes when implemented in society.

The approach in this research involves the statute approach, conceptual approach, and comparative approach, using positive legal materials from several other countries. It also utilizes primary data sources such as statutes and secondary data sources like books, journals, and the internet (Ali, 2009).

3 RESULTS AND DISCUSSION

3.1 BANKING TRANSACTIONS IN THE METAVERSE

The concept and implementation of banks providing services to customers, especially within the Metaverse, have recently become a crucial topic of discussion in the banking industry (Zainurin et al., 2023). The emergence of the term "Fintech" in the
virtual Metaverse has sparked widespread discussions. Every aspect of human life has undergone significant changes as a result of the rapid advancements in financial technology. In the banking industry, the Metaverse is considered a vital technology, as it allows customers to interactively make financial payments and engage in other banking transactions. Within the banking sector, the Metaverse facilitates virtual payments and enables users to experience branch features virtually (Turdialiev, 2022). Collaborations between financial institutions and Fintech companies aim to eliminate physical barriers, making Fintech more attractive, user-friendly, interactive, and immersive through the use of Virtual Reality, Artificial Intelligence, and the Metaverse (Vakiti & S L, 2023).

Conventional banks, which have physical locations and licenses for domestic banking, are known for their physical presence, such as regional offices in each country where they operate, ATMs with their own branding and logo, and a substantial workforce, including managers and customer service representatives, including tellers and other officers. On the other hand, online banking in the metaverse is virtual in nature. With the support of the Metaverse today, it becomes possible to conduct financial transactions in a virtual space, creating a uniquely engaging experience, especially for virtual bank customers in the metaverse (Vakiti & S L, 2023).

The Metaverse offers a new digital experience in the form of virtual avatars, providing an immersive alternative to the traditional concept of a virtual world. Several banks worldwide are aligning their services with the Metaverse technology trend after achieving success in digital banking. Financial institutions strive to remain relevant and resilient by seizing new opportunities in the Metaverse, which has suddenly captured attention in a unique way rarely seen in the business world.
In the Metaverse, analytics becomes a crucial aspect, especially for Fintech companies and banks, to understand how customers utilize virtual financial services. Customer interactions serve as a clear example of how the "Metaverse" can impact banking. Serving bank customers in the virtual world may be the logical next step in the digital customer experience, as demonstrated by CBM Bank based in the United States. CBM Bank has developed a fully immersive virtual world experience for its customers, accessible through smartwatches and augmented reality headsets (Vakiti & S L, 2023). With the advent of the digital metaverse, several banks worldwide are also involved in investing in and implementing virtual banking (Banker, 2022).

3.2 THE LEGAL REGULATIONS CONCERNING THE PROTECTION OF BANKING TRANSACTIONS IN THE METAVERSE

Currently, some countries regulate digital banks and apply their laws based on conventional banking regulations. However, there are also several countries developing a legal framework specifically for digital banks. The main differences between the licensing requirements for digital banks and conventional banks lie in the technological elements and the goals of the business itself. In the case of digital banks, licensing requirements emphasize management in the field of technology and achievement targets in technology, including a commitment to financial inclusion (Anggara et al., 2022).

In Indonesia, regarding digital banking activities, the Financial Services Authority (OJK) has issued two regulations to accommodate new rules for digital banking activities in Indonesia. These are POJK No. 12/2021 and POJK No. 13/2021. POJK No. 12/2021...
defines digital banks as banks that provide and conduct their business activities primarily through electronic channels without physical branches, except for the headquarters or by using technology. Therefore, digital banks in Indonesia must comply with the requirements set out in both regulations (Anggara et al., 2022).

Article 25 of Regulation No. 12/2021 stipulates that digital banks can be established and operated through two methods: the establishment of a new BHI bank or the transformation of an existing BHI bank into a pure digital bank. Regulation No. 13/2021 on the Implementation of Products and Transactions of Commercial Banks is expected to accelerate the digital transformation of banking, providing space for banks to innovate in offering digital products and services. Article 15 of Regulation No. 13/2021 also requires banks to submit additional documents related to the offering of digital banking services, such as a description of the collaboration mechanism with bank partners and the results of an independent examination of product characteristics and the sufficiency of information technology security systems (Anggara et al., 2022). With these regulations, it is expected to address the security needs of customers in digital banking services.

In banking transactions in the metaverse, in addition to using currencies recognized by some digital banks, cryptocurrencies are also utilized. Below are the crypto regulations in some countries:

3.2.1 The United States

Regarding regulations in the United States, government agencies such as the Commodity Futures Trading Commission (CFTC), Department of Justice, Financial Crimes Enforcement Network, Federal Board of Governors, and the Securities and Exchange Commission believe that blockchain technology falls under their jurisdiction. The regulation also depends on the specific use of the blockchain (Sugiharto et al., 2022).

3.2.2 Australia

In Australia, in 2015, the government released a report through the Australian Parliament titled "Digital Currency - Game Changer or Bit Player," addressing digital currency or cryptocurrencies and their impact on the Australian economy. The report covers various aspects, including benefits, risks, regulatory provisions, taxation, and money laundering. The Australian Taxation Office (ATO) has issued guidelines
regarding the taxation of digital currency. Cryptocurrencies in Australia are considered speculative assets (capital gain) subject to taxation. However, if cryptocurrencies are used for buying and selling transactions, the seller is the one who receives and records it as ordinary income. Currently, the ATO continues to monitor and develop regulations related to cryptocurrencies in Australia.

3.2.3 Indonesia

In Indonesia, regulations regarding crypto are governed by the Commodity Futures Trading Regulatory Agency (Bappebti) Number 2 of 2020 concerning the Second Amendment to the Commodity Futures Trading Regulatory Agency Regulation Number 5 of 2019 concerning the technical aspects of Crypto Asset physical market implementation on Commodity Futures Exchanges. Concerning tax implementation, the Indonesian Directorate General of Taxation has not yet issued specific regulations regarding cryptocurrency taxation in Indonesia.

3.3 SEVERAL CRIMES IN THE METAVERSE, INCLUDING DEEPFAKE

Several criminal activities nowadays, such as fraud, hacking, and crimes involving deepfake technology, are some of the crimes in the current digital economy, especially in banking. Financial crimes continue to experience significant growth each year, both detected and undetected, with a substantial increase (KATTERBAUER et al., 2022). Furthermore, the losses due to fraud can result in additional costs due to the expensive handling. In general, banks face various risks arising from cybercrime, including vulnerabilities to financial crimes and fraud in the context of automation and digitization, significant growth in transactions, and the integration of financial systems, particularly in banking transactions within the metaverse.
Financial crimes in the current digital economy have prompted a significant number of regulators to revise and review regulations and accounts related to fraud, money laundering (Nicholls et al., 2021) and even crimes involving digital deepfake technology.

In each country, institutions are increasingly realizing that conventional approaches to combating financial crimes in the current digital economy are not effective in addressing cybercrime. This has led several countries to become more adaptive. To enhance detection, prevention, and handling, distinctions exist between fraud and financial crimes. New cyber threats have blurred and given multiple interpretations to these concepts, making criminal activities more complex and interconnected. Legally and generally, there is no regulatory difference between these concepts, but differences arise mainly in the organizational structure of each country. Financial crimes are usually related to money laundering and other criminal offenses, including bribery and tax evasion. It also involves the use of financial services to support criminal activities. These challenges typically arise as a result of compliance issues, especially when financial institutions attempt to avoid fines or refuse to engage in anti-money laundering activities (Leukfeldt et al., 2019).

Several fraud-related crimes generally involve forgery, credit card fraud, and sometimes include the use of deception by personnel or financial services to steal. Fraud is commonly regarded as a loss issue, and financial institutions use sophisticated analytics to detect and prevent it in real-time. Challenges arise because these crimes often occur together and are interconnected in the metaverse (Karpoff, 2021).
Starting from the definition of Deepfake itself, it is a result of artificial intelligence and machine learning technology that combines, substitutes, or arranges various types of content to create synthetic media forms that function to blur the original differences from the imitated media or forms (Maras & Alexandrou, 2019). The utilization of Artificial Intelligence, especially deepfake, involves using datasets of voices, images, or videos to create a resemblance of someone to another person. The use of deepfake technology in criminal activities, particularly in the digital economy of the metaverse, serves as an example of individuals saying and doing things they did not say or do, especially in virtual banking transactions in the metaverse (Samani, 2022).

Some challenges posed by deepfake in the financial and banking sector in the metaverse include:

3.3.1 Ghost Fraud

Perpetrators of this crime typically use the personal data of deceased individuals or customers to gain financial advantages. This can occur during online service transactions, monitoring savings accounts, and applying for funds or other transactions. Deepfake technology provides credibility to such applications because the application sees a moving and talking figure on the screen, believed to be a living customer or client.
3.3.2 Fraudulent claims from the deceased

Similarly, perpetrators also create false insurance claims in the name of individuals who have passed away. These claims can continue to be successfully made for pensions, life insurance, and benefits for a considerable period after the person's death and may be carried out by family members or professional fraudsters. The use of deepfakes can also be employed to convince officials or authorities that the claimant is still alive, thereby increasing the level of fraud (Samani, 2022). In the metaverse, insurance activities have also expanded into the virtual world alongside banking activities (Generali, 2022).

3.3.3 New account fraud

This fraud involves criminals stealing someone else's identity or abusing that identity to open a bank account, particularly in the metaverse. The criminals create a false identity for the applicant and use it to open an account, successfully bypassing many of the verification processes typically applied by banking service providers. Once they have access to the account, criminals can use it for money laundering or accumulating debts with significant amounts.

3.3.4 Synthetic identity fraud

This type of fraud can also be considered one of the most advanced deepfake strategies because it is challenging to detect. Unlike identity theft, criminals typically combine fake and stolen information to create a completely new individual that does not exist (Samani, 2022). This new identity is then used to create credit cards and conduct other banking affairs. This should also be a particular concern for banking service providers in the metaverse.

In addressing the challenges in the virtual world, especially in the metaverse, the importance of cyber ethics and AI ethics is crucial to provide a framework for solutions in policies to minimize cybercrimes related to interpersonal deepfake, especially in the metaverse (Han, 2022). Also, the establishment of regulations governing banking transactions in the metaverse is essential. Regarding AI guidelines, several countries are still in the process of development, and Indonesia recently issued ethical guidelines for AI based on the circular from the Ministry of Communication and Informatics (Kominfo) Number 9 of 2023 to serve as a mitigation guide for AI usage.
3.4 BLOCKCHAIN AND ITS IMPACT ON FINANCIAL CRIME IN THE METAVERSE

Blockchain technology has been a driving force in the development of cryptocurrencies in recent years. Cryptocurrencies can be likened to a collection of binary data designed to serve as a medium of exchange, with ownership recorded in a secure public ledger. This ledger also employs a robust cryptographic system to protect the data of each transaction. While some cryptocurrencies emphasize their decentralized nature, some crypto schemes use validators to enhance security and maintenance. The "proof of stake" model allows token owners to stake their tokens and receive rewards proportionate to the amount they own. Another advantage of token ownership is the reduction of network costs, the creation of new tokens, and reward mechanisms (KATTERBAUER et al., 2022).

Among the main characteristics of cryptocurrencies, it is not issued by a central authority, unlike central banks that are adapting to digital currencies such as the euro and yuan. In essence, cryptocurrencies are not tied to a central authority and do not use decentralized control. This also opens up opportunities to minimize transaction costs and enables direct transactions without intermediaries (Reddy & Minnaar, 2018).

Even though the opportunities presented by cryptocurrencies are promising, on the other hand, criminal activities also exploit these opportunities. The decentralized and independent nature of cryptocurrencies poses its own challenges as it is difficult to trace, not passing through conventional banking or central banks. The lack of supervision over unvalidated transactions creates a loophole for criminal activities. For example, transactions using cash make all involved parties anonymous. For instance, the Indian government attempted to reduce crime and minimize transactions in the black market by demonetizing the 500 and 1000 INR banknotes. The assumption was that by eliminating these banknotes suddenly, criminals would have to declare and deposit their funds in banks, making it easier for authorities to track suspicious transactions (Sivathanu, 2018).

Despite efforts such as demonetization impacting the general public's economic difficulties, the benefits have not been fully realized. Some challenges lie in the abundance of illegal transactions stored in forms other than the banknotes themselves or already processed through the banking system. Wealth is held in various forms, including properties, foreign currencies, and industrial investments. However, criminals face a vulnerability because physical banknotes are issued by the relevant authorities, making it...
difficult to freely transfer funds. For example, almost all transactions in USD involve the SWIFT network with intermediaries in the United States. If a criminal is caught conducting a transaction, it can be canceled, and their funds can be frozen. While this is not entirely foolproof, it does help minimize criminal activities in banking transactions (KATTERBAUER et al., 2022).

Cryptocurrencies have their own uniqueness due to their decentralized nature, allowing two parties to engage in transactions directly without the presence of an intermediary to validate the transaction. For example, in a kidnapping situation, criminals might demand ransom to be paid in Bitcoin, which can later be exchanged or traded on the open market without any intervention or monitoring by authorities to review such transactions, as Bitcoin cannot be easily identified within the blockchain. This poses a challenging task for the authorities (Trozze et al., 2022).

The non-transparent and anonymous nature of the system opens up opportunities, especially for criminals. For example, in a cyber attack on the oil industry, criminals prefer cryptocurrency for their transactions due to its anonymous and undetectable nature, making it easy to convert or trade. Meanwhile, transactions using USD would only complicate matters for criminals (Teichmann & Falker, 2021).

Recommendations for institutions or governments involve addressing these challenges by creating specific regulations related to blockchain itself. This includes requiring name verification or ease of information for digital wallet providers and digital banks to identify their customers. Moreover, there should also be regulations governing virtual banking in the metaverse.

3.5 THE LEGAL PROTECTION AGAINST THE MISUSE OF DEEPFAKE TECHNOLOGY IN BANKING TRANSACTIONS IN THE METAVERSE

Regarding the protection against the misuse of AI deepfake technology, preventive measures can include raising awareness and promoting ethical practices when using technology, especially Artificial Intelligence. It is crucial to validate the accuracy of customer information, both in transaction validation and customer identity verification for each banking transaction in the metaverse. There is a need for continuous technological improvement and development to anticipate and minimize cyber and banking crimes. Collaboration between institutions and agencies is essential to preempt technological crimes in the banking sector (Anggara et al., 2022). For banking service
providers, ensuring the security of digital banking platforms in the metaverse is paramount to safeguarding customers’ personal data. Governments should review copyright laws and data protection regulations to accommodate the needs of the public conducting banking transactions in the metaverse, particularly in Indonesia. Establishing regulations specifically addressing the protection of personal data in the metaverse is crucial.

Repressive actions can involve reporting incidents to law enforcement to deter perpetrators of deepfake and digital crimes in the banking sector, especially in the metaverse. Government oversight and involvement from relevant agencies are necessary components of an effective strategy.

4 CONCLUSION

Based on the analysis related to the protection of transactions in the metaverse against deepfake technology, several conclusions can be drawn. Firstly, regulations governing banking transactions in the metaverse and blockchain vary from country to country, with some still in the developmental stage, including Indonesia. In Indonesia, existing regulations such as the ITE Law and the Financial Services Authority (OJK) regulations serve as a general legal framework but lack specific provisions for metaverse banking transactions. There is a need in Indonesia to review and reconstruct regulations or establish new ones specifically addressing the mechanisms of banking transactions in the metaverse and blockchain. Establishing an oversight institution to monitor transactions and creating tax regulations related to metaverse banking transactions and dispute resolution mechanisms is also essential. The implementation of Cyber Ethics is crucial to minimize cybercrime and financial crime in blockchain and the metaverse. Additionally, ethical considerations in the use of Artificial Intelligence are necessary to ensure compliance with the law. Regarding the legal protection against the misuse of deepfake technology in banking transactions in the metaverse in Indonesia, both preventive and repressive measures are essential. Preventive steps involve banking service providers ensuring the security of services and transactions in the metaverse. Regulatory bodies, particularly in Indonesia, need to review regulations related to the protection of personal data and copyright laws, as deepfake falls within the realm of copyright. Creating specific regulations that provide protection for customers in
metaverse banking is crucial. Repressive actions involve reporting incidents of deepfake crimes or other cybercrimes in metaverse banking to relevant authorities or institutions.
REFERENCES


TERDESENTRALISASI INDONESIAN LEGAL STUDY FOR CRYPTO ASSET AND BLOCKCHAIN.


