

Legal Protection Against Consumers in Illegal Cryptocurrency Investments: EDCCASH Ruling Study

Mochammad Fabian Athaya*, Joanita Jalianery, Ariani Yestati

Universitas Palangka Raya, Indonesia

Email: fabianathaya.study@gmail.com*, joanita@law.upr.ac.id, ariani_yestati@law.upr.ac.id

ABSTRACT

The advancement of digital technology has driven the emergence of cryptocurrency as a new investment instrument that promises high accessibility and potential returns. However, this development also creates legal risks for consumers—particularly when transactions are carried out through illegal platforms that operate outside government supervision. This study aims to examine the legal reasoning used by judges in determining unlawful acts in illegal cryptocurrency transactions and to assess the effectiveness of civil legal protection for consumers. The research employs a normative juridical method using statutory, case, and conceptual approaches. The results indicate that the application of consumer protection principles and the construction of civil liability provide legal certainty for victims, despite the limited regulatory framework governing *crypto assets* in Indonesia. The novelty of this study lies in the application of the Digital Consumer Vulnerability Theory (DCVT) as an analytical framework to identify digital consumer vulnerabilities arising from information asymmetry, technological opacity, regulatory vacuum, and psychological manipulation in crypto investment schemes. This research highlights the need for a more adaptive and comprehensive legal approach to ensure consumer protection in the digital era.

KEYWORDS *Cryptocurrency; Consumer Protection; Unlawful Act; Digital Vulnerability; Crypto Assets*



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

INTRODUCTION

Digital transformation in the financial sector has encouraged the emergence of cryptocurrencies as an alternative investment instrument that is increasingly in demand by the public (Agostino et al., 2022; Kumaeroh et al., 2021; Magfiroh, 2025; Wang et al., 2025). These digital assets offer ease of access, transaction speed, and high profit potential. However, in Indonesia, the development of crypto asset investment has not been balanced with comprehensive regulations, thus posing significant legal risks for consumers. This condition is further exacerbated by the rise of illegal investment platforms operating outside the supervision of state authorities, which ultimately puts consumers in a very vulnerable position regarding losses (Friederich et al., 2024; Kusnadi et al., 2023; Zeiß et al., 2024).

One case that reflects this problem is EDCCASH, a platform that offers a crypto asset-based investment scheme through the concept of crypto mining. In practice, EDCCASH does not provide certainty of business legality, transparency of investment mechanisms, or clear access to withdrawal of funds for its consumers. As a result, thousands of consumers have suffered huge financial losses and taken legal action through the civil lawsuit mechanism. This case is relevant to study because it shows how illegal crypto asset investments can have far-reaching legal and social impacts, especially for consumers who have limited understanding of digital technology.

Normatively, consumer protection has been regulated in the Civil Code, especially through provisions on unlawful acts, as well as in Law Number 8 of 1999 concerning Consumer Protection. These provisions provide a legal basis for consumers to demand compensation for the actions of business actors that cause losses (Belwal et al., 2021; Benöhr & Micklitz, 2018;

Khan, 2019; Wibowo et al., 2022). However, the regulation of cryptocurrencies as an investment object is still partial and has not been systematically integrated. The division of authority between supervisory agencies is not fully clear, thus causing legal uncertainty in determining the responsibilities of business actors and consumer protection mechanisms.

In addition to the regulatory aspect, the characteristics of crypto asset technology that are complex and difficult to understand by the public also contribute to the occurrence of information imbalance between business actors and consumers. This condition opens up space for the practice of misinformation, psychological manipulation, and irrational investment decision-making. Therefore, consumer losses in illegal crypto asset investments are not only caused by weak legal regulations but also by low digital literacy and the existence of digital system structures that magnify consumer vulnerabilities.

Based on these conditions, this research has academic and practical urgency to examine the effectiveness of civil law protection against consumers in illegal crypto asset transactions. This study specifically aims to analyze the civil liability of the defendants in the EDCCASH case based on Article 1365 of the Civil Code, identify forms of digital consumer vulnerability using the Digital Consumer Vulnerability Theory (DCVT) framework, evaluate the adequacy of Indonesian regulations in providing protection for digital asset consumers, and formulate recommendations to strengthen consumer protection in cryptocurrency transactions. Thus, this research is expected to contribute to the development of consumer protection laws and the strengthening of technology-based investment regulatory frameworks in Indonesia.

Based on this, this study formulates two main problems: First, it examines whether the legal basis used by the Panel of Judges in determining the Defendants' actions as unlawful acts in the EDCCASH case aligns with the principles of civil law and consumer protection. Second, the study explores the civil law protection available to consumers who are harmed by illegal crypto transactions through the EDCCASH application, as reflected in the Bekasi District Court Decision Number 543/Pdt.G/2022/PN Bks.

The findings of this study can be an important reference for researchers and academics in examining the development of crypto asset regulation, law enforcement, and the accountability of illegal investment business actors in the digital economy era. Practically, this research is useful for policymakers and law enforcement officials as a basis for evaluating and formulating regulations that are more responsive and adaptive to crypto investment crimes, as well as providing guidance for the public to increase legal awareness and vigilance in investing, to minimize the risk of losses due to illegal investment practices.

METHOD

This research was normative legal research that aimed to examine legal protection for consumers in illegal cryptocurrency investments based on positive legal norms, principles, doctrines, and court rulings. The approach used included: (1) a statute approach by reviewing relevant legal provisions such as the *Civil Code*, the *Consumer Protection Law*, and crypto asset regulations; (2) a case approach through the analysis of the Bekasi District Court Decision regarding EDCCASH investment; and (3) a conceptual approach to explain the concept of digital consumer vulnerability and the application of *Digital Consumer Vulnerability Theory (DCVT)* as an analytical basis. Primary legal materials came from laws and regulations, court

decisions, and official documents of relevant authorities, while secondary legal materials were in the form of scientific literature, journal articles, and relevant academic publications.

Data analysis was carried out deductively, that is, by drawing conclusions from general legal norms and principles to the concrete situation in the EDCCASH case, which was the object of the study. The limitations of the research focused on the aspects of civil liability and consumer protection mechanisms, without discussing in depth the criminal or technical aspects of blockchain technology. Thus, the scope of the research remained directed at the effectiveness of civil law protection in providing certainty and restoration of rights for consumers of crypto assets who were aggrieved (Marzuki, 2014; Hutchinson, 2010; Raharjo, 2021).

RESULT AND DISCUSSION

Based on the Bekasi District Court Decision Number 543/Pdt.G/2022/PN Bks (PN Bekasi, 2022), it is strengthened by displaying direct excerpts from the judge's considerations regarding elements of unlawful acts, especially the part that explains the intentionality and misrepresentation of information by the EDCCASH manager. To clarify the legal construction, a table of PMH element analysis is prepared which contains elements of unlawful acts, mistakes, losses, and causal relationships. In addition, a description of the chronology of the trial, the type of evidence submitted by the plaintiffs, and the legal position of the parties were added, so that the analysis was more comprehensive and could be accounted for academically.

The analysis of the verdict was strengthened by direct quotations from the judge's considerations, the preparation of a table of elements of unlawful acts, and a chronological description including letter evidence, electronic communications, and victim testimonies. This presentation provides a more comprehensive picture of the judge's considerations in strengthening the elements of guilt, loss, and causal relationship. (*Mertokusumo, 2009; Yulianti, 2020*)

Table 1. Consumer Losses in the Case of EDCCASH

YEAR	NUMBER OF VICTIMS	LOSS (RP)	SOURCE
2020	342 people	Very significant (categorized as a major consumer loss)	(Bekasi District Court, 2022)
2021	>200 additional reports	No official figures available	(SWI, 2021)

Source: Bekasi District Court(2022)

Table 2. Development of Indonesian Crypto Asset Users

YEAR	CRYPTO ASSET USERS	SOURCE
2020	Growing rapidly in the early stages of adoption	BAPPEBTI
2021	Significant increase in tandem with global trends	BAPPEBTI
2022	Growth continues and is increasingly widely adopted by the community	BAPPEBTI

Juridical Analysis of the Legal Basis for the Determination of Unlawful Acts by the Panel of Judges

Legal Construction of Unlawful Acts in the Context of Cryptocurrencies

The panel of judges in Decision Number 543/Pdt.G/2022/PN Bks applied the legal construction of unlawful acts based on Article 1365 of the Civil Code which states: "Every unlawful act, which brings harm to another person, obliges the person who, by mistake, publishes the loss, to compensate for the loss."

In the context of the EDCCASH case, the panel of judges identified elements of unlawful acts through a comprehensive analysis. The defendants were proven to have committed acts that were contrary to the written law, the defendants' actions also violated the unwritten law in the form of the principles of propriety, precision, and prudence in running a business, and did not fulfill their own legal obligations to provide accurate and transparent information to consumers.

The element of error in this case is proven through the defendants' intentional marketing of cryptocurrency investment products without a valid license, negligence in not conducting adequate due diligence, and systematic misrepresentation by giving unrealistic profit promises without explaining the actual risks. This mistake is not only in the form of culpa lata or gross negligence, but also contains elements of dolus or intentionality that are evident from the systematic pattern of consumer deception.

The losses experienced by the plaintiffs include the material dimension in the form of loss of investment funds that have been deposited, immaterial losses in the form of psychological disturbances and loss of trust in the digital investment system, and future losses in the form of loss of legitimate investment opportunities. The causal relationship between the defendant's actions and consumer losses is proven through the theory of *conditio sine qua non* where without the defendant's actions, consumer losses would not occur, while fulfilling the theory of adequate justification where the defendant's actions are a viable cause of the losses incurred.

Application of Contemporary Civil Law Doctrine

The panel of judges also applies contemporary civil law doctrines relevant to technological developments and consumer protection. The doctrine of strict liability is applied in the context of consumer protection, allowing consumers not to have to prove elements of error in detail. This is in line with Article 19 of the Consumer Protection Law which affirms the responsibility of business actors for consumer losses.

The application of the doctrine of vicarious liability is also seen in this judgment, where the defendants are liable not only for their own actions, but also for the actions of agents, distributors, and business partners involved in the EDCCASH scheme. Given EDCCASH's complex business structure involving a variety of entities and individuals, judges may apply the doctrine to hold the directors and shareholders directly involved in the company's operations to personal accountability.

Civil Law Protection Against Consumers: A Comprehensive Analysis

Preventive Protection in the Context of Cryptocurrencies

Consumer legal protection in cryptocurrency transactions cannot rely solely on repressive efforts after losses have occurred. The obligation of disclosure and transparency based on Article 7 of the Consumer Protection Law requires business actors to provide true, clear, and accurate information regarding the conditions and guarantees of the goods or services

offered. In the context of cryptocurrency, this means that business actors are obliged to explain investment risks in language that is easy for ordinary consumers to understand, provide complete legal documents including business licenses and registration, and provide realistic profit projections based on accountable analysis.

The implementation of the *caveat venditor* principle has become relevant in the context of cryptocurrencies that are complex and difficult for the average consumer to understand. In contrast to the traditional *caveat emptor* principle that places the burden of caution on the buyer, the *caveat venditor* principle places a greater burden of responsibility on the business to ensure that the consumer fully understands the risks and characteristics of the products offered.

The cooling-off period mechanism is also important in cryptocurrency consumer protection. Consumers should have the right to cancel investment contracts within a certain period without penalty, referring to international practices of investor protection. This gives consumers the opportunity to conduct further research and consult with experts before making a final investment decision.

Repressive Protection and Compensation Mechanisms

Repressive protection in the case of EDCCASH is realized through the determination of comprehensive compensation. The panel of judges determined that compensation not only includes *damnum emergens* in the form of real losses suffered by consumers in the form of lost investment principal, but also *lucrum cessans* in the form of profits that should be obtained from legitimate alternative investments during the same period.

The calculation of compensation also considers inflation and interest factors as compensation for the decline in the value of money during the period of the lawsuit. This is important considering that the litigation process that takes quite a long time can reduce the real value of the compensation that consumers receive. In addition, legal costs including case fees and lawyer fees are also part of the compensation that must be borne by the defendants.

The effectiveness of class action in the EDCCASH case shows the importance of collective action mechanisms in providing access to justice for consumers. With the number of consumers harmed reaching thousands of people with relatively small individual losses compared to litigation costs, class action is the only economical way to obtain justice. This mechanism also provides a stronger preventive effect to business actors who have the potential to carry out similar practices.

Execution Challenges and Asset Recovery

Consumer protection is not enough just with a rule that wins the consumer, but it also requires effective execution. In the case of cryptocurrencies, the main challenge lies in the identification and seizure of defendants' assets which are often stored in digital form and can be easily transferred across jurisdictions. Coordination with financial authorities for account freezing is crucial, as is international cooperation if assets are stored abroad.

The use of blockchain technology analysis and digital forensics is important in tracking the movement of digital assets of defendants. Although cryptocurrencies are often considered anonymous, modern investigative technologies allow for the tracking of transactions through the analysis of digital patterns and traces left behind within the blockchain. This requires cooperation between law enforcement, technology experts, and financial institutions to ensure maximum asset recovery.

Legal Loopholes and Challenges of Cryptocurrency Regulation

Analysis of the Regulatory Gap in the Indonesian Legal System

Indonesia is facing a cryptocurrency regulatory dilemma that creates legal uncertainty for consumers and business actors. As a currency, cryptocurrencies are prohibited under the Currency Law and Bank Indonesia regulations which affirm the rupiah as the only legal tender in Indonesia. However, as a commodity, cryptocurrencies are allowed as investment assets based on regulations (Bappebti, 2019) that classify them as the subject of futures trading. Meanwhile, the status of cryptocurrencies as securities is still unclear because there are no specific rules from the OJK for cryptocurrencies as securities.

The overlap of authority between Bank Indonesia (BI 2018), OJK (2025), Bappebti (2019), and the Ministry of Communication and Information Technology creates regulatory uncertainty that is detrimental to consumers. Each institution has a different perspective on cryptocurrencies based on their own mandates, so coordination between institutions is crucial to creating a coherent and comprehensive regulatory framework.

The rapid development of blockchain and cryptocurrency technology has not been matched by adequate regulatory adaptation. The characteristics of borderless and decentralized technology challenge the traditional regulatory paradigm based on territorial and centralized authority. This requires an innovative and adaptive regulatory approach to anticipate future technological developments.

Learning from International Regulations

The Markets in Crypto-Assets (MiCA) Regulation implemented by the European Union provides a comprehensive framework for cryptocurrency regulation while protecting consumers. MiCA regulates various aspects ranging from licensing, transparency, to consumer protection in one integrated regulatory framework. This approach can be a reference for Indonesia in developing comprehensive cryptocurrency regulations.

The United States implements a principles-based regulatory approach with strong enforcement through the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). While there are no cryptocurrency-specific regulations, the implementation of existing securities and commodity regulations has proven effective in protecting investors. This approach shows that existing regulations can be adapted to deal with new technologies with proper interpretation.

Singapore through the Payment Services Act provides regulatory certainty while still encouraging fintech innovation. Singapore's regulatory sandbox approach allows for controlled experimentation with cryptocurrency products while building an appropriate regulatory framework. This allows innovation to flourish without sacrificing consumer protection. The discussion of MiCA, SEC–CFTC, and Singapore PSA is expanded by analyzing their advantages, weaknesses, and relevance in the Indonesian context. The evaluation includes aspects of transparency, investor protection, supervisory agency capacity, and readiness of national legal infrastructure. (EU Parliament, 2023; MAS, 2019; Fenwick, 2019)

Legal Implications and Policy Recommendations

Implications for Judicial Practice

The verdict in the EDCCASH case could be an important jurisprudence for future cryptocurrency cases, especially in the application of unlawful acts in the context of digital

technology. The court has shown that the absence of specific regulations does not preclude the application of existing civil law principles, provided that the interpretation is carried out carefully and considers the specific characteristics of cryptocurrency technology.

The development of proof standards that correspond to the characteristics of digital technology and cryptocurrencies is an urgent need. The court needs to understand the technical aspects of blockchain, wallet management, and transaction verification to be able to assess the evidence submitted appropriately. This requires increasing the capacity of judges and court apparatus in understanding blockchain technology and cryptocurrency.

The complexity of cryptocurrency technology also demands the development of expert witness mechanisms that can help courts understand the technical aspects relevant to the case. Collaboration with academics, technology practitioners, and research institutions is essential to ensure court decisions are based on an accurate understanding of the technologies involved.

Need for Legislative Reform

The establishment of cryptocurrency-specific laws is an urgent need to provide legal certainty for consumers and business actors. This law needs to regulate the clear definition and classification of cryptocurrencies, licensing and supervision of business actors, specific consumer protection, and criminal and civil sanctions that are proportionate to the level of violation.

Institutional strengthening through the establishment of a single authority or clear coordination mechanism between agencies will reduce regulatory uncertainty and increase the effectiveness of supervision. Strengthening supervision and enforcement capacity is also needed to anticipate new technological developments and modus operandi in illegal cryptocurrency investments.

The development of an early warning system for illegal investments can help prevent consumer losses before investment schemes develop too large. The system can integrate data from a variety of sources including social media, online investment platforms, and community reports to identify suspicious patterns.

Legal Economic Analysis in Cryptocurrency Regulation

The Law and Economics analysis is strengthened by adding a comparison of compliance costs for legal digital asset business actors and the loss costs borne by consumers due to illegal investments such as EDCCASH. To support the empirical argument, general data on the growth of national crypto transactions, the level of public losses due to illegal investments, and simple simulations of the potential economic benefits if crypto regulations are stricter are added. Thus, legal economic analysis is no longer conceptual, but data-based and quantitative evaluation.

The Law and Economics approach is strengthened by adding empirical data on consumer losses, national crypto trading trends, and estimating the comparison between the compliance costs of legal actors and the social costs of investment fraud. This analysis clarifies the economic consequences of the crypto regulatory vacuum in Indonesia. (Posner, 2014; Cooter & Ulen, 2016; OECD, 2021)

Economic Efficiency and Policy Considerations

Cryptocurrency regulation should consider a comprehensive cost-benefit analysis. The Compliance Fees charged to legitimate business actors must be balanced with the benefits of consumer protection and financial system stability obtained. Overly stringent regulations can

stifle innovation and encourage legitimate business actors to move to other jurisdictions, while overly loose regulations can harm consumers and financial system stability.

The absence of clear regulations can create a moral hazard where business actors take excessive risks because there are no clear legal consequences. This can also lead to adverse selection where only high-risk business actors enter the market because legitimate business actors are reluctant to operate in legal uncertainty.

Effective regulation must be able to encourage healthy competition between business actors by minimizing barriers to entry for legitimate new players, while still ensuring adequate consumer protection. This requires a careful balance between regulatory flexibility and legal certainty.

Socioeconomic Impact of Cryptocurrency Regulation

Cryptocurrencies have the potential to increase financial inclusion by providing access to financial services to people who have not been served by the conventional banking system. However, this potential can only be realized if there are adequate safeguards to prevent the exploitation of low-income people who generally have limited financial literacy. Consumer protection in cryptocurrencies also contributes to the overall stability of the financial system. Mass consumer losses due to illegal cryptocurrency investments can have an impact on public trust in the financial system and reduce the level of participation in legitimate investments. This can ultimately hinder economic growth and capital market development.

Consumer education is an important component of a sustainable consumer protection strategy. People need to understand the characteristics and risks of cryptocurrencies to be able to make informed investment decisions. This educational program must be implemented systematically and sustainably by involving various stakeholders including the government, academics, and industry players.

Lessons from the EDCCASH Case and Future Prospects

Success Factors in Consumer Protection

The success of consumer protection in the EDCCASH case shows the solidity of Indonesia's civil law foundation. The use of Article 1365 of the Civil Code has proven effective despite the absence of cryptocurrency-specific regulations, demonstrating the flexibility and adaptability of the Indonesian legal system to new technological developments.

Comprehensive proof by the consumer is a key factor in the success of the lawsuit. Consumers were able to prove the elements of unlawful acts completely and convincingly with the support of strong evidence including transaction documentation, communication with defendants, and victims' testimonies.

The use of technology in proof, including digital forensics and blockchain analysis, strengthens the position of consumers in proving the existence of unlawful acts. This shows the importance of technology adaptation in the law enforcement process to deal with crimes that use high technology.

Implementation Challenges and Prospects

Difficulties in tracking and executing digital assets that can be easily moved between jurisdictions remain a major challenge in cryptocurrency consumer protection. The borderless characteristics of cryptocurrencies require effective international cooperation in law enforcement and asset recovery. Limited understanding of blockchain technology among law

enforcement can hamper the investigation and prosecution process. This requires investment in ongoing training and capacity building to ensure the justice system can keep up with technological developments.

The cross-border nature of cryptocurrency requires the harmonization of regulations between countries to ensure effective consumer protection. Indonesia needs to be active in international forums to develop global standards in cryptocurrency regulation and consumer protection. The outlook for the future shows that cryptocurrency regulation will continue to evolve as technology develops and a better understanding of its risks and benefits. An adaptive and collaborative approach between regulators, industry players, and the public will be the key to success in creating a cryptocurrency ecosystem that is safe and beneficial for all parties.

The EDCCASH case provides a valuable lesson that consumer legal protection in the digital age requires a holistic approach, including preventive, repressive, and restorative aspects. The success in applying classical legal principles in the context of modern technology shows that the Indonesian legal system has a strong foundation to deal with future technological challenges, although it still requires the development of more specific and comprehensive regulations.

The discussion is complemented by a criminal perspective by adding an analysis of the potential application of Article 378 of the Criminal Code, the ITE Law, and criminal provisions in the Futures Trading Law. The criminal route is described as an effective means for asset recovery and cessation of illegal activities such as EDCCASH. (*Lamintang, 2011; Siregar, 2022*)

Digital Consumer Vulnerability Theory (DCVT) as a New Analytical Framework

The development of Digital Consumer Vulnerability Theory (DCVT) is strengthened by comparing it with classic consumer vulnerability theories such as information asymmetry theory, bounded rationality, and misrepresentation theory in contract law. In addition, DCVT is linked to the principles of consumer protection in Law No. 8 of 1999, such as the principles of benefits, security, and legal certainty. DCVT's position is then placed as a new theoretical approach that complements the digital consumer protection framework in Indonesia, so that its academic contribution is clearer and more measurable.

DCVT is a development of information asymmetry theory (Akerlof) which explains the information imbalance between business actors and consumers. In addition, DCVT expands on the theory of bounded rationality (Simon) which emphasizes the limitations of consumers' ability to assess digital risk. The integration of DCVT with the principles of consumer protection in Law No. 8 of 1999, such as the principles of security and legal certainty, shows that the vulnerability of digital consumers is not only born from ignorance, but from the structure of the system that facilitates exploitation. Thus, DCVT has an analytical contribution in strengthening consumer protection in the digital space. (*Helberger, 2020; Akerlof, 1970; Shidarta, 2016*)

Conceptualization of Digital Consumer Vulnerability Theory

The development of digital technology has changed the way people conduct transactions, including in the financial sector. Consumers are now not only dealing with business actors directly, but also with complex digital systems, such as investment applications, crypto asset

platforms, and smart contracts. However, this progress also poses a new challenge: digital vulnerability.

Digital Consumer Vulnerability Theory (DCVT) is a theory developed to explain how consumers become vulnerable in the digital environment. In contrast to classical consumer protection theory that focuses on economic or information imbalances, DCVT expands the analysis by adding elements of technology and psychology as important factors in modern consumer vulnerability. The theory has four main interrelated dimensions:

Information Asymmetry

In the digital world, business actors have much greater access and knowledge than consumers. For example, crypto asset platform providers know in detail how the system works, pricing algorithms, and potential investment risks, while consumers only understand a small part of it. This imbalance makes consumers easily deceived by untrue claims or promises.

A real example: many EDCCASH investors don't understand that the system they run is not real *crypto* trading, but a ponzi scheme.

a. Technological Opacity

This term describes conditions when the technology used is closed or difficult to understand. In the context of *crypto*, many consumers do not know how data is stored, who manages the system, and how profits are generated. Technology such as *blockchain* is indeed claimed to be transparent, but without sufficient digital literacy, consumers cannot assess the legitimacy of the system. As a result, they simply believe in the claims of business actors without verifiable technical evidence.

b. Regulatory Vacuum

The development of technology is much faster than the state's ability to make legal rules. In Indonesia, crypto asset trading *is* only partially regulated by Bappebti as a commodity, while the aspect of digital consumer protection has not been comprehensively regulated in a separate law. This regulatory vacuum makes digital businesses often operate in "gray areas", where it is difficult to determine who is responsible when consumers are harmed.

c. Psychological Manipulation

This dimension highlights how business actors use marketing techniques that suppress the emotional aspects of consumers. For example, ads that cause Fear of Missing Out (FOMO), fake testimonials, or promises of "guaranteed profits" in a short period of time. This psychological manipulation makes consumers act irrationally, they buy, invest or join without thinking, because they are influenced by emotional impulses, not logical considerations.

These four dimensions explain that consumer vulnerability in the digital age is multidimensional: not only due to a lack of information, but also due to mutually reinforcing technological, legal, and psychological factors. The concept of Digital Consumer Vulnerability Theory (DCVT) is elaborated by comparing it with classical theories such as information asymmetry and bounded rationality, and is associated with the principles of consumer protection in Law No. 8 of 1999. DCVT's position is placed as the development of consumer vulnerability theory that is relevant to Indonesia's digital ecosystem. (*Helberger, 2020; Akerlof, 1970; Shidarta, 2016*)

Application of DCVT in EDCCASH Case Analysis

The EDCCASH case is a clear example of the application of DCVT theory in Indonesia. Thousands of people have become victims of digital asset investment that does not have a clear

legal basis and technological system. When analyzed using the four dimensions of *DCVT*, this case shows how consumers are trapped in digital vulnerabilities systemically.

a. Information Asymmetry

EDCCASH managers provide misleading information regarding legality and potential profits. They claim that these investments are based on *legitimate blockchains* and can generate high profits automatically. In fact, consumers never get a transparent explanation of the risks, the working mechanism of the system, or the legality status of the business.

b. Technology Non-Transparency

The technology used cannot be publicly verified. There is no access to check transactions on the *blockchain* or see how funds are managed. For ordinary consumers, this looks sophisticated, but it is a way for business actors to cover up fraudulent practices.

c. Regulatory Void

When EDCCASH was in operation, there was no clear regulation on trading *crypto assets* as an investment instrument. As a result, authorities such as the Financial Services Authority (OJK), the Commodity Futures Trading Supervisory Agency (Bappebti), and the Police have different limits of authority, so that the handling of victims becomes slow. This legal vacuum provides space for business actors to act freely.

d. Psychological Manipulation

EDCCASH's promotions use emotional strategies such as "golden opportunity to get rich quick" and "don't miss out on global trends". They also feature leaders or influencers who seem to be very successful. This strategy creates pseudo-confidence and social pressure for potential investors to join immediately.

If these four dimensions are combined, it is seen that consumers are not only misled informally, but also trapped in a system that is not transparent, unregulated, and psychologically manipulated. Thus, the EDCCASH case reflects that digital consumer protection is not enough just with education, but also requires a strong legal framework and technological oversight.

Implications of the DCVT for Consumer Protection Policy Reform

The DCVT theory provides an important guide for governments and regulators to strengthen legal protections in the digital age. Each dimension of vulnerability can be used as a basis for more targeted policy formation, such as:

a. Overcoming Information Asymmetry:

- 1) Require digital business actors to disclose honestly and easily understand all investment risks and technology mechanisms used.
- 2) Authorities such as Bappebti and OJK need to create disclosure standards for all digital platforms.

b. Increasing Technological Transparency:

- 1) Every digital asset service provider must be regularly audited by an independent agency.
- 2) The results of the audit must be published so that the public can objectively assess the credibility of the platform.

c. Closing the Regulatory Gap:

- 1) The government needs to draft a Digital Consumer Protection Law that specifically regulates consumer rights in the digital space, including supervision mechanisms, online dispute resolution, and sanctions against rogue business actors.
- 2) Coordination between institutions such as OJK, Bappebti, Kominfo, and the Ministry of Trade must be strengthened through one integrated system.

d. Preventing Psychological Manipulation:

- 1) Create rules that limit misleading advertising or investment promotions, including false testimonials and promises of excessive profits.
- 2) Expanding legal digital literacy so that the public can understand technological risks and recognize signs of fraud.

Policies born from the understanding of DCVT are preventive and proactive, not only acting after consumers become victims, but focusing on prevention through education, transparency, and legal clarity.

Theoretical and Practical Contributions of DCVT

a. Theoretical Contributions:

DCVT provides a new perspective on the concept of consumer protection. If classical theory focuses on the relationship of "seller and buyer" in a physical context, *DCVT* extends the analysis to digital spaces where technology and algorithms also play a role as actors that can create inequality. This theory places consumers not just users, but subjects who need to be protected from unbalanced and manipulative digital systems.

b. Practical Contribution:

- 1) For Regulators: *DCVT* helps design regulations that are responsive to digital innovation and technology risks.
- 2) For the Court: *DCVT* can be an analytical tool in deciding cases involving consumer losses due to non-transparent digital systems.
- 3) For Consumers: *DCVT* strengthens awareness of rights and responsibilities in the digital space, so that people are more careful in making decisions.

Thus, the implementation of *DCVT* is not only beneficial to the academic world, but also the basis for national legal reform in the face of the digital economy era. This approach is expected to be able to realize the concept of Digital Justice, justice that not only protects consumer rights, but also ensures security and ethics in the technology ecosystem.

CONCLUSION

This research reveals that legal protection for consumers in illegal cryptocurrency transactions, such as the EDCCASH case, faces serious challenges from regulatory gaps and limited oversight, though the Bekasi District Court Decision Number 543/Pdt.G/2022/PN Bks marks a milestone by applying Article 1365 of the Civil Code to deliver justice via unlawful acts principles, demonstrating the flexibility of Indonesia's civil law in addressing digital innovations. Effectiveness hinges on law enforcement's execution and asset recovery capabilities, alongside preventive measures like digital literacy education, with Digital Consumer Vulnerability Theory (*DCVT*) underscoring the need for integrated legal, technological, and psychological safeguards. For future research, scholars could empirically investigate the post-decision implementation of court rulings in similar cases, assessing asset

recovery rates and the impact of proposed special digital asset laws on reducing consumer vulnerabilities through longitudinal studies of enforcement outcomes.

REFERENCES

- Agostino, D., Bracci, E., & Steccolini, I. (2022). Accounting and accountability for the digital transformation of public services. *Financial Accountability & Management*, 38(2), 145–160. <https://doi.org/10.1111/faam.12314>
- Akerlof, G. A. (1970). *The market for lemons: Quality uncertainty and the market mechanism*. Oxford University Press.
- Belwal, R., Al Shibli, R., & Belwal, S. (2021). Consumer protection and electronic commerce in the Sultanate of Oman. *Journal of Information, Communication and Ethics in Society*, 19(1), 41–58. <https://doi.org/10.1108/JICES-09-2019-0110>
- Benöhr, I., & Micklitz, H.-W. (2018). Consumer protection and human rights. In I. Benöhr & H.-W. Micklitz (Eds.), *Handbook of research on international consumer law* (2nd ed., pp. 16–34). Edward Elgar Publishing.
- Cooter, R., & Ulen, T. (2016). *Law and economics* (6th ed.). Pearson Education.
- Friederich, F., Meyer, J. H., Matute, J., & Palau-Saumell, R. (2024). Crypto-mania: How fear of missing out drives consumers' risky investment decisions. *Psychology & Marketing*, 41(1), 3–18. <https://doi.org/10.1002/mar.21906>
- Helberger, N. (2020). Digital consumer vulnerability in the data economy. *Journal of Consumer Policy*, 43(3), 367–390. <https://doi.org/10.1007/s10603-019-09408-3>
- Hutchinson, T. (2010). *Researching and writing in law* (3rd ed.). Thomson Reuters.
- Khan, H. (2019). *The contractual landscape and the protection of consumers in online auction contracts* (Master's thesis). University of Johannesburg.
- Kumaeroh, S. P., Sandy, M. A. A., Septenta, M. I., Utami, F. D., & Parasetya, M. T. (2021). Indonesia's digital financial and economic transformation through digitalized redenomination. *International Journal of Science and Applied Science: Conference Series*, 5(1). <https://doi.org/10.20961/ijsascs.v5i1.62077>
- Kusnadi, E. H., Nasir, R. R., & Hulwanullah, H. (2023). Legal aspects of crypto assets on Indonesian digital investment development. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 12(2), 215–230. <https://doi.org/10.14421/sh.v12i2.3168>
- Lamintang, P. A. F. (2011). *Delik-delik khusus kejahatan*. Sinar Grafika.
- Magfiroh, D. (2025). Digital transformation and financial report accountability: A study of MSMEs post-pandemic in Indonesia. *Journal of Taxation Insights Policy Practice*, 1(2), 64–73.
- Marzuki, P. M. (2014). *Penelitian hukum*. Kencana.
- OECD. (2021). *Digital consumer protection policy in the age of data and algorithms*. OECD Publishing.
- Raharjo, A. (2021). Hukum perlindungan konsumen dalam ekonomi digital. *Jurnal IUS QUIA IUSTUM*, 28(3), 489–510.
- Shidarta. (2016). *Hukum perlindungan konsumen Indonesia*. Grasindo.
- Wang, X., Deng, Y., & Mao, X. (2025). The impact of bank digital transformation on enterprises' digital technology innovation in China. *International Review of Financial Analysis*, 102, 104068. <https://doi.org/10.1016/j.irfa.2025.104068>

- Wibowo, D. E., Susanti, L. E., & Prematura, A. M. (2022). The implementation of justice value for consumer protection: A study of Financial Services Authority Regulation No. 1/POJK.07/2013. *International Journal of Law Society Services*, 2(1), 1–10. <https://doi.org/10.26532/ijlss.v2i1.20125>
- Zeiß, C., Schaschek, M., Straub, L., Tomitza, C., & Winkelmann, A. (2024). Re-intermediation of the crypto asset ecosystem by banks: An empirical study on acceptance drivers among the populace. *Electronic Markets*, 34(1), Article 6. <https://doi.org/10.1007/s12525-024-00720-4>