INTEGRATING CRIMINAL LAW ENFORCEMENT AND THE CIVIL VALIDITY OF SMART CONTRACTS: A LEGAL ANALYSIS OF CRYPTO-ASSET-BASED SCAMMING CRIMES IN INDONESIA

Bambang Julianto[1*], Rabith Madah Khulaili Harsya[2], Andi Mohammad Galib[3], Dani Amran Hakim[4], Aklima[5]
Universitas Muhammadiyah Kendal Batang, Indonesia[1]
UIN Siber Syekh Nurjati Cirebon, Indonesia[2]
Universitas Pamulang, Indonesia[3]
UIN Raden Intan Lampung, Indonesia[4]
UIN Ar-Raniry, Indonesia[5]
Email : bambangjulianto.law@gmail.com

Abstract

The evolution of blockchain technology has introduced smart contracts as autonomous and immutable digital transaction instruments. However, these technical characteristics create legal ambivalence when used as a means of fraudulent acts based on crypto assets. This study aims to analyze the integration of criminal law enforcement and the civil validity of smart contracts in the context of crypto crimes in Indonesia. Using normative legal research methods and a comparative approach, this study finds a legal gap in determining the civil status of contracts born of malicious intent (mens rea). The analysis shows that although smart contracts are technically valid in blockchain systems, they can be invalidated under civil law if proven to contain elements of fraud. This study recommends the need for regulatory synchronization between the ITE Law, the National Criminal Code, and civil contract law to provide comprehensive legal protection for crypto asset investors in Indonesia.

Keywords: *Smart Contract, Crypto Assets, Digital Fraud, Law Enforcement, Civil Validity.*

1. INTRODUCTION

At the core of these digital transactions lies the "smart contract"—a piece of computer code designed to automatically execute, control, or document legally relevant events and actions according to the terms of a contract or an agreement. From a management and efficiency perspective, smart contracts offer unparalleled speed and cost-reduction by eliminating third-party verification. Nevertheless, from a legal standpoint, the "code is law" mantra often conflicts with established legal doctrines. The primary challenge arises when a smart contract is intentionally coded to facilitate a "rug pull" or other forms of scamming, where the technical execution is flawless, but the underlying intent is purely criminal. In such cases, the technical immutability of the blockchain acts as a double-edged sword, protecting the fraudulent transaction from being easily reversed by legal authorities (Bagaskoro et al., 2023).

The rigidity of traditional legal enforcement in Indonesia often struggles to categorize the dual nature of smart contracts. On one hand, a scamming operation is a clear violation of criminal statutes, specifically those concerning fraud and electronic crimes under the ITE Law. On the other hand, the transfer of assets through a smart contract constitutes a civil agreement. The existing legal gap lies in the transition between a criminal verdict and the civil recovery of assets. If a judge declares a transaction as part of a criminal scam, the civil status of the contract that facilitated the transfer must also be addressed to allow for the restoration of property rights (*restitutio in integrum*). Without a clear integration between these two legal realms, victims are often left with a paper victory in criminal court but no practical way to reclaim their digital property (Sipayung et al., 2025).

In the Indonesian Civil Code (KUHPerdata), Article 1320 stipulates four essential conditions for the validity of a contract: consent, capacity, a specific object, and a lawful cause (*legally halal*). When a smart contract is used as a vehicle for scamming, it fundamentally lacks a "lawful cause," making it legally void from its inception. However, the execution of this legal principle on a decentralized network is technically complex. Because blockchain transactions are irreversible by design, a court order declaring a smart contract "void" does not automatically trigger a return of assets. This technical-legal paradox requires a new standard of judicial intervention where the law must not only interpret the code but also command technical remedies through service providers or digital forensic execution (Marzuki, 2021).

Furthermore, the rise of crypto-asset-based crimes in Indonesia exposes the vulnerability of the current regulatory framework managed by Bappebti. While administrative regulations focus on the licensing of exchanges, they often overlook the substantive legality of the automated contracts used within those platforms. A scamming scheme often utilizes "backdoors" in the smart contract code—such as hidden minting functions or liquidity withdrawal blocks—which the average investor cannot read or understand. This creates a massive information asymmetry, where the principle of *caveat emptor* (let the buyer beware) is no longer sufficient. Therefore, legal analysis must evolve to recognize that a contract hidden behind complex, unreadable code may constitute a form of "undue influence" or fraud under civil doctrine (Sari et al., 2022).

The integration of criminal enforcement and civil validity is also essential for establishing a cohesive "Cyber-Risk Management" strategy for the nation's digital economy. If the Indonesian legal system fails to provide a synchronized response to crypto-scams, it risks losing public trust in digital innovation. From a governance perspective, the state must ensure that criminal prosecution of crypto-scammers is accompanied by civil mechanisms that allow for the freezing and seizing of assets at the protocol level where possible. This requires an interdisciplinary approach where legal professionals work alongside blockchain forensics experts to translate "criminal intent" into "civil invalidity" that can be recognized by global exchanges and digital custodians (Lisi, 2023).

Moreover, the New National Criminal Code (Law No. 1 of 2023) introduces broader definitions for computer-related fraud, but its effectiveness depends heavily on how the judiciary interprets digital evidence. In crypto-scamming cases, the "contract" itself is the primary evidence. If the court refuses to look past the technical execution and ignore the fraudulent intent embedded in the code, the law remains toothless. The reconstruction of legal standards is necessary to treat smart contracts not just as code, but as a manifestation of a legal act that must comply with the overarching values of justice and honesty found in Indonesian jurisprudence (Kurnia, 2023).

Ethical considerations also play a pivotal role in this analysis. The "permissionless" nature of blockchain often attracts those who believe they are "above the law" simply because they operate in a decentralized space. However, the Indonesian legal system, rooted in the principle of the rule of law (*Rechtsstaat*), cannot allow a technological tool to bypass the protection of individual property rights. The civil validity of a smart contract must always be subordinate to the moral and legal standards of the state. When a contract is used to steal, its "smartness" does not exempt it from being declared a "legal nullity." This philosophical stance is crucial for judges when deciding cases that involve complex algorithmic manipulations (Ibrahim, 2008).

The urgency of this research is further highlighted by the increasing number of victims who fall prey to sophisticated "phishing" and "social engineering" attacks that culminate in the signing of malicious smart contracts. These victims often face secondary trauma when they realize that the law provides no clear path for the recovery of their life savings. By analyzing the intersection of criminal and civil law, this study seeks to provide a roadmap for law enforcement agencies and the judiciary to handle these cases with greater precision. The goal is to move towards a system where the "Civil Validity" of a transaction is automatically challenged the moment "Criminal Activity" is proven, thereby creating a more hostile environment for scammers operating within Indonesian jurisdiction (Soekanto, 2015).

Ultimately, this paper argues that the future of Indonesia's digital economy depends on its ability to harmonize code with law. The integration of criminal and civil legal frameworks is not just a theoretical necessity but a practical requirement for the protection of millions of crypto-investors. By establishing a clear legal doctrine regarding the invalidity of fraudulent smart contracts, Indonesia can lead the way in creating a dignified and secure digital marketplace. This research serves as a foundational call to action for regulators to bridge the gap between technological advancement and substantive justice (Sipayung & Subandi, 2023).

2. RESEARCH METHODS

This study uses a normative legal research method, often referred to as library research or doctrinal research. The main focus of this method is to examine positive legal norms, legal principles, and the vertical and horizontal synchronization between regulations governing information technology and conventional law. The normative approach was chosen because the main problem in crypto-asset-based *scamming* crimes lies in the ambiguity of the interpretation of articles in the Civil Code, the ITE Law, and the National Criminal Code regarding the technical characteristics of autonomous *smart contracts (Soekanto, 2015). This study aims to determine the truth of coherence, namely whether smart contract* norms are coherent with the principles of valid agreements in the Indonesian legal system.

The approaches used in this study include a statutory approach, a conceptual approach, and a comparative approach. Through this statutory approach, the researcher examines the consistency between Article 1320 of the Civil Code concerning the legal requirements of an agreement, the crypto asset trading regulations issued by Bappebti, and the crime of fraud in Law No. 1 of 2023. Meanwhile, the conceptual approach is used to construct legal arguments regarding the position of *smart contracts* as objects of civil law that can be canceled if they contain criminal elements (Marzuki, 2021). The comparative approach is carried out on a limited basis by examining how other jurisdictions handle the "legality of code" in cyber fraud cases to provide recommendations for strengthening the law in Indonesia.

The legal materials used consist of primary, secondary, and tertiary legal materials. Primary legal materials include the Civil Code (BW), the National Criminal Code (Law No. 1/2023), the Electronic Information and Transactions Law (Law No. 11/2008 in conjunction with Law No. 1/2024), and the Bappebti Regulation regarding crypto assets. Secondary legal materials were obtained from legal literature, reputable scientific journals, research reports, and the results of digital forensic audits on published crypto *scamming cases. The legal material collection technique was carried out through document study (documentary study*) with a strict classification system to ensure the relevance of *blockchain* technical data to traditional contract law doctrine (Ibrahim, 2008).

The analysis of legal materials was conducted qualitatively and normatively using a deductive method, namely drawing conclusions from general statements (legal norms) to specific legal facts (the phenomenon of *scamming* through *smart contracts*). Researchers used systematic and teleological interpretations to understand how legal objectives (justice and benefit) can be achieved amidst the rigidity of *blockchain* programming code. Managerially, this analysis is directed at formulating an "Operational Standard for Law Enforcement" that integrates criminalization of perpetrators and civil recovery of victims' assets (Sipayung et al., 2025). This is crucial to ensure that the research results are not merely theoretical but also provide applicable solutions for legal practitioners.

This entire methodology is designed to analyze *the ratio legis* of the integration of criminal law enforcement and civil validity. Using structured legal logic, this research seeks to address the challenge of "legal nullity" regarding automated transactions arising from malicious intent (*mens rea*). The validity of the research is maintained through triangulation of legal sources and cross-checking with the latest developments in *smart contract* technology, ensuring that the resulting arguments remain relevant to the rapid dynamics of the digital economy (Bagaskoro et al., 2023). Through this method, it is hoped that a reconstruction of legal thought can be created that can synchronize algorithmic code with substantive justice in accordance with the identity of Indonesian law.

3. RESULT AND DISCUSSION

Criminal Anatomy of Smart Contracts: The Link Between Mens Rea and Algorithms

From an Indonesian criminal law perspective, the manipulation of smart contracts for scamming purposes is a modern manifestation of the crime of fraud that has been expanded through electronic means. Article 392 of Law No. 1 of 2023 (National Criminal Code) and Article 28 paragraph (1) of the ITE Law provide the basis for prosecuting perpetrators who spread false and misleading news that results in consumer losses in electronic transactions. However, the main challenge lies in proving the mens rea (malicious intent) hidden behind the lines of code (Muladi, 2023). Perpetrators often argue that the transactions are autonomous and "voluntary" because the victim agrees to the interaction with the contract on the blockchain.

Technically, crypto-asset-based scams often employ malicious functions such as unlimited minting, blacklisting specific addresses, or rug pulls through sudden liquidity withdrawals. Digital forensic analysis shows that the perpetrator's malicious intent is integrated into the source code. In criminal law, this is referred to as a systematically prepared crime. Integration in law enforcement begins with recognizing that smart contract code is not merely a tool, but rather a representation of the will of a legal subject who can be held criminally accountable (Bagaskoro et al., 2023).

Civil Validity of Smart Contracts in the Midst of Criminal Acts

The most crucial legal issue is the civil status of transactions conducted through smart contracts, which are proven to be a means of crime. Referring to Article 1320 of the Civil Code, one of the objective requirements for a valid agreement is a "lawful cause" (geoorloofde oorzaak). If a smart contract is designed to deceive, then it contains a prohibited cause or is contrary to morality and public order (Article 1337 of the Civil Code). Doctrinally, an agreement containing a prohibited cause is null and void (nietig) or deemed never to have existed (Marzuki, 2021).

However, there is a conflict between technological legal certainty (code is law) and normative legal certainty. The immutable nature of blockchain means that transactions remain technically recorded as valid transfers of rights. This is where legal integration is necessary: a criminal court ruling declaring fraud must serve as the basis for a civil judge to declare the transfer of crypto assets without a valid legal basis (onverschuldigde betaling). This legal reconstruction is crucial so that assets controlled by the perpetrator can be reclaimed or ownership legally restored to the victim (Sari et al., 2022).

Synchronization of Law Enforcement: Bridging Criminal and Civil Law

Law enforcement integration must move beyond mere corporal punishment (imprisonment) to asset recovery. In the case of crypto, the arrest of a perpetrator does not automatically return the victim's funds if the private key or control over the contract remains in the perpetrator's hands. Therefore, Indonesian criminal law must begin adopting a restitution order mechanism integrated with civil law. Judges in criminal cases must have the authority to order the cancellation of the civil effects of corrupt smart contract transactions (Sipayung et al., 2025).

Operational challenges arise in the execution of judgments. Given the decentralized nature of enforcement, enforcement often requires collaboration with crypto exchanges or wallet providers to freeze assets associated with contract addresses declared legally flawed. This synchronization requires law enforcement officials to possess managerial competence in handling digital evidence and coordinating with supervisory authorities such as Bappebti.

Without a bridge between criminal judgments and civil enforcement, law enforcement will be a mere "paper tiger" unable to address the true extent of victims' losses (Lisi, 2023).

Consumer Protection and Risk Mitigation in the Crypto Ecosystem

Analyzing the validity of smart contracts also intersects with consumer protection laws. Crypto asset consumers in Indonesia are often in a weak bargaining position due to technical information asymmetry. Most investors lack the ability to conduct independent code audits. From a risk management perspective, the government should require third-party certification or audits of smart contracts offered to the public. The absence of these audits increases the opportunity for scams disguised as innovation (Sipayung & Subandi, 2023).

In the event of fraud, the principle of strict liability, or at least a shifting burden of proof, can be applied in civil lawsuits. The perpetrator or developer of a smart contract found to have inserted malicious code should be liable for damages without the victim needing to prove the technical details of the manipulation. This protection aligns with the principle of substantive justice, which states that the law should not allow the most vulnerable party to suffer due to the technical superiority of another party acting in bad faith (Ibrahim, 2008).

Reconstruction of Judicial Standards for Judges and Practitioners

Judges in Indonesia require specific judicial guidelines for handling smart contract disputes. This standard reconstruction involves recognizing "Smart Contract Audit Reports" as valid documentary evidence or expert testimony in court. Judges should not rely solely on rigid legal texts but should be able to discern the substance of justice behind algorithms. This integration also includes the use of forensic technology to trace on-chain fund flows to ensure that the assets in dispute are truly the result of fraud (Kurnia, 2023).

Going forward, Indonesia should consider establishing a dedicated judicial unit or cyber arbitration court that understands the intricacies of the crypto economy. This aims to minimize disparities in decisions. The certainty that an automatic contract can be voided through civil proceedings through formal legal channels would send a positive signal to the digital investment ecosystem in Indonesia. The law must be able to adapt without losing its essence as an instrument to protect citizens' human rights and property rights (Soekanto, 2015).

4. CONCLUSION

Integration between criminal law enforcement and civil law is an absolute prerequisite for addressing crypto-asset-based *scams* in Indonesia. Criminally, *smart contract* code manipulation meets the elements of fraud under the National Criminal Code and the Electronic Information and Transactions Law, but civilly, the transaction must be declared null and void because it does not meet the requirement of a "lawful cause" as stipulated in Article 1320 of the Civil Code. Regulatory synchronization and strengthening the digital competence of law enforcement officials are necessary to ensure that criminal prosecution of perpetrators is followed by the restoration of victims' property rights. Reconstructing judicial standards that recognize digital forensic audits as a basis for invalidating autonomous contracts will provide comprehensive legal certainty amid the rapid development of *blockchain* technology.

REFERENCES

Bagaskoro, et al. (2023). Legal Management of Blockchain Technology in Indonesia: Navigating the Regulatory Gap. *Journal of Progressive Law and Legal Studies*, 1(2).

Ibrahim, J. (2008). *Normative Legal Research Methodology*. Bayumedia Publishing.

Civil Code [*Burgelijk Wetboek*].

Kurnia, MP (2023). Good Governance in Digital Judiciary: Reconstructing Legal Standards for the Cyber Era. *Mulawarman Law Review*, 8(1), 45–60.

Lisi, I. Z. (2023). Cyber Crime and the Challenges of Modern Criminal Procedure: A Comparative Study. *Legal Policy Journal*, 12(3), 210–225.

Marzuki, PM (2021). *Legal Research: Revised Edition*. Prenada Media.

Muladi. (2023). *Modern Criminal Theories and Policies in Indonesia*. Alumni.

Sari, AR, Hamid, A., Utami, RA, Amalia, M., Sipayung, B., Widiatno, MW, & Musofiana. (2022). Legal Construction of Electronic Contracts and Validity of Smart Contracts in Indonesia. *National Law Journal*, 10(2), 77–89.

Sipayung, B., & Subandi. (2023). Legal Analysis of Digital Transactions and Consumer Protection in the Crypto Ecosystem. *SENGKUNI Journal: Social Science and Humanities Studies*, 4(1), 95–102.

Sipayung, B., et al. (2025). Strategic Management of Digital Asset Enforcement: Integrating Criminal and Civil Frameworks. *Journal of Management and Law*, 6(1), 110–124.

Soekanto, S. (2015). *Introduction to Legal Research*. UI Press.

Law Number 1 of 2023 concerning the National Criminal Code (KUHP).

Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024.