WHEN CODE COMMITS A CRIME: LEGAL CHALLENGES OF CRIMINAL ACTIVITY VIA SMART CONTRACTS

Ayesha Khanum, LL.M., Amity Law School, Amity University, Bengaluru.

Jyotirmoy Banerjee, Assistant Professor, Amity Law School, Amity University, Bengaluru

ABSTRACT

The rise of blockchain technology and the use of smart contracts have revolutionized how transactions and agreements are carried out across various industries.[1] These self-executing programs operate autonomously on decentralized networks, offering benefits like transparency, efficiency, and the elimination of intermediaries. Yet, these same features—immutability, decentralization, and autonomy—also make smart contracts susceptible to misuse. Criminals are increasingly leveraging these tools for illicit activities such as ransomware schemes, dark web transactions, financial fraud, and even markets tied to unlawful acts like assassinations. These developments present serious challenges to traditional legal frameworks based on human intent (mens rea) and action (actus reus), as smart contracts often function without further human input and are deployed anonymously. Compounding the problem is the jurisdictional ambiguity associated with decentralized networks. A smart contract can be created in one country, executed globally, and impact users in multiple jurisdictions, undermining the territorial nature of criminal law enforcement. Existing national laws are often outdated and ill-suited to address crimes involving decentralized technologies, creating legal grey areas that bad actors readily exploit. Historical incidents, such as the 2016 DAO hack and the controversial use of platforms like Augur for incentivizing unethical prediction markets, illustrate the murky legal landscape surrounding smart contract-enabled crimes. Globally, legal responses vary. The U.S. relies on traditional cybercrime laws, while the EU has adopted the MiCA framework, which still lacks provisions on criminal liability in autonomous systems. India applies legacy IT laws without specific reference to smart contracts, and China has enforced sweeping bans, though international threats persist. Addressing these challenges requires technical safeguards like contract audits and kill switches, along with adaptive legislation and international collaboration. As code increasingly shapes societal functions, legal systems must redefine responsibility and

[1] Agata Ferreira, "Regulating smart contracts: Legal revolution or simply evolution?," 45 *Telecommunications Policy* 102081 (2021).

accountability to safeguard public interest while supporting technological innovation.

Keywords: Smart contracts, Blockchain technology, European Union.

INTRODUCTION

The advent of blockchain technology and its application through smart contracts has significantly altered how transactions and agreements are executed in modern society. These self-executing pieces of code, embedded with predefined terms and conditions, run autonomously on decentralized blockchain networks.[2] Their promise of automation, transparency, and removal of intermediaries has made them highly appealing in sectors such as finance, logistics, digital identity, and even governance. However, the very attributes that make smart contracts revolutionary—immutability, decentralization, and autonomy—also make them ripe for criminal exploitation.[3] Their capabilities have introduced novel avenues for crime that traditional legal systems were never designed to handle.

Criminal actors are increasingly exploiting smart contracts for illegal activities including ransomware, dark web commerce, financial fraud, and prediction markets tied to unlawful actions. These activities fundamentally disrupt traditional criminal law principles based on human intent and action. Legal systems are built around the doctrines of *mens rea* (criminal intent) and *actus reus* (criminal action), typically linked to identifiable human perpetrators. Smart contracts complicate this by executing commands without human intervention, often initiated anonymously, making attribution and legal accountability a daunting task.[4] For example, once a malicious contract is deployed on the blockchain, it operates beyond the reach of its creator, complicating notions of ongoing intent or responsibility.[5]

Jurisdictional ambiguity adds to the challenge. Smart contracts function across borders, and their decentralized nature means a contract created in one jurisdiction can execute transactions

[2] Madhusudan Singh and Shiho Kim, “Chapter Four - Blockchain technology for decentralized autonomous organizations,” in S. Kim, G. C. Deka, *et al.* (eds.), *Advances in Computers* 115–40 (Elsevier, 2019), cxv.

[3] Adam J. Kolber, “Not-So-Smart Blockchain Contracts and Artificial Responsibility,” 21 *Stanford Technology Law Review* 198 (2018).

[4] Shuai Wang et al., “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” 49 *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 2266–77 (2019).

[5] Amit Kumar Tyagi et al., “Role of Blockchain Technology in Smart Era: A Review on Possible Smart Applications,” 23 *Journal of Information & Knowledge Management* 2450032 (2024).

and cause harm in multiple others.[6] This undermines the territorial basis of criminal law, which relies on physical presence and sovereignty to investigate and prosecute offenses. As such, prosecuting crimes involving smart contracts requires an overhaul in how jurisdiction is understood and applied in digital contexts. National laws are often outdated and ill-equipped to deal with crimes committed through decentralized technologies, and this legal vacuum is actively being exploited.

Historical cases highlight how smart contracts can facilitate or shield criminal conduct. The 2016 DAO hack, where approximately $60 million in Ether was drained from a decentralized investment fund due to a flaw in the contract's code, challenged the notion of illegality.[7] Since the contract performed "as written," legal experts debated whether the hacker committed a crime or merely exploited poor coding. Similarly, platforms like Augur have enabled users to create prediction markets for outcomes like assassinations or terrorist attacks, raising serious concerns about incentivized criminal behavior under the guise of decentralized finance.[8]

Comparative legal analysis shows a fragmented global approach to regulation. The United States enforces smart contract-related crimes through existing securities and cybercrime laws, though with limited effectiveness. The European Union has taken a more proactive stance with its Markets in Crypto-Assets Regulation (MiCA), offering legal clarity for digital assets but falling short on addressing criminal liability in autonomous systems.[9] India remains largely unregulated in this space, applying legacy IT laws with limited success, while China has banned most crypto and smart contract applications domestically, though threats from cross-border platforms persist.

Addressing these challenges requires a hybrid approach that combines technical safeguards, updated legislation, and international cooperation. Proposed solutions include mandatory third-party audits for high-risk contracts, the introduction of legal "kill switches" to disable malicious code, and the development of global standards for smart contract deployment. Flexible legal frameworks that evolve with technology are essential to ensure accountability

[6] Martina Černá, "Challenges and limitations of granting legal personality to distributed/decentralized autonomous organizations" (2024).

[7] Randolph A. II Robinson, "The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings," 85 *Tennessee Law Review* 897 (2017).

[8] Jack Peterson et al., "Augur: a decentralized oracle and prediction market platform" (arXiv, 2020).

[9] Cristina Carata and William J. Knottenbelt, "An Analysis of the MiCA Regulation and Its Impact for the Blockchain-Based Economies," in S. Leonardos, E. Alfieri, *et al.* (eds.), *Mathematical Research for Blockchain Economy* 359–70 (Springer Nature Switzerland, Cham, 2024).

without stifling innovation. The discussion also invites deeper philosophical questions about the role of code in society—if code can act like law, should developers bear the same responsibilities as lawmakers? Smart contracts are not inherently criminal, but they have introduced a new paradigm that challenges long-held legal concepts.[10] The legal system must evolve, not only by amending outdated laws but by reimagining legal responsibility in the age of autonomous digital agents.

LEGAL CHALLENGES IN ATTRIBUTION AND RESPONSIBILITY

In the rapidly evolving realm of blockchain and decentralized technologies, smart contracts have emerged as transformative tools, enabling automation and efficiency without the need for intermediaries. These self-executing codes operate autonomously once deployed on a blockchain, drastically altering how agreements and transactions function.[11] However, this technological innovation has introduced complex legal challenges, particularly when smart contracts are used for criminal purposes.[12] A central dilemma arises around attribution and accountability: when a smart contract facilitates a crime, who is to be held legally responsible? Traditional legal systems—based on human action and intent—struggle to adapt to a digital world where code executes actions independently of its creator.

One of the major concerns is identifying the responsible party when a crime is committed via a smart contract. Unlike conventional offenses where the perpetrator is a person or an identifiable entity, smart contracts act without further human intervention once deployed.[13] Their immutability means they cannot be altered or stopped, even if their effects are harmful. This leads to complex legal questions: should responsibility lie with the developer who wrote the code, the individual who deployed it, or the user who benefits from it? In decentralized finance (DeFi), where smart contracts handle billions of dollars, this ambiguity becomes more than theoretical.[14] In 2023 alone, over $3.1 billion was lost to smart contract-based scams and

[10] Raina S. Haque et al., "Blockchain Development and Fiduciary Duty," 2 *Stanford Journal of Blockchain Law & Policy* 139 (2019).

[11] Madhusudan Singh and Shiho Kim, "Chapter Four - Blockchain technology for decentralized autonomous organizations," in S. Kim, G. C. Deka, *et al.* (eds.), *Advances in Computers* 115–40 (Elsevier, 2019), cxv.

[12] Agata Ferreira, "Regulating smart contracts: Legal revolution or simply evolution?," 45 *Telecommunications Policy* 102081 (2021).

[13] Ari Juels, Ahmed Kosba and Elaine Shi, "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts" *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 283–95 (ACM, Vienna Austria, 2016).

[14] Johannes Rude Jensen, Victor von Wachter and Omri Ross, "An Introduction to Decentralized Finance (DeFi)" *Complex Systems Informatics and Modeling Quarterly* 46–54 (2021).

rug pulls—frauds where developers disappear with users' funds (Chainalysis, 2024). With blockchain's pseudonymity, law enforcement struggles to link wallet addresses to real-world identities, complicating investigations and prosecutions.

The issue of intent, or *mens rea*, is equally problematic. Criminal law relies heavily on proving a perpetrator's intention. But smart contracts, once coded and deployed, act without discretion.[15] For instance, if a developer creates a contract that is later used for money laundering, can they be held liable despite not directly participating in the illegal act? This was seen in the U.S. Treasury's 2022 sanctions against Tornado Cash, a privacy mixer accused of laundering over $1.5 billion, including funds linked to North Korea's Lazarus Group.[16] The developers argued they no longer had control over the deployed code, but the government still held them accountable (U.S. Department of the Treasury, 2022).

Recent legal developments suggest a shift toward holding decentralized actors accountable. In 2023, the U.S. Commodity Futures Trading Commission (CFTC) sued the creators of Ooki DAO for operating an unregistered trading platform.[17] The court ruled that even members of decentralized organizations who vote on governance decisions could be held legally responsible (CFTC v. Ooki DAO, 2023). This indicates that decentralization does not exempt individuals from legal obligations.

In India, the legal landscape remains vague. The Information Technology Act, 2000, does not directly address blockchain-related offenses or liabilities from smart contracts. With an estimated 18 million crypto users in India in 2023 (Statista, 2024), the lack of specific legal provisions leaves victims of blockchain crimes with limited recourse, while courts and police lack the expertise to navigate such technical issues.

Smart contracts also raise thorny jurisdictional questions. They can be deployed anywhere and interacted with globally, challenging the enforcement powers of national legal systems. There is no universal legal standard for resolving these cross-border disputes, though efforts like the EU's MiCA framework and G20 discussions signal a push for international harmonization.

[15] Eliza Mik, "Smart contracts: terminology, technical limitations and real world complexity," 9 *Law, Innovation and Technology* 269–300 (2017).

[16] Emily Arterbury, "Coin Center v. Yellen Prompts Reconsideration of the Vast Deference Afforded to the Department of the Treasury," 73 *Catholic University Law Review* 473 (2024).

[17] Richard Fair, "DECENTRALIZATION AND SUPREMACY: CONSTITUTIONAL LIMITS ON STATE DAO LLC STATUTES" (Rochester, NY, 2025).

Ultimately, legal systems must evolve to meet the challenges of code-based crimes. Concepts like "algorithmic accountability" are gaining traction, suggesting that developers should bear a duty of care when creating potentially harmful code. Simultaneously, investments in blockchain forensic capabilities, cyber law reforms, and public awareness are necessary. As technology reshapes the legal landscape, innovation must be balanced with accountability to safeguard digital society.

CASE STUDIES AND EXAMPLES OF CRIMINAL USE

Year	Case Name / Project	Nature of Crime	Impact	Legal Action Taken
2016	The DAO Hack (Ethereum)	Exploitation of recursive call vulnerability in smart contract	Theft of 3.6 million ETH (~$60M); led to Ethereum–Ethereum Classic split	No direct criminal prosecution; led to Ethereum hard fork
2021	AnubisDAO	Rug pull scam (developers vanished with funds)	Loss of ~$60M in investor funds; eroded trust in DeFi projects	No legal action; developers remained anonymous
2022	Beanstalk Protocol	Flash loan governance exploit	Loss of $182M; undermined DAO-based financial protocols	Ongoing investigations; no confirmed arrests
2022	Tornado Cash (U.S. Treasury)	Money laundering via privacy-enhancing smart contracts	Used to launder $1.5B, including $455M by North Korea's Lazarus Group	U.S. Treasury sanctioned the protocol; developers arrested in the EU
2023	Mango Markets (Solana)	Price manipulation using flash loans	Exploit of $114M; attacker returned part of funds claiming "legal arbitration"	Avraham Eisenberg arrested and charged by U.S. DOJ for market manipulation
2023	Crime-as-a-Service (Various)	Smart contracts used for automated ransomware payouts	~15% of ransomware gangs used smart contracts for extortion payments	Monitored by Europol; legal action depends on jurisdictional cooperation

In recent years, several high-profile cases have demonstrated how smart contracts are being weaponized for criminal purposes, exposing both technological vulnerabilities and legal gaps. The 2016 DAO hack allowed a hacker to drain $60 million in Ether by exploiting a flaw in the contract's code, raising debates about the legality of actions executed through "code as law" and resulting in no legal charges.[18] In 2021, the AnubisDAO rug pull saw developers vanish with nearly $60 million, taking advantage of anonymity and the absence of jurisdictional clarity.[19] The 2022 Beanstalk Protocol exploit used a flash loan to manipulate governance and steal $182 million, but no prosecutions occurred due to the decentralized and anonymous setup.[20] That same year, Tornado Cash, an Ethereum-based coin mixer, was sanctioned by the U.S. Treasury after laundering over $1.5 billion, including funds stolen by North Korea's Lazarus Group, leading to the arrest of several developers in Europe. In 2023, Avraham Eisenberg manipulated Mango Markets by inflating its token value and extracting $114 million, later facing arrest and market manipulation charges—setting a precedent for prosecuting crimes committed within the "rules" of smart contracts.[21] Meanwhile, ransomware groups are increasingly integrating smart contracts into extortion schemes, automating decryption key releases upon crypto payment and using mixers like Tornado Cash to obscure transactions. Europol's 2024 report noted that 15% of ransomware gangs employed smart contracts, up from 6% in 2021.[22] These cases illustrate how smart contracts—originally praised for transparency and efficiency—are now exploited for scams, laundering, and market manipulation, particularly affecting retail investors in developing countries. The global legal response remains inconsistent and underdeveloped, highlighting an urgent need for coordinated international regulation, smarter enforcement strategies, and technological safeguards to mitigate the criminal abuse of decentralized technologies.

[18] Vikram Dhillon, David Metcalf and Max Hooper, "The DAO Hacked," in V. Dhillon, D. Metcalf, *et al.* (eds.), *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You* 67–78 (Apress, Berkeley, CA, 2017)

[19] Wulf A. Kaal, "DAO Fallacies: Common Myths and Uses for Decentralized Autonomous Organizations" *Decentralized Autonomous Organizations* (Routledge, 2024).

[20] Aida Manzano Kharman and Ben Smyth, "DAO Governance Protocols and their Vulnerabilities" *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2024.

[21] Quel luminoso spirito partenopeo: Intersezioni simboliche tra Napoli e Israele nella saga familiare di Mariastella Eisenberg - ProQuest,"*available at*: https://www.proquest.com/openview/179e6e63dba6f721a4e3b98eb4ac1d63/1?cbl=4524990&pq-origsite=gscholar (last visited May 21, 2025).

[22] Thomas Wahl, "Europol" *Research Handbook on EU Criminal Law* 429–61 (Edward Elgar Publishing, 2024).

COMPARATIVE LEGAL PERSPECTIVES AND REGULATION EFFORTS

Country/Region	Legal Framework/ Regulation	Focus Area	Notable Case/ Action	Effectiveness
European Union	MiCA (2023), Data Act (2023)	Investor protection, data-sharing laws	Tornado Cash sanctions; increased audit obligations	High – Structured and harmonized approach
United States	Fragmented (SEC, DOJ, State Laws)	Fraud, securities violations	Mango Markets exploit – DOJ prosecution	Medium – Strong enforcement, lacking unified laws
United Kingdom	Law Commission Reports (2022–2023)	Legal recognition, smart contract logic	Ongoing – No major enforcement case yet	Moderate – Flexible adaptation of existing law
Singapore	Payment Services Act (updated in 2022)	AML, licensing, financial regulation	Licensed crypto exchanges with contract audit mandates	High – Clarity and strong compliance environment
India	No specific regulation (as of 2024)	Under IT Act and RBI circulars	No major case law; low capacity for enforcement	Low – Regulatory ambiguity and limited awareness

The global rise of smart contracts has forced legal systems to reevaluate traditional models of regulation and enforcement, as these self-executing codes on decentralized platforms like Ethereum and Solana introduce both efficiency and unprecedented legal challenges when misused for criminal activity. Legal responses remain fragmented as of 2024, creating jurisdictional loopholes exploited by cybercriminals. The European Union has adopted a proactive stance through its Markets in Crypto-Assets Regulation (MiCA), offering a harmonized legal framework to enhance investor protection and reduce market abuse, while the 2023 Data Act includes smart contract provisions for data sharing, especially within the Internet of Things.[23] Although MiCA does not directly regulate smart contracts, it signals a growing emphasis on developer accountability. In contrast, the United States lacks unified federal legislation; instead, bodies like the SEC, CFTC, and DOJ intervene on a case-by-case basis, as seen in the 2023 arrest of Avraham Eisenberg for exploiting Mango Markets.[24] Some U.S. states like Arizona and Tennessee have recognized smart contracts' civil enforceability

[23] Cristina Carata and William J. Knottenbelt, "An Analysis of the MiCA Regulation and Its Impact for the Blockchain-Based Economies," in S. Leonardos, E. Alfieri, *et al.* (eds.), *Mathematical Research for Blockchain Economy* 359–70 (Springer Nature Switzerland, Cham, 2024).

[24] Edward J. Kane, "Regulatory Structure in Futures Markets: Jurisdictional Competition Among the SEC, the CFTC, and Other Agencies" (National Bureau of Economic Research, 1984).

since 2017, but such statutes rarely address criminal misuse. Countries like Singapore and the UK favor a regulatory sandbox model.[25] Singapore's MAS enforces strict licensing and anti-money laundering rules under its Payment Services Act, while the UK Law Commission has explored integrating smart contracts into existing legal doctrines, championing technological neutrality. Meanwhile, developing nations like India lack specialized laws or sufficient enforcement capability, with a 2023 NITI Aayog report revealing only 27% of law enforcement felt equipped to handle blockchain crimes. This global regulatory inconsistency is dangerous, as blockchain-enabled crimes cross borders with ease—criminals deploy smart contracts from lenient jurisdictions, targeting victims worldwide with minimal accountability. The resulting societal harm includes financial losses, eroded trust in digital innovation, and underprepared legal systems. To address this, international collaboration, standardized laws, and cross-border enforcement mechanisms are urgently needed.

POLICY RECOMMENDATION

As smart contracts continue to transform digital interactions and financial transactions, the need for updated and effective legal policies has become more urgent than ever. Their ability to execute pre-defined conditions autonomously, without centralized oversight, presents both innovation and risk. While smart contracts hold immense potential for automating processes and reducing human error, they have also been exploited in various criminal schemes—from rug pulls and flash loan exploits to laundering illicit funds. In this fast-evolving landscape, policy recommendations must be forward-looking, technologically adaptive, and socially grounded. A key issue with current frameworks is the disconnection between technical functionality and legal accountability. Therefore, any policy intervention must aim to bridge this gap in a manner that promotes innovation while protecting users.

One of the most immediate recommendations is the introduction of a global "Smart Contract Code Audit & Accountability Policy" (SCAAP). This proposed policy would mandate that all publicly deployed smart contracts undergo third-party security audits from certified blockchain auditors before being integrated into financial ecosystems. Much like how pharmaceutical products must pass safety tests before hitting the market, smart contracts too must meet minimum security benchmarks. These audits should check for known vulnerabilities, exploit

[25] Christopher C. Chen, "Regulatory Sandboxes in the UK and Singapore: A Preliminary Survey" (Rochester, NY, 2019).

possibilities, and logic flaws. Governments can incentivize compliance by offering tax benefits or legal safe harbor to platforms that adhere to such policies. At the same time, contracts that are unaudited or found to have malicious intent should be flagged in public registries similar to blacklists maintained by financial institutions. Such a registry can help consumers and investors make informed decisions and avoid interacting with potentially harmful code.

Implementation of this policy could be overseen by a multi-stakeholder body comprising government agencies, blockchain experts, consumer protection groups, and legal professionals. A decentralized but verifiable registry system—perhaps operating as a consortium-led blockchain—could host audit records, timestamps, and the identities of verifiers. This would not only ensure transparency but also create traceable points of accountability. To ensure global cohesion, regulatory cooperation with international bodies such as the Financial Action Task Force (FATF), INTERPOL, and the International Telecommunication Union (ITU) should be fostered. These institutions can help harmonize cross-border enforcement and prevent regulatory arbitrage by rogue actors operating in unregulated jurisdictions.

Beyond technical scrutiny, policies should also promote smart contract literacy among the general public. Much like financial literacy campaigns have been pivotal in empowering individuals in the banking sector, blockchain literacy initiatives should become a part of national education and awareness programs. A 2023 survey by Chainalysis found that over 62% of crypto investors globally were unaware of how smart contracts functioned, leaving them vulnerable to scams. Public-private partnerships can fund educational campaigns, workshops, and school-level courses that demystify blockchain technology and explain the legal rights of users.

Lastly, governments should consider setting up specialized digital courts or legal task forces equipped with blockchain expertise. Traditional courts often lack the technical know-how to resolve disputes involving smart contracts, leading to delays or unjust rulings. By establishing dedicated tech-legal teams under existing cybercrime units, cases involving smart contract fraud, misuse, or breach can be adjudicated with precision and efficiency. These units should be empowered to use forensic blockchain tools, issue international notices, and coordinate with exchanges and developers to freeze malicious contracts in real time. The evolution of smart contracts demands not only reactive regulation but proactive policymaking. Policies like SCAAP, combined with strong educational outreach and digital legal infrastructure, can ensure that societies harness the promise of blockchain while defending against its misuse. A well-regulated smart contract ecosystem will not only build user trust but also attract responsible innovation that benefits society as a whole.