



Journal of Business Crime

e-ISSN: 3090-4412
Vol 02 (2) 2026 p. 61-77

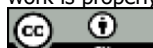
© Christopher Hamerton, 2026

Corresponding author:

Christopher Hamerton
Email:
christopher.hamerton@citystgeorges.ac.uk

*Received 7 August 2026;
Accepted 28 September 2026;
Published 30 September 2026.*

This is an Open Access article distributed under the terms of the [Creative Commons Attribution 4.0 International license](#), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.



Conflict of interest statement:

Author(s) reported no conflict of interest

DOI: [http://doi.org/10.70764/gdpu-jbc.2026.2\(2\)-01](http://doi.org/10.70764/gdpu-jbc.2026.2(2)-01)

THE ILLUSION OF TRUSTLESS COMPLIANCE: CODE, COERCION AND BUSINESS-CRIME VULNERABILITIES IN SMART CONTRACTING

Christopher Hamerton¹

¹ University of London, United Kingdom

ABSTRACT

Objective: This article interrogates the claim that smart contracts enable 'trustless compliance' in international commerce, arguing that blockchain automation relocates trust rather than eliminates it, and that the resulting governance, liability, and criminogenic conditions demand sustained legal engagement.

Research Design & Methods: A qualitative, doctrinal, and interdisciplinary methodology combines socio-legal analysis, an adapted Cressey's Fraud Triangle supplemented by Routine Activity Theory, and illustrative case analysis. Doctrinal review covers the UNCITRAL Model Law on Automated Contracting, the ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, FATF virtual-asset standards, and the UNIDROIT Principles on Digital Assets and Private Law. Illustrative cases include the 2016 DAO incident, the Aragon governance dispute, oracle manipulation exploits, and flash-loan attacks.

Findings: Three emerge. First, immutable execution supplants contextual doctrines (good faith, frustration, unconscionability, proportionality) through which contract law absorbs uncertainty, producing rigidity where judicial flexibility is most needed. Second, the adapted Fraud Triangle and Routine Activity Theory show that algorithmic opportunity, intensified pressure in continuously operating markets, weakened guardianship, and the rationalisation that 'code is law' reorganise rather than remove the conditions for business and financial offending. Third, recent international instruments reaffirm that automation changes only the means by which obligations are performed, not the principles by which responsibility is allocated.

Implications: The article proposes a shift from trustlessness towards a legally embedded framework incorporating human-in-the-loop governance, technology-neutral attribution of liability to commercial beneficiaries, transparent oracle oversight, and internationally harmonised standards.

Contribution & Value Added: This research explains how smart contracts impact trust in global commercial transactions, highlighting the need for human oversight and clear accountability.

Keywords: Business Crime, Smart Contracts, Blockchain Governance, Fraud Triangle, Legal Embeddedness.

JEL codes: K12, K22

Article type: research paper

INTRODUCTION

The rapid digitalisation of international commerce has reshaped how contractual relationships are formed, executed, and enforced. At the centre of this transformation sits the smart contract built upon blockchain technology: a computer protocol that automatically executes obligations once predetermined conditions are satisfied, replacing traditional legal intermediaries with deterministic software (Bassan and Rabitti, 2024; De Filippi and Hassan, 2016; Wang and Xu, 2022). Blockchain systems propose a form of algorithmic governance in which cryptographic verification supplants interpersonal trust, with self-enforcing, immutable, and transparent transactions theoretically eliminating many opportunities for breach (Taherdoost, 2023; Küçükaltan et al., 2024; Zetzsche et al., 2018).

The narrative of trustless commerce rests on assumptions that warrant scrutiny (Cornelius, 2018; Bratspies, 2018). It presumes that contractual disputes arise primarily from intentional breach and that eliminating opportunities for non-performance eliminates commercial misconduct. This reasoning overlooks decades of criminological scholarship demonstrating that wrongdoing continuously adapts to institutional change (Hamerton &

[Webber, 2026](#); [Di Nicola, 2022](#); [Schuchter and Levi, 2015](#)). Criminal opportunities rarely disappear; they evolve alongside new technologies and economic incentives.

Immutable code cannot distinguish between lawful and unlawful outcomes where both follow the system's programmed logic. Software executes instructions without regard to fairness, proportionality, unconscionability, or public policy. The very characteristics celebrated as strengths - automation, determinism, and immutability - may therefore become sources of acute legal vulnerability ([Sotiropoulos, 2026](#)).

This article argues that trustless compliance is illusory. Smart contracts relocate trust from legal institutions toward technological infrastructure, software developers, data providers, and governance mechanisms that frequently operate beyond traditional regulatory oversight ([Gottschalk and Hamerton, 2022](#); [Lukyanenko et al., 2022](#); [Zetsche et al., 2018](#)). As markets become more automated, opportunities for fraud become algorithmic. Traditional forms of commercial misconduct are increasingly replaced by code manipulation, oracle corruption, governance attacks, flash-loan exploits, and automated market manipulation. The technology develops, human behaviour changes; and the underlying criminogenic conditions adapt and persist ([McGuire, 2012](#)).

Four interrelated problem areas frame the analysis. The first is compliance: automated execution is routinely presented as compliance, yet code enforces programmed instructions rather than legal obligations and cannot recognise fraud, duress, or a sanctions breach embedded within a valid-looking transaction. The second is governance: decision-making shifts from identifiable corporate organs to token-weighted voting, developers, and protocol maintainers whose authority is seldom matched by formal accountability. The third is liability: responsibility fragments across developers, node operators, oracle providers, and token holders, leaving no obvious defendant when automated systems cause loss. The fourth is business and financial crime: the same architecture that reduces routine transaction risk generates fresh opportunities for oracle manipulation, flash-loan exploits, governance takeovers, and automated market abuse. The study's scope is deliberately bounded. It is a qualitative, doctrinal, and literature-based inquiry and does not attempt quantitative measurement of blockchain-related crime, nor does it claim comprehensive coverage of national implementations of the instruments examined; both remain tasks for future research.

The analysis proceeds in four stages. The literature review synthesises scholarship on smart contracts, legal pluralism, regulatory theory, and technological crime. The methodology section sets out the doctrinal and conceptual approach adopted. The results section presents the analysis of criminogenic vulnerabilities through an adapted Fraud Triangle model and Routine Activity Theory, drawing on contemporary incidents. The discussion section interprets these findings in relation to the theoretical framework and previous studies. Finally, the article evaluates recent international legislative developments and proposes a tentative legally embedded framework.

The objective is therefore twofold: to analyse how automated execution reshapes the governance, liability, and criminogenic conditions of international commerce, and to identify the legal and architectural responses capable of situating smart contracting within an accountable commercial-law framework thereby addressing the gap identified below: the absence of an integrated account that treats smart contracts simultaneously as commercial instruments, governance structures, and criminogenic environments.

Existing scholarship has largely examined smart contracts from a single disciplinary vantage point. Contract-law and doctrinal scholars address enforceability, error, and doctrinal fit ([Sotiropoulos, 2026](#); [Rijanto, 2021](#)); regulation and governance scholars treat code as a regulatory instrument ([Lessig, 1999](#); [Yeung, 2017](#); [Prifti et al., 2024](#)); and criminologists have applied the Fraud Triangle and Routine Activity Theory extensively to cybercrime and corporate offending ([Cressey, 1953](#); [Hutchings and Clayton, 2016](#); [Willison et al., 2018](#)) but rarely to contractual automation. These literatures have not been systematically connected. The study's novelty lies in that integration: by applying an adapted Fraud Triangle, supplemented by Routine Activity Theory, within a socio-legal analysis of automated contracting, it treats doctrinal rigidity, redistributed governance authority, and criminogenic opportunity as features of a single phenomenon rather than as separate problems, and tests the resulting account against recent international instruments.

Because the design is qualitative, doctrinal, and literature-based, formal hypothesis testing is neither appropriate nor claimed. Three analytical propositions guide the analysis instead. P1: automation does not eliminate trust in commercial exchange but relocates it to developers, data providers, and governance mechanisms that are less visible to regulators and courts. P2: the conditions for business and financial crime are reorganised rather than removed, with opportunity embedded in code, pressure intensified by continuously operating markets, guardianship weakened by design, and rationalisation supplied by the 'code is law' ideology. P3: legal instruments that attribute responsibility to those who deploy, control, or benefit from automated systems can materially narrow the accountability gap that automation creates.

LITERATURE REVIEW

The emergence of smart contracts has produced an interdisciplinary body of scholarship spanning law, economics, computer science, governance, and criminology. While early literature celebrated blockchain as a disruptive mechanism, more recent research has adopted a more critical posture, questioning whether technological automation can genuinely substitute for the normative functions performed by legal institutions (Ding et al., 2026; Nelken, 2025; Selçuk et al., 2025; Scott, 2004).

Wright & De Filippi argued that blockchain represents a shift toward *lex cryptographia* - a decentralised regulatory order in which software increasingly governs social and economic interactions independently of state institutions (Wright and De Filippi, 2015: 4). To an extent this proposition resembles Lawrence Lessig's theory that 'code is law,' embedding regulatory constraints within computational architecture (Lessig, 1999). Here, Lessig argued that software code and network architecture function as the primary legal system of the digital world. While traditional laws punish rule-breakers after the fact, digital code inherently prevents non-compliant behavior from happening at all. This shifts regulatory power from elected politicians to private programmers, who embed values directly into internet infrastructure representing a significant march towards technocracy over the past thirty years (Cozzolino et al., 2026; Gratton and Edenhofer, 2025).

Socio-legal scholars have increasingly questioned whether technological regulation can substitute for legal judgment (Onțanu and Tjong Tjin Tai, 2025; Smuha, 2024; van den Berg, 2011). Unlike software, contract law deliberately incorporates ambiguity because human relationships occur within dynamic environments characterised by uncertainty, unforeseen events, and competing normative values (Cornelius, 2018; Howells, 2020). Foundational work in the sociology of law shows that law derives legitimacy from its embeddedness within broader social relations (Kozak-Isik, 2026; Nelken, 2025). Legal institutions perform interpretive, ethical, and distributive functions that extend beyond mechanical rule application; they balance competing interests, evaluate proportionality, and engage with questions of justice - at the present time, software cannot perform these nuanced evaluative functions.

As is historically the case with economic transaction, trust is of particular and enduring concern (Gottschalk and Hamerton, 2025a; Grillo, 2016; Moore, 1999). Luhmann-influenced scholarship on AI and autonomous systems argues that trust functions as a mechanism for reducing social complexity rather than eliminating uncertainty altogether, and that trust frameworks in automated systems require institutional anchors (Lukyanenko et al., 2022; Luhmann, 1995). AI trust research stresses that human cooperation with automated decision-making depends upon interpretive, accountable institutions because full transparency can never be achieved.

This tension between computational determinism and legal flexibility gains force when examined through criminological scholarship. White-collar crime research demonstrates that criminal opportunities evolve alongside organisational and technological change (Schuchter and Levi, 2015; Gottschalk and Hamerton, 2021, 2024a, 2025b). To illustrate this, the classical Cressey Fraud Triangle has been extensively adapted to contemporary corporate offending, cybercrime, and organisational misconduct (Hutchings and Clayton, 2016; Cressey, 1953). Applied to blockchain environments, the adapted fraud triangle framework suggests automation alters each dimension without eliminating fraudulent behaviour. Opportunities become embedded in software architecture; pressures intensify through competitive digital markets; and rationalisations emerge through technological ideologies that portray algorithmic outcomes as inherently legitimate.

To an extent Routine Activity Theory (RAT) informs and reinforces the impact of socio-technological change in online business transactions. For RAT theorists and cybersecurity specialists online criminality frequently depends upon the convergence of motivated offenders, suitable targets, and the absence of capable guardians (Cohen and Felson, 1979; Madarie et al., 2026; Junger et al., 2020; Hutchings and Clayton, 2016). Clearly, smart contracts potentially weaken traditional guardianship by replacing human oversight with automated execution, expanding opportunities for sophisticated exploitation. Taken together, this literature suggests that blockchain technology represents a profound transformation of regulatory architecture - reshaping relations between law, technology, governance, and criminal opportunity.

What remains unresolved. Read together, the scholarship reviewed above establishes two propositions: that automation alters regulatory architecture, and that criminogenic opportunity adapts to technological change. It does so, however, along three largely parallel tracks. Legal and socio-legal work on smart contracts concentrates on enforceability, consumer protection, and the limits of code as regulation, and tends to treat criminality as a peripheral risk. Criminological work tests the Fraud Triangle and Routine Activity Theory against online and organisational offending, but seldom against contractual automation. Regulatory scholarship maps international instruments without asking how offenders might exploit the gaps between them. Three gaps therefore remain. First, no framework connects contractual rigidity, redistributed governance authority, and criminal opportunity within a single explanation. Second, the Fraud Triangle and Routine Activity Theory have not been applied to automated commercial contracting. Third, a comparative assessment of the UNCITRAL, ELI, FATF, and UNIDROIT instruments against the criminogenic features identified in the theoretical literature is still missing. The present study addresses each of these gaps as illustrated in Table 1.

Table 1. What the current literature addresses and what it leaves unresolved (Hamerton, 2026)

Literature strand	Representative works	Addressed	Unresolved
Code as regulation	Lessig (1999) ; Wright and De Filippi (2015) ; Oster (2021)	Code and architecture function as regulatory instruments; emergence of <i>lex cryptographia</i>	Whether code can perform the interpretive and evaluative functions of contract law; not tested against criminal exploitation
Socio-legal and legal pluralism	Nelken (2025) ; Kozak-Isik (2026)	Legal legitimacy depends on embeddedness in social relations	Application to automated commercial governance remains thin
Trust in AI and autonomous systems	Luhmann (1995) ; Lukyanenko et al. (2022)	Trust reduces complexity and requires institutional anchors	How relocated trust affects criminal opportunity in commerce is unexplored
White-collar crime and the Fraud Triangle	Cressey (1953) ; Schuchter and Levi (2015) ; Gottschalk and Hamerton (2021, 2024a, 2025b)	Extensively adapted to corporate offending, cybercrime, and organisational misconduct	Not applied to smart-contract commerce
Routine Activity Theory	Cohen and Felson (1979) ; Junger et al. (2020) ; Madarie et al. (2026)	Convergence of motivated offender, suitable target, and absent guardian in online settings	Guardianship in deliberately decentralised automated systems
International instruments	UN (2024) ; ELI (2022) ; Pavlidis (2020) ; UNIDROIT (2023)	Technological neutrality; attribution; consumer and private-law protections	Largely reactive; oracle governance remains underdeveloped

METHODS

This article adopts a qualitative, doctrinal, and literature-based methodology that brings together socio-legal scholarship, criminological theory, and contemporary developments in international commercial law with an interdisciplinary focus.

First, doctrinal analysis assesses emerging international frameworks, including the UNCITRAL Model Law on Automated Contracting ([UN, 2024](#)), the European Law Institute Principles on Blockchain Technology, Smart Contracts and Consumer Protection ([ELI, 2022](#)), and related international instruments ([Busch, 2025](#); [Jin and Park, 2025](#)). These frameworks were examined alongside established contract-law, consumer-protection, and private-international-law principles.

Secondly, the article employs socio-legal analysis to explore the relationship between legal rules, technological architecture, and institutional trust. Smart contracts are examined as governance mechanisms that redistribute authority between developers, commercial actors, regulators, and courts, not merely as technical artefacts.

Thirdly, the article adopts a criminological framework centred on the Fraud Triangle, supplemented by contemporary scholarship on white-collar crime, organised / organisational crime, and cybercrime ([Gottschalk and Hamerton, 2021, 2025a](#); [Hamerton, 2020](#)). Here, precis illustrative case studies including the original DAO incident, Aragon's governance dispute, oracle manipulation episodes, and flash-loan exploits are incorporated to demonstrate how theoretical vulnerabilities materialise in operational blockchain ecosystems ([Kharman and Smyth, 2024](#)). This type of conceptual approach is deemed appropriate as the legal and criminological challenges of smart contracting are formative and rapidly evolving.

RESULT

Socio-Legal Friction: When Immutable Code Collides with Fluid Law

The philosophical foundation of smart contracting rests on the proposition that contractual certainty can be achieved through computational determinism. From a socio-legal perspective, however, this certainty represents both the principal strength and the principal weakness of automated contracting.

Traditional contract law, particularly in cross-jurisdictional transactions, evolved because commercial relationships could not be reduced to binary classifications. Both common law and civil law jurisdictions therefore preserve judicial discretion through doctrines such as good faith, frustration, hardship, force majeure, unconscionability, mistake, proportionality, and commercial reasonableness ([Brownsword, 1996](#); [Howells, 2020](#); [Gottschalk and Hamerton, 2025a](#)). These doctrines acknowledge that rigid or uniform enforcement may itself produce injustice. Smart contracts appear to invert this jurisprudential philosophy. Their legitimacy derives from

the elimination of interpretative discretion. Software cannot distinguish between intentional breach and unavoidable disruption, between opportunistic delay and humanitarian necessity, or between commercial bad faith and genuine impossibility.

Law functions through interpretation: judges evaluate evidence, infer intention, weigh proportionality, and balance competing rights. Software performs none of these functions because algorithms execute instructions irrespective of social context unless explicitly encoded. As disputes involving algorithmic trading systems have demonstrated, sophisticated exchanges can produce executions at price levels far removed from prevailing market conditions, with ordinary mistake doctrine providing only limited remedial traction (Loke, 2020).

The 'code is law' thesis remains influential, yet blockchain exposes an important limitation. Code regulates conduct only within the narrow parameters anticipated by its programmers (Yeung, 2017; Oster, 2021). Courts, arbitrators, and commercial institutions exist precisely because uncertainty cannot be fully eliminated from complex economic relations. Blockchain does not remove uncertainty; it suppresses the legal mechanisms designed to respond when uncertainty materialises (Nelken, 2025).

The implications become stark during systemic disruption. Under conventional commercial law, courts may excuse delayed performance through force majeure or frustration where circumstances render contractual obligations temporarily impossible or fundamentally different (Rijanto, 2021). An automated smart contract possesses no equivalent capacity for contextual reasoning. If the code specifies that payment must occur upon delivery before a specified deadline, execution proceeds as programmed regardless of whether delay resulted from war, embargoes, cyberattacks, or humanitarian emergencies.

Computational certainty may, in such cases, produce legally irrational outcomes precisely because it excludes the contextual flexibility upon which commercial justice has historically depended (Zetzsche et al., 2018). Accordingly, the consequence is not merely technical rigidity but a redistribution of power. Smart contracts thus expose what commentators describe as the dark side of lex cryptographia: an inflexible, networked governmentality in which the technical implementation of rules forecloses legal challenge (Rijanto, 2021).

Automated Coercion and Structural Power Imbalances

Contract law has long recognised that formal consent does not necessarily produce substantively fair agreements. Consumer protection legislation, unfair-terms regimes, and doctrines concerning economic duress all reflect judicial recognition that stronger parties may exploit informational or economic asymmetries during negotiation (Cornelius, 2018; Bratspies, 2018; Howells, 2020). Mass or normative automation has the potential to magnify these asymmetries (Hamerton and Webber, 2026).

Large multinational corporations possess access to specialist blockchain developers, cybersecurity experts, financial engineers, and legal teams capable of constructing extraordinarily sophisticated contractual architectures. Small enterprises, developing-country firms, and individual commercial participants rarely possess comparable expertise (Bui and Le, 2025). Many counterparties may understand the commercial purpose of an agreement while remaining unable to evaluate the code governing its execution (Alimohammadlou and Alinejad, 2023). Unlike traditional written contracts, whose language remains open to legal interpretation, smart contracts frequently conceal their practical consequences beneath layers of technical complexity. Even where source code is publicly available, meaningful understanding often requires advanced programming knowledge unavailable to ordinary commercial actors. This informational asymmetry transforms software architecture into a mechanism of structural power.

Automated collateral-liquidation mechanisms provide a vivid example (ESMA, 2023; Barcentewicz et al., 2024) as they may be programmed to execute immediately after minor fluctuations in market price. Although economically rational from the perspective of capital preservation, such mechanisms may produce disproportionate losses for counterparties experiencing temporary liquidity constraints during volatile periods. Under ordinary contract law, courts could intervene to prevent enforcement that becomes punitive rather than compensatory. Smart contracts eliminate this possibility by ensuring that asset transfers occur instantaneously, before judicial review becomes practically available (Rijanto, 2021).

Legal challenge therefore becomes retrospective rather than preventative. This inversion fundamentally alters the balance of procedural justice. Rather than requiring powerful actors to justify coercive enforcement before neutral institutions, weaker parties become responsible for reversing completed transactions through expensive, often jurisdictionally uncertain civil litigation.

Jurisdictional Arbitrage and the Emergence of Legal Black Holes

A further consequence of decentralised smart contracting concerns its capacity to undermine the territorial assumptions upon which private international law has traditionally operated (Berdibayev, 2026). Commercial law remains deeply connected to geography. Questions concerning jurisdiction, applicable law, recognition of judgments, and enforcement depend upon identifiable connecting factors – situs and place of contracting, habitual

residence, location of performance, or situs of property. Blockchain deliberately disrupts these connecting factors (Pinheiro, 2023). Distributed ledger technology stores transactional data simultaneously across nodes located in multiple jurisdictions. Smart contracts execute autonomously without reference to any single national legal system. Participants may remain pseudonymous, while assets circulate through networks possessing no identifiable territorial headquarters.

Determining where an automated contract was formed, performed, or breached becomes correspondingly difficult. This creates opportunities for sophisticated jurisdictional arbitrage (Draganidis, 2023). Corporate actors may intentionally route transactions through decentralised protocols precisely to exploit uncertainty regarding applicable law. The resulting regulatory ambiguity has been described as creating 'legal black holes,' spaces in which commercial activity continues while the practical capacity of any single legal system to regulate that activity weakens substantially (Rodríguez, 2025).

From a criminological perspective, such environments are highly attractive. Organised financial crime has historically flourished wherever regulatory fragmentation creates uncertainty regarding enforcement responsibility (Gottschalk and Gunnesdal, 2018; Gottschalk and Hamerton, 2021, 2024b). Offshore banking, shell corporations, and beneficial-ownership secrecy demonstrate how legal complexity becomes a valuable criminogenic resource. Blockchain extends this logic into digital infrastructure, permitting commercial actors to operate between legal systems and complicating attribution, investigation, evidence gathering, and asset recovery simultaneously (Berdibayev, 2026).

Reframing the Fraud Triangle for Automated Commerce

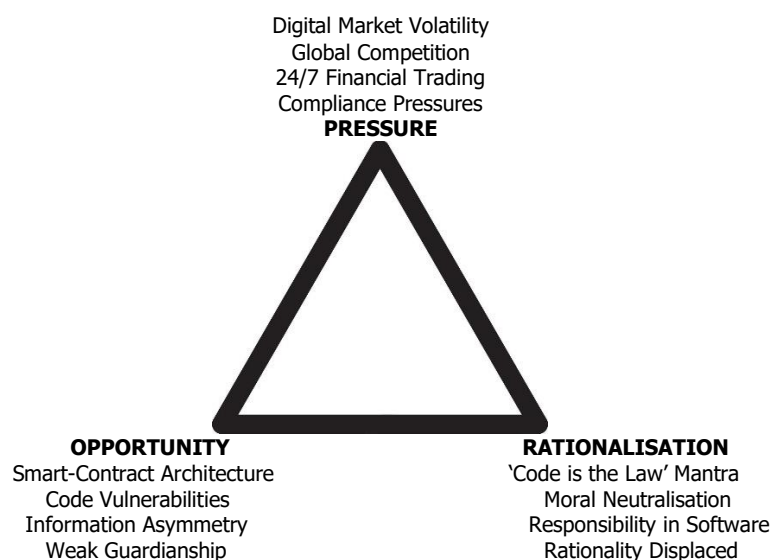


Figure 1. Adapted Model of Cressey's Fraud Triangle

Donald Cressey's Fraud Triangle is a classic model that explains why otherwise honest employees commit workplace fraud by breaking down the phenomenon into three essential, interacting components – Pressure, Opportunity and Rationalisation. Pressure represents the initial motivation, often stemming from an unshareable financial problem like significant debts or expensive habits. Opportunity represents the perceived ability to execute the fraud and abuse a position of trust without getting caught. Rationalisation represents the internal psychological justification that allows the perpetrator to reconcile the illegal act with their self-image as an honest person. According to Cressey's framework, fraud rarely occurs in a vacuum, it is the toxic convergence of these three factors that ultimately drives an individual to cross ethical lines (Cressey, 1953).

While blockchain advocates frequently present smart contracts as mechanisms that eliminate opportunities for fraud, criminological theory suggests technological innovation rarely removes criminal opportunity. Instead, it reshapes the environments within which offending occurs (Rijanto, 2021). The Fraud Triangle provides a useful framework for examining this transition (Almalita and Tjahjono, 2026), and an adapted model (Figure 1.).

Table 2. Business crime vulnerabilities in smart contracting mapped to the adapted Fraud Triangle and guardianship

Vulnerability	Fraud Triangle vertex / RAT element	Illustrative incident	Legal or instrument response
Code complexity and developer–user information asymmetry	Opportunity	Re-entrancy exploitation in the 2016 DAO incident	Attribution of automated system actions to deploying persons
Dependence on external data feeds	Opportunity; weak guardianship	Oracle price manipulation	Transparency, redundancy, and auditability requirements for oracle providers
Flash-loan price distortion	Motivated offender; opportunity	Flash-loan attacks on lending and collateral systems	Judicial scrutiny of mistake, fraud, and unexpected results (MLAC; ELI)
Token-weighted governance capture	Opportunity; governance	Aragon governance dispute	Private-law treatment of control and transfer
Pseudonymity and fragmented responsibility	Absent capable guardian; rationalisation	Diffusion of liability across developers, validators, and token holders	Responsibility gaps framework; technology-neutral attribution
Immutability foreclosing remedies	Socio-legal rigidity	Automated liquidation during volatility	Retention of court oversight for fraud, mistake, and unauthorised transfers

Vertex A Pressure

Commercial pressure has intensified considerably within digitally interconnected global markets. Modern multinational corporations operate within increasingly volatile environments characterised by instantaneous financial transactions, algorithmic trading, and globally integrated supply chains (Gottschalk and Hamerton, 2024a; Gottschalk and Gunnesdal, 2018; Rijanto, 2021). These pressures may incentivise organisations to prioritise technological innovation over legal robustness, particularly where compliance obligations are perceived as barriers to competitiveness (Gottschalk and Hamerton, 2022). Decentralised financial markets operate continuously across multiple jurisdictions without the temporal limitations of conventional banking systems. Twenty-four-hour trading environments amplify commercial volatility, increasing incentives for market participants to exploit technological vulnerabilities.

Vertex B Opportunity

The opportunity component undergoes the most profound transformation. Smart contracts remove certain opportunities by automating execution, while simultaneously generating entirely new opportunity structures embedded within software architecture (Qian et al., 2023; Tjiam et al., 2021). The complexity of blockchain systems creates substantial informational asymmetries between developers and users. Sophisticated organisations capable of auditing, modifying, or designing smart-contract code possess significant advantages over counterparties who rely on software without fully understanding its operational logic.

Moreover, blockchain ecosystems frequently prioritise decentralisation over institutional oversight. Many decentralised ecosystems deliberately minimise the compliance officers, internal auditors, anti-money-laundering teams, regulators, and judicial enforcement mechanisms that collectively function as capable guardians against misconduct in conventional finance (Gottschalk and Hamerton, 2026). Here, RAT suggests that offending becomes more likely where motivated offenders encounter suitable targets in the absence of effective guardianship (Hutchings and Clayton, 2016).

Vertex C Rationalisation

The rationalisation component assumes a uniquely technological character within blockchain communities (Hutchings and Clayton, 2016; Willison et al., 2018). The slogan ‘code is law’ functions not merely as a technical observation but as a powerful moral neutralisation strategy (Drummer and Neumann, 2020). Individuals exploiting programming vulnerabilities argue that software executed exactly as designed and that no deception occurred, because all participants voluntarily accepted the computational rules governing the system (De Filippi and Hassan, 2016).

This reasoning fundamentally alters ethical evaluation. Rather than asking whether conduct was fair, fraudulent, or exploitative, attention shifts to whether software technically permitted the transaction. Where code authorises wealth extraction, exploitation is reframed as innovation. Such reasoning bears striking similarities to Sykes and Matza’s classic techniques of neutralisation replicated in a technological register. Responsibility is displaced onto software architecture itself, allowing offenders to portray themselves as exceptionally competent participants operating within legitimate market rules.

Oracle Manipulation: Exploiting the Weakest Link

One of the most significant criminogenic vulnerabilities within smart contracting arises not from blockchain technology but from its dependence upon external information (Tjiam et al., 2021). Blockchains are intentionally isolated systems, they cannot independently verify events beyond their own distributed ledger. Consequently, smart contracts rely upon external data providers, known as oracles, to supply information concerning commodity prices, exchange rates, shipping confirmations, weather conditions, customs clearances, and other real-world events (Arora et al., 2024). Although blockchain architecture may itself remain cryptographically secure, contract execution becomes only as reliable as the external information entering the system (Qian et al., 2023).

As a consequence, Oracle providers are highly attractive targets for manipulation. Unlike attacking blockchain consensus mechanisms, manipulating an oracle frequently requires compromising only a single external information source (Arora et al., 2024; Tjiam et al., 2021). Temporary distortion of market prices, falsified shipping confirmations, manipulated commodity indices, or corrupted financial feeds may trigger irreversible contractual execution despite the underlying blockchain functioning exactly as intended.

The empirical magnitude of the problem is substantial and costly (Aspembitova and Bentley, 2023). By the end of 2020, total funds lost to exploits involving oracle manipulation had reached approximately USD 100 million, doubling from approximately USD 50 million earlier that year (Certik, 2025). Empirical studies examining real-world flash-loan attack incidents confirm that price-oracle manipulation remains one of the dominant attack categories, while existing off-chain tools detect only a small fraction of relevant vulnerabilities (Gao et al., 2025; Qian et al., 2023). Such manipulation carries particular significance for international commerce: increasing numbers of supply-chain platforms propose linking automated payment mechanisms directly to shipping milestones, customs documentation, inventory systems, and commodity pricing indices (Küçükaltan et al., 2024). If these external data sources become compromised, even briefly, smart contracts may automatically release payments, liquidate collateral, impose penalties, or transfer ownership despite underlying commercial obligations remaining unfulfilled—an actionable breach of contract.

Flash Loans, Economic Exploits and Automated Commercial Delinquency

Recent developments within decentralised finance illustrate how deterministic software may facilitate highly sophisticated economic exploitation without involving conventional software defects (Gao et al., 2025). Flash loans permit market participants to borrow extremely large quantities of cryptocurrency without collateral, provided the loan is repaid within the same blockchain transaction. While economically innovative, these instruments permit temporary concentration of extraordinary purchasing power capable of influencing relatively illiquid markets (Xu et al., 2022). Sophisticated attackers commonly employ flash loans to manipulate decentralised-exchange prices over extremely short timeframes (Al-Zubaidie and Jebbar, 2024). Price distortions subsequently influence oracle feeds relied upon by independent smart contracts governing lending platforms, collateral management systems, or asset valuations (Arora et al., 2024).

Once manipulated data enters dependent contracts, automated execution proceeds exactly as programmed. Assets may be liquidated at artificially depressed prices, collateral transferred below market value, or contractual rights redistributed in favour of the attacker. Importantly, these incidents often involve no programming defect; the software behaves exactly as intended (Qian et al., 2023). The exploit arises because designers failed to anticipate strategic economic behaviour exploiting interactions between multiple automated systems operating simultaneously.

From a socio-legal perspective, these incidents challenge conventional understandings of fraud (Hamerton and Webber, 2026). Traditional fraud generally requires deception whereas Flash-loan attacks frequently involve no false statements whatsoever. Instead, offenders temporarily reshape market conditions until software voluntarily produces economically advantageous outcomes. The distinction between legitimate arbitrage and unlawful market manipulation becomes correspondingly difficult to define.

Decentralised Autonomous Organisations and the Governance Paradox

The emergence of Decentralised Autonomous Organisations (DAO) further illustrates how blockchain redistributes rather than eliminates governance challenges (Scharfman, 2024; Kharman and Smyth, 2024). DAOs replace conventional corporate hierarchies with decentralised voting systems in which governance tokens determine decision-making authority.

In theory, such arrangements democratise organisational governance by reducing managerial discretion and increasing transparency. In practice, governance itself becomes susceptible to economic capture. Token-based voting legalises coups: anyone can legitimately buy their way to power, and the incentive structure makes takeovers economically rational whenever the cost of acquiring sufficient votes is lower than the expected reward.

The Aragon governance dispute provides a particularly illustrative example (Peña-Calvin et al., 2024). In Aragon activist investors accumulated sufficient governance tokens to influence treasury decisions, they sought to

initiate proposals designed to unlock organisational assets for private financial gain (Morrison et al., 2020). Project developers characterised these actions as a coordinated governance attack. The activist investors argued they were merely exercising governance rights explicitly granted by the protocol. Both positions possessed internal legitimacy - with the software functioned precisely as designed yet its intended democratic governance structure simultaneously enabled concentrated economic extraction.

The earlier 2016 controversy surrounding the original Decentralised Autonomous Organisation (DAO) offers an even more striking precedent. A re-entrancy vulnerability in the code allowed an attacker to drain roughly one-third of the DAO's funds, worth approximately USD 55–60 million in Ether, into a separate 'child DAO.' Crucially, the attacker argued that their actions violated no rules, claiming that the software had functioned exactly as programmed code as law and that the exploit was simply a legitimate application of an explicitly coded feature within the contract (Morrison et al., 2020).

Ultimately, Aragon's founders intervened by transferring assets outside the DAO's autonomous governance structure into a traditional legal entity. Ironically, preserving decentralisation required centralisation (Peña-Calvin et al., 2024; Kharman and Smyth, 2024). These episodes reveal an important socio-legal paradox: where software faithfully implements predetermined governance rules, disputes increasingly concern the legitimacy of outcomes rather than compliance with procedure. Trust therefore re-enters the system through human judgment (Gottschalk and Hamerton, 2022, 2025a; Lukyanenko et al., 2022; Tjiam et al., 2021).

Diffusion of Liability and the Accountability Crisis

Arguably the most profound legal consequence of automated commerce concerns the diffusion of accountability. Here, autonomous software executes commercial decisions approved by geographically dispersed pseudonymous token holders, thus identifying legally responsible actors becomes significantly more difficult (Königs, 2022; Mannobova, 2024). With the geographical diffusion, responsibility fragments across multiple participants - developers may argue they merely produced open-source software, token holders may argue they simply participated in governance, node operators merely validate transactions, and oracle providers merely supplied information. The protocol itself possesses no independent legal personality in most jurisdictions (Hamerton and Webber, 2026).

From a criminological perspective, diffusion of responsibility has long been recognised as reducing perceived personal culpability (Croall, 1992; Gottschalk and Gunnesdal, 2018). Where responsibility becomes collective, individuals frequently experience diminished moral restraint. Increased reliance on Artificial Intelligence and Blockchain governance may unintentionally amplify this phenomenon by dispersing decision-making across thousands of pseudonymous participants.

Recent scholarship on the 'responsibility gap' in artificial intelligence and autonomous systems provides a useful conceptual frame (Simmler, 2024; Königs, 2022; Sio and Mecacci, 2021). Where affected parties cannot obtain explanations for automated decisions, where no human agent can be identified as causally responsible for harmful outcomes, and where no moral subject can bear praise or blame, each of these gaps translates into blockchain ecosystems, where the interaction of immutable code, pseudonymity, and distributed governance renders the ascription of legal and moral responsibility extraordinarily difficult (Sio and Mecacci, 2021).

For multinational corporations, this presents openings for strategic regulatory arbitrage. High-risk commercial activities may be transferred into DAO structures while economic benefits continue flowing towards conventional corporate entities (Mannobova, 2024) with the architecture itself becoming a mechanism of regulatory insulation. Consequently, rather than concealing wrongdoing, blockchain may obscure responsibility.

Emerging International Regulatory Responses

The rapid expansion of blockchain technologies has not occurred in complete regulatory isolation. Although legal responses initially developed in ad hoc and jurisdictionally fragmented ways, international organisations have increasingly recognised that automated contracting presents questions extending beyond conventional electronic-commerce legislation). Recent international instruments acknowledge that automation requires legal governance precisely because software cannot independently resolve disputes concerning fairness, attribution, or public policy (UN, 2024; Busch, 2025; Jin and Park, 2025).

The UNCITRAL Model Law. The UNCITRAL Model Law on Automated Contracting (MLAC) represents one of the most significant recent developments in the regulation of automated transactions, providing the first comprehensive international framework specifically addressing contracts concluded or performed through automated systems (UN, 2024). Rather than creating an entirely new legal category, the MLAC builds upon the existing principles of electronic commerce while recognising that machine-to-machine contracting presents distinct legal challenges that traditional contract law was not designed to address. A central feature of the Model Law is its commitment to the principle of technological neutrality, ensuring that contracts cannot be denied legal validity or enforceability solely because they were formed or executed through automated systems (Busch, 2025; Lohsse et

al., 2026; Rodríguez de las Heras Ballell, 2025). By adopting this approach, the MLAC promotes legal certainty while allowing innovation in automated and digital commerce to develop within established legal frameworks.

Importantly, the MLAC rejects the notion that autonomous software operates independently of human responsibility. Instead, it establishes clear rules for attributing the actions of automated systems to the natural or legal persons who deploy, control, or benefit from them (UN, 2024). Organisations cannot therefore avoid contractual or regulatory obligations simply because software performed the immediate transactional act. This principle is particularly significant in the context of smart contracts and blockchain-based transactions, where contractual performance may occur automatically without direct human intervention. The Model Law makes clear that automation changes the method of performance, not the allocation of legal responsibility.

The MLAC also recognises that automated systems, although functioning precisely as programmed, may nevertheless produce legally undesirable outcomes. Its provisions addressing material error and unexpected results acknowledge that coding errors, inaccurate data inputs, unforeseen interactions between algorithms, or fraudulent manipulation may give rise to disputes requiring legal intervention. Accordingly, the Model Law preserves the ability of courts to consider issues such as mistake, fraud, and the proper attribution of contractual obligations, rather than treating automated execution as conclusive evidence of a legally valid transaction. In doing so, the MLAC reinforces a common theme emerging across modern digital commerce frameworks: while automation and smart contracts can enhance efficiency and reduce reliance on intermediaries, they cannot replace the need for legal accountability, human oversight, and effective remedies where fraud or injustice occurs.

The ELI Principles. The European Law Institute (ELI) Principles on Blockchain Technology, Smart Contracts and Consumer Protection (ELI, 2022) provide a framework for integrating blockchain technology and smart contracts within existing legal systems while safeguarding consumer rights (Uzelac, 2025). Unlike technical approaches that view smart contracts as self-sufficient, the ELI Principles emphasise that they operate within established principles of contract, consumer, and private law. Although smart contracts can automate contractual performance through distributed ledger technology, they do not replace the legal requirements of consent, capacity, fairness, or legality. Consequently, the automated execution of contractual terms does not prevent courts from determining whether an agreement is void, voidable, or unenforceable due to fraud, mistake, misrepresentation, or other legal defects.

The Principles also recognise both the strengths and limitations of trustless transactions. Blockchain technology enables parties to transact without relying on trusted intermediaries because cryptographic verification and consensus mechanisms ensure that agreed instructions are executed as programmed. However, trustless execution does not eliminate fraud or misconduct. Transactions may still result from phishing attacks, stolen private keys, coding vulnerabilities, or deceptive practices that undermine genuine consent. In these circumstances, the blockchain faithfully executes the transaction, but the legal validity of the transfer remains open to challenge. The ELI Principles therefore reinforce that legal oversight remains essential to allocate responsibility, resolve disputes, and provide remedies where automated systems execute transactions tainted by fraud or illegality.

From a consumer protection perspective, the ELI Principles advocate transparency, accountability, and effective legal remedies to ensure that technological innovation does not weaken existing legal safeguards. They encourage smart contracts to be understandable to users rather than existing solely as computer code and recognise that consumers must continue to benefit from applicable statutory protections despite the automated and potentially irreversible nature of blockchain transactions (Busch et al., 2025). In doing so, the Principles demonstrate that the success of smart contracts depends not only on technological efficiency but also on the continued application of legal principles that promote fairness, prevent abuse, and maintain confidence in digital commerce.

FATF Standards. The Financial Action Task Force (FATF) is the leading international body responsible for developing and promoting policies to combat money laundering, terrorist financing, and other threats to the integrity of the global financial system. It achieves these objectives by working closely with a network of regional partner organisations, which collectively monitor, assess, and promote compliance with FATF standards across most jurisdictions worldwide (Gottschalk and Hamerton, 2022).

In 2018–2019, the FATF expanded its regulatory framework to address the money laundering and terrorist financing risks associated with virtual assets and virtual asset service providers (Pavlidis, 2020). A key component of these reforms is Recommendation 16, commonly known as the 'Travel Rule,' which requires virtual asset service providers to transmit originator and beneficiary information for virtual asset transfers above specified thresholds (Abdullaeva, 2025).

Despite widespread adoption, implementation has been inconsistent. By 2025, more than 85 jurisdictions had enacted Travel Rule legislation, yet only 35 had undertaken meaningful enforcement actions. In addition, the ongoing 'sunrise issue' where transactions occur between jurisdictions with differing implementation timelines - continues to hinder effective cross-border supervision and regulatory compliance (Takei and Shudo, 2024; Gottschalk and Hamerton, 2022, 2026).

The UNIDROIT Principles. The UNIDROIT Principles on Digital Assets and Private Law, published in 2023, represent the first comprehensive international attempt to harmonise private law rules governing digital assets (UNIDROIT, 2023). Unlike regulatory frameworks such as the Financial Action Task Force (FATF) Recommendations, which focus primarily on anti-money laundering and counter-terrorist financing, the UNIDROIT Principles address the private law challenges arising from digital assets, including ownership, transfer, custody, secured transactions, and insolvency. Recognising the legal uncertainty created by distributed ledger technology (DLT), the Principles adopt a technology-neutral approach capable of accommodating cryptocurrencies, tokenised securities, and other blockchain-based assets. Although the Principles are not legally binding, they provide a model framework for legislators, courts, and commercial parties, promoting greater legal certainty and consistency in cross-border digital asset transactions (Kanda, 2026).

A significant feature of the Principles is their recognition that blockchain technology enables trustless transactions, whereby parties can transact without relying on a central intermediary because the distributed ledger and cryptographic verification mechanisms provide assurance that contractual obligations will be executed as agreed. While this technological innovation reduces certain transactional risks, the Principles acknowledge that it cannot eliminate legal disputes or fraudulent conduct. Smart contracts may execute automatically, but they cannot independently determine whether consent was obtained through fraud, whether a transaction resulted from theft or coercion, or whether an asset was transferred in breach of fiduciary or contractual obligations.

To address these limitations, the Principles introduce the concept of control as the functional equivalent of possession, enabling existing private law doctrines governing ownership, transfer, and priority to operate effectively in respect of digital assets. They also preserve the role of courts and legal remedies in cases involving fraud, mistake, or unauthorised transfers, ensuring that technological automation does not displace the broader objectives of commercial law. In doing so, the Principles demonstrate that trustless technology and legal oversight are complementary rather than contradictory: blockchain can reduce the need for institutional trust in routine transactions, while private law remains essential for resolving disputes, protecting good-faith acquirers, and maintaining confidence in digital asset markets (Smith and Weise, 2026). Collectively, these international initiatives demonstrate that legal systems increasingly reject the proposition that blockchain technologies operate beyond conventional legal doctrine.

Table 3. Comparative overview of the international instruments examined

Instrument	Year	Core focus	Contribution to business-crime risk reduction
UNCITRAL Model Law on Automated Contracting	2024	Automated contracting; technological neutrality	Attributes actions of automated systems to those who deploy, control, or benefit from them; preserves remedies for material error and unexpected results
ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection	2022	Consumer protection within existing contract and private law	Confirms that automated execution does not prevent review of consent, fairness, or legality
FATF virtual-asset standards (incl. Recommendation 16, the Travel Rule)	2018-2019	AML/CFT for virtual assets and service providers	Requires originator and beneficiary information for transfers above specified thresholds
UNIDROIT Principles on Digital Assets and Private Law	2023	Private law of digital assets	Introduces control as the functional equivalent of possession; preserves remedies for fraud, mistake, and unauthorised transfer

DISCUSSION

The findings presented above sustain three connected claims about trust, opportunity, and responsibility in automated commerce. Trust is relocated rather than eliminated. The socio-legal analysis showed that immutable execution suppresses the doctrines - good faith, frustration, proportionality, unconscionability - through which contract law absorbs uncertainty, while jurisdictional fragmentation displaces the territorial connecting factors on which private international law depends. Read alongside the Luhmann-influenced literature on automation, these are not failures of trust but transfers of it: authority moves from courts and regulators to developers, oracle providers, and token-weighted governance structures whose decisions are neither readily visible nor routinely reviewable (Lukyanenko et al., 2022; Luhmann, 1995). The Aragon dispute, resolved by transferring assets into a conventional legal entity, and the DAO, resolved by a coordinated hard fork, each demonstrate that human judgment re-enters the system precisely where deterministic governance proves insufficient (Peña-Calvin et al., 2024; Morrison et al., 2020). This supports P1 and extends prior work arguing that trust in automated systems requires institutional anchors.

The criminogenic conditions are reorganised rather than removed. The adapted Fraud Triangle and Routine Activity Theory together explain why automated execution neither reduces nor simply relocates offending: opportunity is embedded in code complexity and information asymmetry, pressure is amplified by continuous global markets, and rationalisation is supplied by a technological ideology in which the software's compliance becomes the measure of the conduct's legitimacy. Oracle manipulation and flash-loan exploits are not coding defects; they are the predictable output of concentrated opportunity, motivated offenders, and the deliberate absence of capable guardianship (Hutchings and Clayton, 2016; Cohen and Felson, 1979). This finding both supports and qualifies prior white-collar crime research: where Schuchter and Levi (2015) found elite fraudsters offending without obvious financial pressure, the present analysis suggests that in automated markets rationalisation and opportunity may carry more explanatory weight than pressure - supporting P2 and indicating that the Fraud Triangle requires reweighting, not abandonment, in digital environments.

Responsibility remains a legal question. The instruments examined converge on a durable principle: automation changes the means by which obligations are performed, not the principles by which responsibility is allocated. They diverge, however, in emphasis. The MLAC attributes system actions to those who deploy, control, or benefit from them; the ELI Principles preserve judicial scrutiny of consent and fairness; the FATF standards target laundering through intermediaries; and the UNIDROIT Principles address private-law incidents of control and transfer. None addresses oracle governance directly - the most conspicuous vulnerability identified in the results - which is why the framework proposed in the next section treats oracle oversight as a condition of accountability rather than an adjunct to it. This supports P3 and answers the gap identified in the literature review.

These interpretations are subject to the limitations noted above: the analysis is doctrinal and conceptual rather than empirical, it draws on a bounded set of illustrative incidents, and the regulatory instruments examined are recent and, in most jurisdictions, not yet fully implemented. The claims advanced are therefore best read as an analytical framework for a fast-moving field rather than as settled conclusions.

Towards a Legally Embedded Framework

Although emerging international instruments represent substantial progress, they remain largely reactive. Most address disputes after automated harm has occurred rather than redesigning commercial systems to prevent such harm from arising (Seneviratne, 2024).

The next phase of international commercial regulation should therefore move beyond technological neutrality towards a proactive legally embedded model of law-by-design (Prifti et al., 2024). Legal-by-design concepts do not reject the impact of automation and technological change within the globalised commercial sphere, rather, it rejects the assumption that computational efficiency should displace legal judgment (Almada, 2023). Thus technological architecture should deliberately embed the procedural values historically protected by commercial law.

Human-in-the-Loop Governance. Automated commercial systems should incorporate mandatory human-in-the-loop governance mechanisms (Lazcoz and de Hert, 2023; Cingillioglu and Lun, 2026). Complete contractual immutability has often been presented as blockchain's defining advantage; yet legal history demonstrates that absolute rigidity rarely produces commercial justice. Courts retain equitable jurisdiction precisely because exceptional circumstances inevitably arise.

Smart contracts governing significant commercial transactions should include authenticated pause, review, or override capabilities capable of temporarily suspending execution where credible allegations of fraud, oracle compromise, coercion, sanctions violations, or manifest injustice exist. Various technical mechanisms can support such intervention: pause patterns set Boolean flags disabling sensitive functions; emergency-stop patterns enable phased interruption; upgradeable contracts and proxy patterns allow underlying logic to be amended while preserving contract identity (Seneviratne, 2024). The DAO hard fork itself demonstrated that even ostensibly immutable chains can be updated through coordinated consensus when the community judges the outcome of pure code execution to be unacceptable.

Some argue that regulatory mechanisms such as identity verification, transaction monitoring, and compliance obligations undermine the decentralised ethos of blockchain technology by reintroducing centralised oversight and reducing user anonymity. From this perspective, these requirements appear incompatible with the original vision of decentralised financial systems that operate without trusted intermediaries. However, this view arguably misunderstands the role and purpose of commercial law (Prifti et al., 2024). The objective of commercial law has never been to maximise technological automation or preserve complete decentralisation. Rather, its purpose is to provide legal certainty, promote market integrity, facilitate legitimate commercial activity, and protect participants from fraud, money laundering, terrorist financing, and other forms of financial abuse. Accordingly, the inclusion of human oversight within blockchain-based financial systems should not be regarded as a technological failure. Instead, it reflects institutional resilience by ensuring that automated systems remain accountable, can be subject to legal scrutiny, and allow regulatory intervention where necessary. In this way, human oversight

complements technological innovation by strengthening trust, legitimacy, and the long-term sustainability of digital financial markets.

Technology-Neutral Liability and the Regulation of Oracle Infrastructure. Liability should attach to commercial benefit rather than to technological architecture. Corporate entities increasingly possess opportunities to distribute operational functions across complex networks of subsidiaries, DAOs, software developers, validators, and decentralised governance structures. Without clear attribution rules, these arrangements risk becoming mechanisms for regulatory arbitrage (Almada, 2023; Berdibayev, 2026).

International commercial law should therefore adopt technology-neutral attribution principles: where organisations materially design, finance, control, or profit from autonomous commercial systems, they should remain jointly responsible for foreseeable harms generated through those systems (Berdibayev, 2026; Mannobova, 2025). Automation should not become a mechanism for externalising legal responsibility. Regulatory attention must also extend beyond blockchain protocols themselves towards oracle infrastructure (Pavlidis, 2020; van der Vlist et al., 2024). External data providers represent one of the most significant vulnerabilities within automated commerce, yet oracle governance remains comparatively underdeveloped.

International standards should establish minimum requirements concerning transparency, redundancy, auditability, and conflict-of-interest management (Pavlidis, 2020). Multi-source verification, decentralised oracle networks, time-weighted average pricing mechanisms, independent certification, and runtime-invariant guards such as deviation checks should become standard components of commercial blockchain infrastructure. Just as modern financial markets regulate credit-rating agencies, auditors, and payment systems, equivalent oversight should apply to entities supplying critical information upon which automated commercial decisions depend. Trust cannot be eliminated from commercial relationships; it can only be relocated. Thus, a primary objective of legal reform should be ensuring that trust remains anchored within accountable institutions rather than opaque technological systems.

CONCLUSION

The smart contract now occupies a near-central position in debates about the future of commercial law. Its proponents promise efficiency, certainty, and a decisive break from the imperfections of human intermediation. The preceding analysis has shown that this promise rests on assumptions the technology itself cannot honour. Smart contracts do not eliminate trust; they migrate it. They do not remove the conditions that produce commercial wrongdoing; they restructure them. And they do not render legal institutions obsolete; they reposition those institutions at precisely the points, automated execution, distributed governance, and reliance on external information, where deterministic systems most thoroughly exceed their own capacity for self-correction. Three main findings carry forward from this brief inquiry.

That the socio-legal displacement produced by automated execution is more substantial than its advocates acknowledge. Immutability, celebrated as blockchain's defining virtue, systematically excludes the doctrinal flexibility - good faith, proportionality, frustration, mistake, unconscionability through which contract law has historically absorbed uncertainty and corrected injustice. What is gained in determinism is forfeited in adjudicated fairness, and the balance tips further as automated systems acquire responsibility for transactions of greater commercial and humanitarian weight.

Additionally, the criminological analysis grounded in the adapted Fraud Triangle demonstrates that criminal opportunity in digital commerce is reorganised rather than removed. Pressures intensify within continuously operating and globally integrated markets. Opportunities proliferate in code complexity, information asymmetry between developers and counterparties, automated market-making protocols, the structural absence of capable guardianship, and the governance vulnerabilities inherent in token-based decision-making. Rationalisation evolves in step with the technology itself, finding renewed expression in the doctrine that "code is law."

Furthermore that the relevant international instruments: the UNCITRAL Model Law on Automated Contracting; the ELI Principles; the FATF standards; and the UNIDROIT Principles on Digital Assets, share a common and probably durable insight: automation changes the means by which legal obligations are performed, but it does not alter the principles by which they are allocated. Attribution, accountability, and remedy remain legal questions; they cannot be outsourced to code.

These findings converge on a single conclusion with practical consequence. This article has accordingly called for a shift away from the ideology of trustless commerce towards a legally embedded framework in which automation operates alongside, and subject to, the established principles of commercial law. Human-in-the-loop governance, technology-neutral attribution of liability, transparent and rigorous oversight of oracle infrastructure, and internationally harmonised standards on automated contracting should become foundational commitments for the next generation of digital-commerce regulation - not in tension with innovation, but as the conditions under which innovation becomes durable.

Technology will continue to advance faster than doctrine. That is not, on its own, harmful. The harm arises when legal systems mistake this lag for irrelevance, or accept the rhetoric of trustlessness as a description of reality rather than an aspiration of design. The future utility of smart contracts will be measured less by the cleverness of their code than by the seriousness with which their surrounding legal environment is constructed. A genuinely trustworthy system of automated commerce is one in which the institutions accompanying it courts, regulators, standard-setters, oracle auditors, and governance bodies are as deliberately designed as the contracts themselves. That is the model that this article has tentatively sought to advance

REFERENCES

- Abdullaeva, S. (2025). FATF standards and the implementation of the travel rule in preventing crypto-related money laundering. *Science of the New Era*, 10(7): 17-24
- Al-Zubaidie, M., & Jebbar, W. A. (2024). Providing Security for Flash Loan System Using Cryptocurrency Wallets Supported by XSalsa20 in a Blockchain Environment. *Applied Sciences*, 14(14): 6361. <https://doi.org/10.3390/app14146361>
- Alimohammadlou, M., & Alinejad, S. (2023). Challenges of blockchain implementation in SMEs' supply chains: an integrated IT2F-BWM and IT2F-DEMATEL method. *Electronic Commerce Research* 25: 907–949. <https://doi.org/10.1007/s10660-023-09696-3>
- Almada M. (2023). Regulation by Design and the Governance of Technological Futures. *European Journal of Risk Regulation*. 14(4): 697-709.
- Almalita, Y. & Tjahjono, R. S. (2026). Reframing Deception: Redefining the Fraud Triangle in the Era of Ethical Governance. *Owner : Riset Dan Jurnal Akuntansi*, 10(1), 527-545.
- Arora, S., Li, Y., Feng, Y., Zhang, R., & Guan, C. (2024). SecPLF: Secure protocols for loanable funds against oracle manipulation attacks. In: *ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*: 1394 - 1405
- Aspembitova, A. T., & Bentley, M. A. (2023). Oracles in Decentralized Finance: Attack Costs, Profits and Mitigation Measures. *Entropy*, 25(1): 60. <https://doi.org/10.3390/e25010060>
- Barcentewicz, M., Sarch, A. and Vasan, N. (2024). Battle of the Crypto Bots: Automated Transaction Copying in Decentralized Finance. *University of Pennsylvania Journal of Business Law*. 26: 672. <https://doi.org/10.58112/jbl.26-3.2>
- Bassan, F. & Rabitti, M. (2024). From smart legal contracts to contracts on blockchain: An empirical investigation, *Computer Law & Security Review*, 55: 106035. <https://doi.org/10.1016/j.clsr.2024.106035>
- Bratspies, R. M. (2018). Cryptocurrency and the Myth of the Trustless Transaction, *Michigan Technology Law Review*. 25(1). Available at: <https://repository.law.umich.edu/mtlr/vol25/iss1/2>
- Berdibayev, S. (2026). Modern form of Law Evasion in International Private Law under the Conditions of the Digital Economy and Mechanisms for Combating. *International Journal of Law and Policy*, 4(1), 55–79.
- Brownsword R. (1996). Good Faith in Contracts Revisited, *Current Legal Problems*, 49 (1): 111–157, <https://doi.org/10.1093/clp/49.1.111>
- Bui, Q.T., & Le, S.T. (2025). Barriers to Blockchain Technology Implementation in Small and Medium-Sized Logistics Enterprises. *Sage Open*, 15(3). <https://doi.org/10.1177/21582440251367622>
- Busch C. (2025). Consumer Law for AI Agents. *German Law Journal*. 26 (7):1367-1382. <https://doi.org/10.1017/glj.2026.10188>
- Busch, C., Sørensen, M.J., Rodriguez de las Heras Ballell, T. & Twigg-Flesner, C. (2025). Towards the Next Generation of Consumer Law: the ELI Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts. *Journal of European Consumer and Market Law*, 14(3): 89-91. <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/14.3/EuCM L2025014>
- Certik. (2025). Oracle Wars: The Rise of Price Manipulation Attacks, *Technical Insights Vulnerability Research*, May 6. Available at: <https://www.certik.com/blog/oracle-wars-the-rise-of-price-manipulation-attacks>
- Cingillioglu, I., & Lun, P. (2026). From AI to AGI: a human-in-the-loop framework for responsible IS futures. *Enterprise Information Systems*. Online first, available here: <https://doi.org/10.1080/17517575.2026.2653244>
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Cornelius, K.B. (2018). Standard form contracts and a smart contract future. *Internet Policy Review*, 7(2). <https://doi.org/10.14763/2018.2.790>
- Cozzolino, A., Ippolito, M., Ercolano, S., & Giannone, D. (2026). Experts and the people: technocrats in government and the shifting patterns of political participation. *International Political Science Review*. Online first, available: <https://doi.org/10.1177/0192512126142544>
- Cressey, D. (1953). Other people's money: a study in the social psychology of embezzlement. *Glencoe: Free Press*.
- Croall, H. (1992). White Collar Crime: Criminal Justice and Criminology. *Milton Keynes: Open University Press*.
- Di Nicola A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organised Crime*. Online first, available at: <https://doi.org/10.1007/s12117-022-09457-y>

- Ding, H., Li, Q., Wang, C., Ren, H. Li, J., Piao, X., Song, H. and Ji, Z. (2026). How far should we go away from smart contract to smarter contractor? *A systematic review, Blockchain: Research and Applications*, 7(5): 100402. <https://doi.org/10.1016/j.bcr.2025.100402>
- De Filippi, P. D., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, 21(12). <https://doi.org/10.5210/fm.v21i12.7113>
- Draganidis S. (2023). Jurisdictional arbitrage: combatting an inevitable by-product of cryptoasset regulation. *Journal of Financial Regulation and Compliance*, 31(2): 170–185. <https://doi.org/10.1108/JFRC-02-2022-0013>
- Drummer, D., & Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology*, 35(4): 337–360.
- European Law Institute (ELI) (2022). ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. *Report of the European Law Institute, Vienna: EU*. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection.pdf
- European Securities and Markets Authority (ESMA) (2023). Decentralised Finance in the EU: Developments and risks, ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis, Paris: EU. https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf
- Gao, C., Ye, j., Yang, W. and Xue, Y. (2025). Flash Loan Attack is More Than Just Price Oracle Manipulation: A Comprehensive Empirical Study. *2025 25th International Conference on Software Quality, Reliability and Security (QRS), Hangzhou, China, 2025*, pp. 691–702, doi: <https://doi.org/10.1109/QRS65678.2025.00073>
- Gottschalk, P., & Gunnesdal, L. (2018). White-Collar Crime in the Shadow Economy: Lack of Detection, Investigation and Conviction Compared to Social Security Fraud. London: Palgrave Macmillan.
- Gottschalk, P. and Hamerton, C. (2021). White-Collar Crime Online: Deviance, Organizational Behaviour and Risk. Chambery: Palgrave Macmillan. <https://link.springer.com/book/10.1007/978-3-030-82132-6>
- Gottschalk, P. and Hamerton, C. (2022). Corporate Compliance: Crime, Convenience and Control, Chambery: Palgrave Macmillan. <https://link.springer.com/book/10.1007/978-3-031-16123-0>
- Gottschalk P. & Hamerton C. (2024a), Categories of white-collar offenders based on the theory of convenience. *Journal of Forensic Practice*, 26(4): 219–228, doi: <https://doi.org/10.1108/JFP-04-2024-0014>
- Gottschalk, P. and Hamerton, C. (2024b). Understanding Business Offenders: A Comparative Analysis of Workplace Deviance, Convenience and Control. Oxford: Berghahn Books. <https://doi.org/10.3167/9781805397892>
- Gottschalk, P. and Hamerton, C. (2025a). Economic Crime and Conceptions of Trust: Offender Convenience by Organizational Opportunity. Chambery: Palgrave Macmillan. <https://link.springer.com/book/10.1007/978-3-031-82315-2>
- Gottschalk, P. and Hamerton, C. (2025b). Characteristics of Crime Convenience: The Case of Corporate Offenders. *Deviant Behavior*, 46(3): 288–298. <https://doi.org/10.1080/01639625.2024.2341088>
- Gottschalk, P. and Hamerton, C. (2026). The Business of Examining Fraud: Comparative Perspectives on Economic Crime, Discovery and Review. London: World Scientific. <https://doi.org/10.1142/14843>
- Gratton, G., & Edenhofer, J. (2025). The rise and fall of technocratic democracies: unstable majorities and delegation to technocrats. *Journal of European Public Policy*, 1–30. <https://doi.org/10.1080/13501763.2025.2576160>
- Grillot, C. (2016). Trust facilitates business, but may also ruin it: the hazardous facets of Sino-Vietnamese border trade. *Asian Anthropology*, 15(2), 169–185. <https://doi.org/10.1080/1683478X.2016.1216281>
- Howells, G. (2020). Protecting Consumer Protection Values in the Fourth Industrial Revolution. *Journal of Consumer Policy* 43: 145–175. <https://doi.org/10.1007/s10603-019-09430-3>
- Hamerton, C. (2020). White-collar cybercrime: evaluating the redefinition of a criminological artifact. *Journal of Law and Criminal Justice*, 8 (2): 67–79. DOI: <https://doi.org/10.15640/jlcj.v8n2a6>
- Hamerton, C. and Webber, C. (2026). Precarious Futures: Crime, Technology and the Web. Chambery: Palgrave Macmillan. <https://link.springer.com/book/9783030868604>
- Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior*, 37(10), 1163–1178. <https://doi.org/10.1080/01639625.2016.1169829>
- Jin, H.-S., & Park, K.-S. (2025). Legal analysis of the UNCITRAL Model Law on Automated Contracting and its implications for digital trade contracts. *International Commerce and Law Review*: 108: 1–31. <https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE12550797>
- Junger, M., Wang, V. & Schlömer, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. *Crime Science*, 9: 13. <https://doi.org/10.1186/s40163-020-00119-4>
- Kanda, H. (2026). Brief Overview of Unidroit Principles on Digital Assets and Private Law. In: Pastor Sempere, C., Morán Bovio, D.A. (eds) UNIDROIT Principles on Digital Assets and Private Law. *Law, Governance and Technology Series, vol 80*. Chambery: Springer. https://doi.org/10.1007/978-3-032-11001-5_1
- Kharman, A. M., & Smyth, B. (2024). Perils of current DAO governance, Computers & Society. arXiv: <https://doi.org/10.48550/arXiv.2406.08605>
- Königs, P. (2022). Artificial intelligence and responsibility gaps: what is the problem?. *Ethics and Information Technology*, 24: 36. <https://doi.org/10.1007/s10676-022-09643-0>

- Kozak-Isik, G. (2026). Relative, Relational, and Affective: Rethinking Legal Consciousness Under Legal Pluralism. *Social & Legal Studies*, 35(3), 371-402. <https://doi.org/10.1177/09646639251379869>
- Küçükaltan, B., Kamasak, R., Yalcinkaya, B., & Irani, Z. (2024). Investigating the themes in supply chain finance: the emergence of blockchain as a disruptive technology. *International Journal of Production Research*, 62(22), 8173–8192. <https://doi.org/10.1080/00207543.2022.2118886>
- Lazcoz, G. & de Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities. *Computer Law & Security Review*, 50: 105833. <https://doi.org/10.1016/j.clsr.2023.105833>
- Lessig, L. (1999). Code and Other Laws of Cyberspace, New York: *Basic Books*.
- Loke, A. (2020). Mistakes in Algorithmic Trading of Cryptocurrencies. *The Modern Law Review*, 83: 1343-1353. <https://doi.org/10.1111/1468-2230.12574>
- Lohsse, S., Schulze, R. & Staudenmayer, D. (2026) AI-Contracting. Münster Colloquia on EU Law and the Digital Economy IX. *Baden-Baden: Nomos*, 2026. <https://doi.org/10.5771/9783748963097>
- Luhmann, N. (1995). Social systems (J. Bednarz Jr. & D. Baecker, Trans.). Redwood: *Stanford University Press*.
- Lukyanenko, R., Maass, W. & Storey, V.C. (2022). Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities. *Electronic Markets* 32, 1993–2020. <https://doi.org/10.1007/s12525-022-00605-4>
- Madarie, R., Weulen Kranenbarg, M., & de Poot, C. (2026). Cybersecurity Expert Perspectives on Data Thieves' Actions in Digital Environments: Potential Refinements for Routine Activity Theory. *Deviant Behavior*, 47(3): 544–562. <https://doi.org/10.1080/01639625.2025.2453440>
- Mannobova, G. (2024). The “accountability gap” in autonomous systems: Reconciling legal personhood with algorithmic opacity. *ZDIF*, 4(31): 142-148. <https://doi.org/10.5281/zenodo.18042463>
- McGuire, M. (2012). Technology Crime and Justice: The Question Concerning Technomia, Oxford: *Routledge*. <https://www.routledge.com/Technology-Crime-and-Justice-The-Question-Concerning-Technomia/McGuire/p/book/9781843928560>
- Moore, M. (1999). Truth, trust and market transactions: What do we know? *The Journal of Development Studies*, 36(1): 74–88. <https://doi.org/10.1080/00220389908422612>
- Morrison R., Mazey N. & Wingreen S.C. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance?. *Frontiers of Blockchain* 3:25. <https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00025/full>
- Nelken, D. (2025). Out of time? Going back to the Cotterrell–Nelken debate. *Journal of Law and Society*. 52(1): S62–S69. <https://doi.org/10.1111/jols.70002>
- Onțanu, E. A., & Tjong Tjin Tai, E. (2025). Digital Technology and Procedural Justice: Towards a Geography of Justice. *Tilburg Law Review*, 30(2), 96–119. <https://doi.org/10.5334/tilr.422>
- Oster, J. (2021). Code is code and law is law - the law of digitalization and the digitalization of law. *International Journal of Law and Information Technology*, 29(2): 101-117. <https://doi.org/10.1093/ijlit/eaab004>
- Pavlidis, G. (2020). International regulation of virtual assets under FATF's new standards. *Journal of Investment Compliance*, 21(1): 1–8. <https://doi.org/10.1108/JOIC-08-2019-0051>
- Peña-Calvin, A., Saldivar, J., Arroyo, J. and Hassan, S. (2024). A Categorization of Decentralized Autonomous Organizations: The Case of the Aragon Platform. in *IEEE Transactions on Computational Social Systems*, 11 (6) 8143-8155. doi: <https://doi.org/10.1109/TCSS.2023.3299254>.
- Pinheiro, L. (2023). Laws Applicable to International Smart Contracts and Decentralized Autonomous Organizations (DAOS). *International Journal of Cryptocurrency Research*, 3(1). <http://dx.doi.org/10.2139/ssrn.4467408>
- Prifti, K., Morley, J., Novelli, C. (2024). Regulation by Design: Features, Practices, Limitations, and Governance Implications. *Minds & Machines* 34, 13. <https://doi.org/10.1007/s11023-024-09675-z>
- Qian, P., Cao, R., Liu, Z., Xiao, Y., & Chen, X. (2023). Empirical review of smart contract and DeFi security: Cryptography and Security. arXiv. <https://doi.org/10.48550/arXiv.2309.02391>
- Rodríguez de las Heras Ballell, T. (2025). Digital Vulnerability in Automated Contracting: The Problem of Unexpected Outcomes. Contract-Law Remedies or Liability?. In: Crea, C., Infantino, M. (eds) Remedies to Digital Vulnerability in European Private Law. *DiVE 2025*. Chambery: Springer. https://doi.org/10.1007/978-3-032-19720-7_13
- Rodríguez, López (2025) Consumer protection in blockchain-based metaverses: a comparative study of cross-border legal gaps and platform governance. *Frontiers of Blockchain* 8:1675735. <https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1675735/full>
- Rijanto, A. (2021). Blockchain Technology Adoption in Supply Chain Finance. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(7): 3078-3098. <https://doi.org/10.3390/jtaer16070168>
- Sio, Santoni de., Mecacci, G. (2021). Four Responsibility Gaps with Artificial Intelligence: Why they Matter and How to Address them. *Philosophy and Technology*. 34, 1057–1084. <https://doi.org/10.1007/s13347-021-00450-x>
- Scharfman, J. (2024). Decentralized Autonomous Organization (DAO) Fraud, Hacks, and Controversies. In: *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II*. Chambery: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-60836-0_3
- Schuchter, A., & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, 39(3), 176–187. <https://doi.org/10.1016/j.accfor.2014.12.001>

- Scott, C. (2004). Regulation in the Age of Governance: The Rise of the Post-Regulatory State. In: The Politics of Regulation. *Jacint Jordana and David Levi-Faur (eds.)*. Cheltenham: Edward Elgar. <https://doi.org/10.4337/9781845420673.00016>
- Selçuk, S., Nesibe, K.K., Serkan K. (2025). AI-driven civil litigation: Navigating the right to a fair trial. *Computer Law & Security Review*, 57: 106136. <https://doi.org/10.1016/j.clsr.2025.106136>
- Seneviratne, O. (2024). The feasibility of a smart contract "kill switch" Cryptography and Security , arXiv. <https://doi.org/10.48550/arXiv.2407.10302>
- Simmler, M. (2024). Responsibility gap or responsibility shift? The attribution of criminal responsibility in human-machine interaction. *Information, Communication & Society*, 27(6), 1142–1162. <https://doi.org/10.1080/1369118X.2023.2239895>
- Smith, E.E. & Weise, S.O. (2026). Unidroit Principles on Digital Assets and Private Law - A Comparison to the Uniform Commercial Code, with an Emphasis on Control, Transfer, Custody, Innocent Acquirers, and Secured Transactions. In: Pastor Sempere, C., Morán Bovio, D.A. (eds) UNIDROIT Principles on Digital Assets and Private Law. *Law, Governance and Technology Series*, 80. Chambray: Springer. https://doi.org/10.1007/978-3-032-11001-5_2
- Smuha, N. A. (2024). From Rule of Law to Algorithmic Rule by Law. In Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law (pp. 151–229). chapter, Cambridge: *Cambridge University Press*.
- Sotiropoulos, L. (2026). The Legal Nature of Smart Contracts: Addressing Errors, Breach, and the Intersection of Blockchain and Contract Law. In I. Efthymiou & K. Kouroupis (Eds.), Legal and Regulatory Impacts on AI Development (pp. 287–310). *IGI Global Scientific Publishing*. <https://doi.org/10.4018/979-8-3373-7996-8.ch009>
- Takei Y., and Shudo, K. (2024). FATF Travel Rule's Technical Challenges and Solution Taxonomy. *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dublin, Ireland, 2024*: 784–799. doi: <https://doi.org/10.1109/ICBC59979.2024.10634360>
- Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, 14(2), 117. <https://doi.org/10.3390/info14020117>
- Tjiam, K., Wang, R., Chen, H., & Liang, K. (2021). Your Smart Contracts Are Not Secure: Investigating Arbitrageurs and Oracle Manipulators in Ethereum. In *Proceedings of the 3rd Workshop on Cyber-Security Arms Race (CYSARM '21)*. Association for Computing Machinery, New York, NY, USA, 25–35. <https://doi.org/10.1145/3474374.3486916>
- UNIDROIT (2023). UNIDROIT Digital Assets and Private Law Principle 2(2). Rome: *UNIDROIT*. <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>
- United Nations (UN) (2024). UNCITRAL Model Law on Automated Contracting with Guide to Enactment. Vienna: *United Nations*. <https://uncitral.un.org/sites/default/files/2424674e-mlautomatedcontracting-rev1-ebook.pdf>
- Uzelac, A. (2025). Principles of civil procedure under ELI-Unidroit rules: convergence through a uniform approach to procedural obligations?, *Uniform Law Review*, 30(1). 18–32, <https://doi.org/10.1093/ulr/unaf017>
- van den Berg, B. (2011). Techno-elicitation: Regulating behaviour through the design of robots. In B. van den Berg, & L. Klaming (Eds.), Technologies on the stand: Legal and ethical questions in neuroscience and robotics (pp. 403–422). *Wolf Legal Publishers (WLP)*.
- van der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241232630>
- Wang, X., & Xu, F. (2022). The Value of Smart Contract in Trade Finance. *Manufacturing & Service Operations Management*, 25(6):2056–2073. <https://doi.org/10.1287/msom.2022.1126>
- Willison, R., Warkentin, M., & Johnston, A. C. (2018) Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28: 266–293. doi: <https://doi.org/10.1111/isj.12129>.
- Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN, (March 10, 2015). Available at: <http://dx.doi.org/10.2139/ssrn.2580664>
- Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2023). SoK: Decentralized exchanges with automated market maker protocols, Trading and Market Microstructure, arXiv. <https://doi.org/10.48550/arXiv.2103.12732>
- Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–136. <https://doi.org/10.1080/1369118X.2016.1186713>
- Zetsche, D. A., Buckley, R. P., & Arner, D.W. (2018). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review*. 1361–1407.