LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 24, NO. 1(2026)

RECONCILING LEGAL FRAMEWORKS: ALIGNING SMART CONTRACT INFLEXIBILITY WITH CONSUMER SAFEGUARDING REGULATIONS

Adi Suranta Ginting[1], Bernard Nainggolan[2], Adi Sulistyono[3] & Dhaniswara K. Harjono[4]

Abstract
Self-executing digital agreements automatically implement encoded conditions, providing enhanced efficiency and clarity in online transactions. Yet, their unchangeable nature within distributed ledger systems presents substantial obstacles for safeguarding user interests, particularly following implementation mistakes or financial damages. Conventional judicial mechanisms struggle to offer corrective measures after these agreements complete execution, having been constructed for modifiable transactions requiring human intervention. Although contemporary regulatory developments such as MiCA and platform-specific remedies show advancement, they remain disjointed and inadequate for comprehensive protection. This investigation employs combined methodologies—examining 153 scholarly articles (2018-2025) from Scopus using targeted search criteria, analyzing regulatory approaches across EU, Singapore, and Japan, reviewing technical specifications, and evaluating incident cases. Findings reveal persistent deficiencies where regulations emphasize preliminary disclosure yet achieve minimal (<10%) success in resolving post-implementation conflicts. The research proposes an integrated five-tier model incorporating algorithmic openness, automated safeguards, combined governance structures, responsibility allocation, and international coordination.

Keywords: Computational Transparency; Distributed Ledger Permanence; User Rights Protection; Post-Implementation Recourse; Automated Digital Contracts.

1. Introduction

Offering unprecedented efficiency and transparency in digital transactions, smart contracts, or coded sets that execute agreements on their own, will notably promise efficiency and transparency (Szabo, 1997; Buterin, 2014). In different sectors, the transaction volumes will go beyond billions of dollars per year by 2024 (DeFi Llama, 2024). Nevertheless, new markets are characterized by strong barriers such as regulatory and consumer mistrust, as many fraud cases due to unregulated tokens and Decentralized Finance (DEFI) scams have occurred in the new markets (Nguyen et al., 2023; Chen et al., 2023).

Instead, smart contracts follow a deterministic "code is law paradigm", in which they are programmed to give a predefined outcome without judicial intervention of interpretation by a human being (Lessig, 1999; De Filippi and Wright, 2018). This inflexibility is essentially incompatible with the consumer right (withdrawal), challenging unfair conditions, or recovering non-conformity (Werbach and Cornell, 2017). Although blockchain immutability poses inherent challenges to conventional regulatory strategies, and some scholars have shown that some compliance mechanisms are computationally impossible (Charoenwong et al., 2025), new models are emerging that do not promptly consider code and law as antagonistic concepts, but instead allow them to develop jointly through responsible system design (Finck, 2019; Werbach, 2018). Whereas developed jurisdictions, such as the EU, Singapore, and Japan, have formulated extensive regulatory frameworks such as the General Data Protection Regulation (GDPR), Consumer Rights Directive, and technical standards to support the traits of smart contracts (European Commission, 2022; Monetary Authority of Singapore (MAS), 2023; Financial Services Agency (FSA) Japan, 2023), developing countries have been relying on laws in the pre-blockchain era, which do not fully serve the purpose of supportive smart contracts (Sooksripaisarnkit,2023).

The legal systems that have been established currently address only the disclosure requirements pre-contract, and pay little or no attention to consumer protection post-execution in situations where conflicts related to the very implementation of algorithms occur (Raskin, 2016; Savelyev, 2017). The inability to reverse consumer losses once a contract has been

implemented in blockchain makes it extremely challenging to have proper legal redress (Fairfield, 2014; Gikay, 2019). The existing systems lack an algorithmic audit scheme, code based dispute resolution, and even technical requirements that assure consumer friendly design. This does not represent a complete failure of the legal systems but a very fundamental issue of adjustment with the old legal workings of the reversible transactions in the impossibility of the irreversible character of the blockchain implementation (Allen, 2018; Zetzsche et al., 2020).

This paper shall address these gaps by proposing a comprehensive post-execution consumer protection framework that is anchored on algorithmic transparency, mandatory code audit and hybrid governance frameworks. The methodology develops a system of accountability necessities in the smart contract life cycle, which involves a just and equitable digital business that appreciates the consumer rights notwithstanding unchangeable execution. The framework focuses on the consideration of the rigidity of blockchain and the principles of consumer protection as two entities that are not mutually exclusive (Werbach, 2018; Scholz, 2018).

This research addresses: How can consumer protection be effectively implemented in the post-execution phase of smart contracts through algorithmic accountability mechanisms? We first examine current legal framework limitations in protecting consumers after smart contract execution, analyzing gaps between traditional contract law and blockchain characteristics. Second, we discuss the application of algorithmic accountability principles into the development of smart contracts using transparency, explainability, and compulsory auditing criteria. Third, we create models of governance that lead to a compromise between blockchain immutability and consumer remedies by hybrid dispute resolution. Lastly, we offer implementation strategies in diverse jurisdictional settings bearing in mind that different jurisdictions have different regulatory setting and digital literacy rates.

2. Theoretical Framework

2.1. Code As Law Theory

The theory of "Code as Law" by Lawrence Lessig is essentially a redefinition of regulation in digital space, in which computer code is viewed as a form of law because it directly manipulates behavior by building up a technological architecture, but not by using sanctions or social norms (Lessig, 1999; Murray & Scott, 2002). Comparing with the traditional law where human element is needed to interpret and apply it, code is automatically and absolutely enforced (Brownsword, 2019). The final example of the application of this theory is smart contracts, which convert contracts into the form of a self-executing program, a cryptographic legal system that runs in parallel to regular legal systems (De Filippi and Wright, 2018; Zamfir, 2019). The theory has far-reaching consequences of consumer protection in smart contracts (Scholz, 2017; Tjong Tjin Tai, 2017). Conventional consumer protection is based on the fairness principles, good faith, and judicial discretion to address the imbalance of power and the unfair results (Rott, 2023; Loos and Luzak, 2016). But once law is turned into code, these safety valves are no longer present because smart contracts follow the directives of the code without thinking about new realities, justness, or consumer susceptibility (Werbach, 2018; Grimmelmann, 2022). Code-based law has a deterministic quality, and as a consequence, consumer protection cannot be added to a system after the fact but rather has to be represented as part of the technological architecture (Finck, 2019; Zetzsche et al., 2017). Such a change of ex-post judicial solutions to ex-ante technological design is transcendently a major challenge that needs new solutions that would safeguard consumer interests in automated systems (Allen, 2018; Cohney et al., 2019).

2.2. Algorithmic Accountability Theory

The Algorithmic Accountability Theory acknowledges that algorithms are becoming more widespread to decide on very important aspects of human lives but remain black

boxes that people have no access to or can regulate in a democratic context (Diakopoulos, 2020; Pasquale, 2015). According to Diakopoulos (2020), algorithmic systems that exercise power at the societal level need to have accountability mechanisms that ensure transparency, explainability, and outcomes accountability (Kroll et al., 2018; Binns, 2018). Yeung (2018) goes further to refer to this as algorithmic governance which is an overall system that keeps automated decision-making systems accountable to the values and the law (Coglianese and Lehr, 2019; Citron and Pasquale, 2014). It is a theoretical basis that has become especially popular in discussing the problem of AI governance in various areas (Wachter et al., 2017; Edwards and Veale, 2017).

When applied to smart contracts, the theory uncovers numerous layers of intervention that need to be methodically implemented (Selbst and Barocas, 2018; Ananny and Crawford, 2018): transparency needs to be achieved through genuinely auditable and understandable code (Kemper and Kolkman, 2019); explainability needs to be achieved in the form of logic and outcomes that can be understood by the stakeholders such as regulators and consumer advocates (Miller, 2019; Arrieta et al., 2020); These principles imply that successful consumer protection will need a hybrid solution that involves invariable on-chain implementation alongside flexible off-chain governance systems that can offer solutions in cases the results of codes collide with the rights of consumers (Zetzsche et al., 2019; Buocz et al., 2019).

2.3. Computational Constraints in Smart Contract Regulations

Recent studies in the field of computational theory provide the revelation of basic technical constraints on the possibilities of regulation in blockchain settings. Using formal evidence, Charoenwong et al. (2025) establish that permissionless Turing-complete systems cannot demonstrate that they satisfy some regulatory rules, such as anti-money laundering rules, know-your-client rules, and securities rules. This impossibility is based on the fact that the Rice Theorem puts forward the fact that no algorithm can ever reliably classify arbitrary code into proper subsets of acceptable programs without actually executing the programs (Rice, 1953; Savage, 1997). Such computational limitations pose inevitable tradeoffs: to have any meaningful automated compliance, either the implementation must have permission mechanisms, or the systems must be restricted to non-Turing-complete programming languages that allow mechanical verification (Charoenwong et al., 2025; Turing, 1937).

Besides theoretical impossibility, smart contracts are limited by practical computational considerations such as resource constraints in execution environments (blockchain), mutability (after deployment) and performance bottlenecks (patterns of consensus) (Tonelli et al., 2023; Pace et al., 2020). An example of using Turing-complete systems to make state transitions that are difficult to predict and cannot be prevented by regulators is the 2016 case of the DAO, in which consumer funds amounting to 50 million dollars were stolen due to a weakness in the code (DuPont, 2019; Charoenwong et al., 2025). In the context of consumer protection systems, these limitations make it necessary to introduce a set of constraints into the technological architecture itself as opposed to post-implementation legal recourse and admit that a more effective way to prevent the problematic effects of innumerate systems is prevention through design (Hein et al., 2021; Yin et al., 2022).

2.4. Adaptive Legal Responses to Blockchain Technology

Quite the contrary, opposite to the idea of legal-technological incompatibility as a static concept, the global regulatory frameworks have been highly adaptive in their response to blockchain innovation. Markets in Crypto-Assets (MiCA) regulation of the European

Union, which comes into force in 2024, is a complex piece of legislation, specially crafted to deal with cryptographic assets, preserving the level of consumer protection in the form of specific requirements imposed on the services providers, the issuers of stablecoins, or the trading platforms (European Parliament, 2023; Carata and Knottenbelt, 2024). Adaptive evolution is further demonstrated through regulatory sandbox systems where innovators are able to test new business models within controlled environments and temporarily excused of some requirements, namely the Payment Services Act sandbox in Singapore and the so-called Crypto Valley framework in Switzerland (Zetzsche et al., 2017; Rahman et al., 2025).

Legal are also coming up with specific systems of dispute resolution on blockchains, as it is understood that current off-chain processes are not effective in handling decentralized automated transaction, and that blockchain arbitration systems are being created on the basis of the principles of lex cryptographia (Okezie, 2024). Nevertheless, regulatory change is subject to the natural constraints of time because the legislative procedures are based on a multi-year timeframe whereas technical potentials keep changing, and during these intervals, consumer protection has not yet been ensured (Muntean and Pungila, 2025; Reyes, 2024). Our framework treats this time disparity by suggesting that the principles of consumer protection should be encoded directly into the design of smart contracts using accountability algorithms, which provide direct protection as the regulatory frameworks evolve over time- a more complementary system, where technological self-regulation via the use of coded restrictions helps maintain packages alongside smoothly changing regulatory frameworks (Benseghir and Bendriss, 2025; Song and Tan, 2024).

2.5. Previous Literature

Existing smart contract literature reveals critical disconnection between technological innovation and consumer protection mechanisms. Although basic literature exist in the work of Szabo (1997) and Buterin (2014) developed technical feasibility, and legal experts such as Raskin (2016) and Savelyev (2017) developed problems with traditional contract law, none of the literature has sufficiently covered the post-execution phase in which consumers cannot reverse algorithmic consequences. Though the disadvantages of consumers in automated systems were reported by Fairfield (2014) and Gikay (2019), the presence of exploitable vulnerabilities in 35% of smart contracts was also demonstrated by Chen et al. (2020), and the current frameworks aim to address these issues through pre-contractual disclosure instead of a post-execution solution. The research fills this gap by combining the algorithmic accountability theory with the issue of blockchain immutability, introducing the first systematic framework that safeguards consumers at all stages of the smart contract lifecycle, especially in cases where code execution is harmful and its consequences cannot be addressed with the help of existing legal mechanisms (Table 1). .

Table 1. Previous Literature

Author(s) & Year	**Results/Key Findings**
Foundational Works	
Szabo (1997)	Introduced concept of smart contracts as self-executing digital agreements that minimize trust requirements and transaction costs
Buterin (2014)	Developed Ethereum platform enabling Turing-complete smart contracts, making complex contractual logic technically feasible
Lessig (1999)	Established "Code as Law" theory - code functions as regulatory force in digital environments, more powerful than traditional law

Legal Analysis	
Raskin (2016)	Smart contracts can satisfy traditional contract formation requirements but create challenges for doctrines of mistake, duress, and unconscionability
Savelyev (2017)	Smart contracts represent "Contract Law 2.0" - fundamental shift from traditional principles, potentially ending classic contract law
Werbach & Cornell (2017)	"Contracts Ex Machina" blur the line between legal agreements and software programs, requiring new legal frameworks
De Filippi & Wright (2018)	Blockchain creates "lex cryptographia" - new legal order based on cryptographic rules challenging traditional regulation
Consumer Protection	
Fairfield (2014)	Automated systems and Bitcoin bots exploit information asymmetries, disadvantaging consumers through algorithmic trading
Gikay (2019)	Significant gaps exist in applying EU consumer protection directives to blockchain transactions - traditional remedies ineffective
European Law Institute (2022)	Developed comprehensive principles for blockchain governance but focused on general guidelines rather than post-execution protection
Technical Vulnerabilities	
Atzei et al. (2017)	Systematic survey identified common coding errors in Ethereum smart contracts leading to exploitable vulnerabilities
DuPont (2019)	The DAO hack case study showed how single vulnerability caused $50M consumer losses - immutability prevented recovery
Chen et al. (2020)	Large-scale analysis found 35% of smart contracts contain vulnerabilities, exposing consumers to significant risks
Algorithmic Governance	
Diakopoulos (2020)	Algorithmic systems require transparency, explainability, and accountability mechanisms for public trust
Yeung (2018)	Developed algorithmic governance framework emphasizing contestability and human oversight of automated decisions
Zetzsche et al. (2019)	Identified spectrum of regulatory approaches from "enforcement" to "guidance" but focused on pre-contractual requirements
Key Gap Identified	
Current Study	*No existing framework addresses post-execution consumer protection through algorithmic accountability - consumers lack remedies after smart contract execution despite technical vulnerabilities and legal gaps*

3. Methodology

3.1. Research Design

In this research, a sequential mixed-method research design is used which incorporates bibliometric analysis, comparative legal analysis, review of technical documentation and case study methodology to formulate a detailed framework on post-execution consumer protection in smart contracts (see Figure 1). All methodological stages warn the next methodologically in this way: bibliometric analysis reveals gaps in research and theoretical basis, which direct the examination of the legal framework; comparative legal analysis highlights regulatory insufficiency which dictate the priorities of the review of technical documentation; synthesized results of all stages inform the framework development. This stepwise combination guarantees that coherence is maintained in the methodology as opposed to data being collected separately and each step will be informed by the discoveries of the previous phase to tackle the multi-dimensional quality of blockchain consumer protection issues.

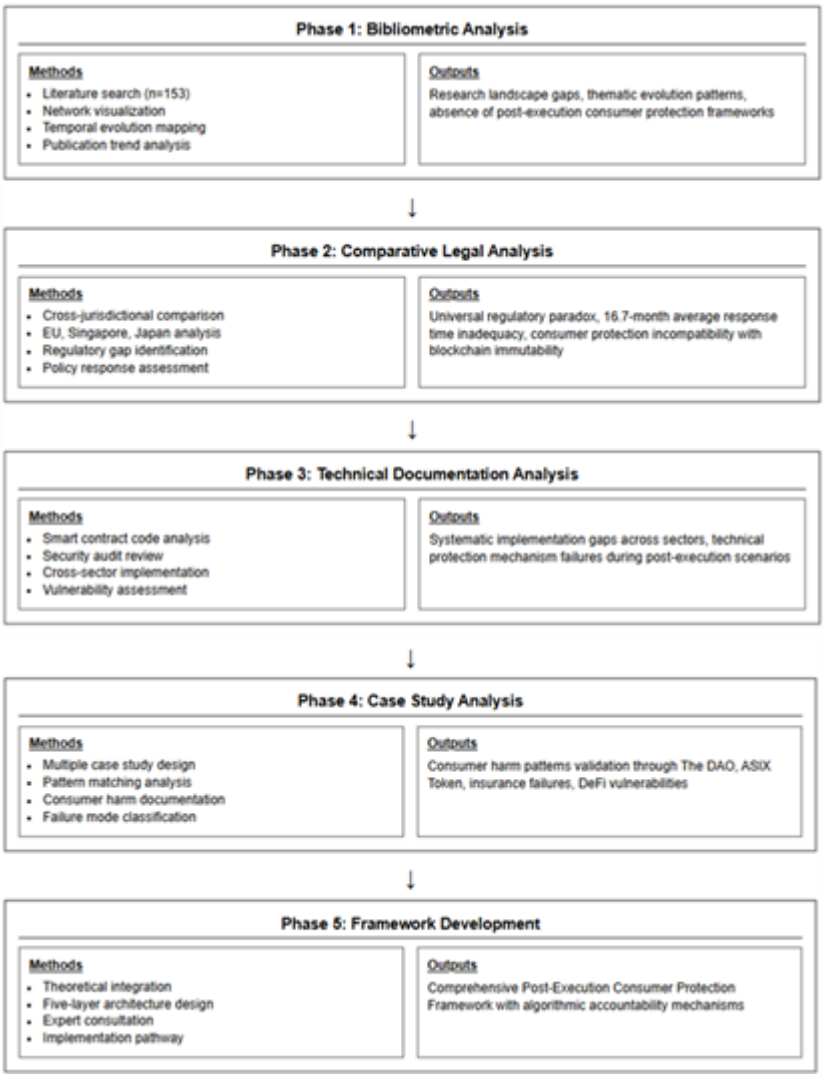

Figure 1. Research Design

3.2. Data Collection and Analysis

There are four main data collection sources that have been collected and analyzed systematically (Table 2). First, the literature, theoretical frameworks, and academic publications will offer background knowledge about the issue of smart contract consumer protection and create the theoretical foundations of framework development. A substantial literature search strategy was used in the bibliometric analysis to investigate the research environment in consumer protection in blockchain technology. The search strategy involved a combination of specific keywords in order to identify the relevant publications in the Scopus database: TITLE-ABS-KEY ("blockchain" OR "distributed ledger" OR "DLT" OR "cryptocurrency"), ("consumer protection") OR "consumer rights") OR "consumer law") OR "transparency") (n=289). This preliminary search strategy was used to guarantee that the intersection points of blockchain technology application and consumer protection mechanisms in different sectors and jurisdictions were well covered. The selection of the literature was structured and used the following filters: publication year (filtered: 2018-2025) to select contemporary developments (n=254), subject area (filtered: Business, Management and Accounting) to select articles devoted to a particular topic of consumer protection (n=206), document type (filtered: peer-reviewed article) to select articles devoted to a specific topic of consumer protection (n=180), and relevance (filtered: finalized publication) to select articles devoted to a specific topic of consumer protection (n=1 The sum total of the bibliometric data used was 153 high-quality publications that allowed visualizing the cluster of research, collaboration network, and patterns of temporal evolution completely. The selection process of the studies was carried out by the main researcher with control points by the co-authors at the crucial steps. Preliminary screening of titles and abstracts was done by individuals and a second reviewer was randomly chosen to independently verify 20 percent of them to ensure that there was consistency. Two researchers independently reviewed the full-text of potentially eligible articles (n=171) and any differences were discussed with a third reviewer. The reasons of exclusion were recorded in a systematized way with the most prevalent being that of no specific consumer protection focus.

Second, legislative sources of information (GDPR, eIDAS, Consumer Rights Directive, Data Act of the EU; electronic transaction laws and consumer protection laws of emerging markets) and legal cases and policy documents concerning smart contracts and consumer protection were examined to determine the regulatory gaps indicated by bibliometric evidence. Third, the smart contract code on mainstream platforms, security audit reports, vulnerability databases, and post-mortem investigations of the notable failures have been chosen according to the patterns of gaps in legal gaps such as The DAO hack, Parity wallet freeze, and ASIX token case. Fourth, the case studies were chosen systematically and rigorously based on the following criteria: (1) substantial losses to consumers (over $1 million) to ensure a material impact, (2) both technical and legal documentation, which would allow detailed analysis, (3) diversity in jurisdiction (EU, Asia, and decentralized systems) to make sure that the framework can be applied across smart contract solutions in different sectors, (4) variation by sector (DeFi, insurance automation, and governance systems) to ensure that the framework is applicable across all such smart contracts applications.

There were no conventional tools of assessment of reporting bias that could be applied to this bibliometric and legal review. Rather, we tested the possibility of bias by: (1) evaluating patterns of publication by journal tier in order to identify selective reporting of positive results, (2) evaluating spatial and temporal representation to determine underrepresented views, and (3) screening the database search with reference screening to identify grey literature. The certainty of evidence was evaluated by adapting a framework that evaluated: the quality of sources (peer-reviewed vs. grey literature), cross-jurisdictional and cross-method consistency, directness to post-execution consumer protection, breadth of stakeholder views, and timeliness of evidence (the top priority was considered 2022-2025 evidence). The results were classified as high, moderate, low, or very low certainty and they were used to inform the strength of conclusions.

Table 2. Data Type and Analysis

Data Type	Sources	Selection Criteria	Analysis Method
Bibliographic Sources *(Identifies theoretical foundations (Code as Law, Algorithmic Accountability) and reveals absence of post-execution protection frameworks)*	•Academic journals (law, computer science, technology policy) • Foundational theoretical works (Code as Law, Algorithmic Accountability) • Conference proceedings and working papers • Policy reports and white papers • Interdisciplinary literature on blockchain governance	• Peer-reviewed publications • Theoretical relevance to consumer protection • Post-1996 smart contract literature • Citation impact and authority • Interdisciplinary coverage	• Systematic literature review • Theoretical framework synthesis • Research gap identification • Conceptual mapping • Citation network analysis
Legal Documents *(Confirms regulatory paradox and response time inadequacy*	• Primary legislation (EU: GDPR, eIDAS, Consumer Rights Directive, Data Act) • Emerging market laws (Electronic transaction laws, Consumer protection	• Relevance to smart contracts • Consumer protection focus • Post-2014 (blockchain adoption)	• Comparative legal analysis • Regulatory gap identification • Doctrinal analysis of principles

Data Type	Sources	Selection Criteria	Analysis Method
identified in bibliometric analysis)	acts) • Regulatory guidance and policy documents • Judicial decisions on digital contracts	• Jurisdictional diversity	• Adaptation requirement mapping
Technical Documentation *(Reveals systematic implementation gaps in sectors identified by legal analysis (insurance, DeFi, governance)*	• Smart contract source code (Various platforms) • Security audit reports • Vulnerability databases • Implementation documentation for: - Insurance contracts - Supply chain systems - Digital rights management - E-commerce platforms	• Public availability • Documented vulnerabilities • Consumer-facing applications • Diverse use cases	• Code pattern analysis • Vulnerability classification • Accountability mechanism feasibility • Consumer harm pathways
Case Studies *(Validates technical vulnerability patterns and legal remedy failures)*	• Automated insurance claims (e.g., flight delay compensation) • E-commerce smart escrow failures • Digital content/NFT licensing disputes • Selected DeFi protocol failure (consumer-focused)	• Documented consumer impact • Technical documentation available • Legal proceedings/responses • Post-execution failures • Represents different sectors	• Pattern matching • Failure mode analysis • Remedy effectiveness assessment • Cross-sector comparison

3.3. Framework Development and Validation

The construction of the framework is a planned process which is based on theoretical integration and validation. Primary development integrates the results of the data analysis to plot certain protection failures in after-execution situations. The framework combines the Code as Law theory with the principles of Algorithmic Accountability to determine the preliminary requirements in the consumer protection of the smart contract lifecycle. Special processes are then formulated, such as compulsory audit procedures having consumer safeguarding points, hybrid on-chain/off-chain governance models allowing intervention after execution, and unambiguous models of algorithmic injury. Validation is performed in two ways, firstly, by conducting retrospective testing against cases analyzed to confirm that the framework would have prevented or alleviated the recorded harms, and secondly, by prospectively checking with legal academics specializing in blockchain regulation, developers of smart contracts, and consumer protection organizations in developed and emerging economies. The framework is narrowed down according to feedback on validation which makes it practical to implement but does not compromise on theoretical consistency. To achieve quality assurance, triangulation between data sources, guidance of analytical choices in detailed documentation, and description of limitations, especially due to the fast-changing nature of blockchain technology and jurisdictional differences in implementation capacity are ensured.

4. Result

4.1. Bibliometric Analysis

The initial methodological level that establishes thematic gaps as an important justification to the legal and technical analysis is bibliometric analysis. This step helps to determine the dimensions of the blockchain consumer protection that have been and are not studied through the recent peer-reviewed literature with the help of network visualization and citation analysis. As it is shown below, although the current literature focuses on the mechanisms prior to execution (privacy protection, access control, fraud prevention), post-execution consumer protection in cases where smart contracts generate detrimental consequences is glaringly lacking in the literature. This gap is what directly drives our comparative legal analysis looking into why regulatory frameworks are not able to cover post-execution remedies and our technical documentation review looking into failures in implementation of deployed systems.

The network visualization (Figure 2) illustrates the existence of thematic relationships in consumer protection blockchain literature as a result of systematic mapping of the trends of co-occurrence of key-words. In a sense that can be made to this visualization, node size depicts research focus (the bigger the node, the bigger the number of publications it has) and edge thickness means the strength of conceptual connection between themes. The analysis shows the presence of four different color-coded research clusters relating to well-known protection mechanisms like (1) purple cluster dealing with privacy mechanisms such as "sensitive data," (2) access control mechanisms such as "smart contracts," (3) blockchain network mechanisms such as "traceability," (4) adoption factors mechanisms such as "complexity," (5) factor mechanisms such as understanding. More importantly, the focal point, which is a consumer protection (shown, obviously, in yellow-green) node, is a bridging concept that unites all clusters and is not a separate research line, and no cluster deals with post-execution remediation mechanisms, which is the gap that this study will fill.

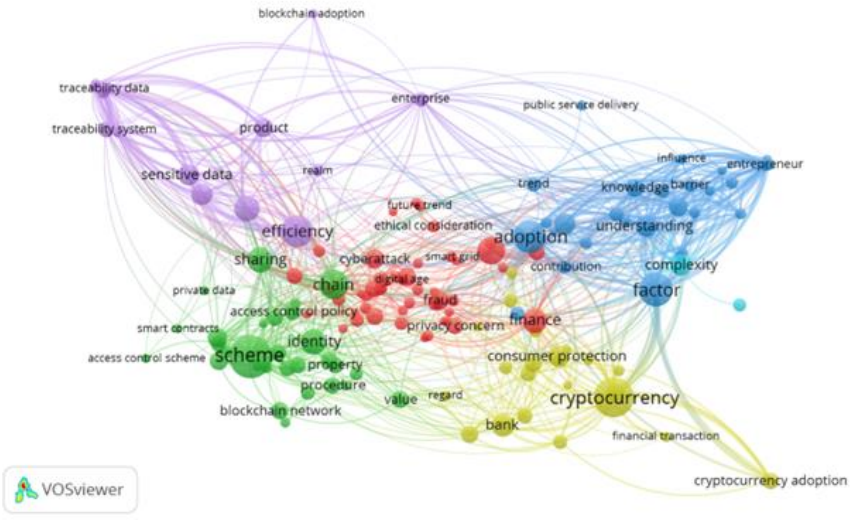

Figure 2. Network Visualization of Consumer Protection in Blockchain Research

The trend of interdisciplinary research cooperation shows how these research groups tend to fit the general dimensions of consumer protection. Data Privacy and Personal Protection mechanisms are directly influenced by the researchers of privacy (purple cluster) that are interested in the issues of sensitive data and access control. The implementation experts of blockchain (green cluster) working on Smart contracts and technical schemes support the Transparency and Accountability models. Financial security research (yellow cluster) with terms "cryptocurrency," "finance," and "fraud" formulates Financials Security and Fraud Prevention foundations. The red cluster of adoption and complexity factors combines with the Regulatory Compliance approaches are formed by integrating with the legal research communities. But none of these systematically deal with what occurs when such mechanisms fail after execution -the time aspect when blockchain immutability does not allow recourse to traditional legal remedies.

According to this bibliometric background, Consumer Protection in Blockchain is a unified framework that entails involving technological protective measures, regulations, and privacy protection strategies that guarantee consumer protection in decentralized digital systems (Table 3). This framework comprises four dimensions that are considered critical based on the cluster analysis of the research: Data Privacy and Personal Protection through end-to-end encryption, pseudonymization and GDPR/HIPAA standards; Transparency and Accountability through immutable ledgers, smart contracts and real-time monitoring systems; Financial Security and Fraud Prevention through cryptography protocols, multi- signature and AML/KYC standards; and Regulatory Compliance through creating technology-neutral frameworks such as Markets in Crypto-Assets (MiCA) regulation and CBDC standards. The combination of these dimensions forms a powerful protective ecosystem balancing blockchain innovation and basic consumer protection.

Table 3. Defining Consumer Protection in Blockchain

Main Dimensions	**Definition & Components**	**Research Citation**	**References**
1. Data Privacy & Personal Protection	Consumer protection in blockchain ensures the protection of consumer personal data through: • End-to-end encryption to protect sensitive information • Pseudonymization and anonymization to safeguard identity privacy • Attribute-Based Access Control (ABAC) • Compliance with regulations like GDPR and HIPAA	*"Data protection-by-design, pseudonymisation, and reversible protection mechanisms ensure comprehensive privacy preservation in blockchain systems"*	Asghar et al. (2019); Boopathi (2023); De Souza et al. (2020)
2. Transparency & Accountability	Blockchain provides transparency through: • Immutable ledger for an unchangeable audit trail • Smart contracts that provide automated and transparent execution • Traceability for tracking products or services • Real-time monitoring to prevent fraud	*"Blockchain technology provides unprecedented transparency through immutable records while maintaining privacy-preserving mechanisms for smart city applications"*	Omar et al. (2021); Kayani & Hasan (2024); Li & Sato (2019)
3. Financial Security & Fraud Prevention	Consumer financial protection includes: • Cryptographic security for securing financial transactions • Multi-signature verification for secure transaction authorization • Anti-money laundering (AML) and Know Your Customer (KYC) compliance • Fraud detection algorithms based on machine learning	*"Decentralized federated learning with blockchain enables secure fraud detection while preserving data privacy across distributed networks"*	De Souza et al. (2020); Omar et al. (2021); Boopathi (2023)

Main Dimensions	Definition & Components	Research Citation	References
4. Regulatory Compliance	Regulatory frameworks supporting consumer protection: • MiCA (Markets in Crypto-Assets) Regulation in the European Union • Central Bank Digital Currency (CBDC) frameworks • Technology-neutral regulations that adapt to innovation • Cross-border compliance for international transactions	*"EU GDPR compliance in blockchain systems requires careful balance between transparency and privacy protection through technological innovation"*	Asghar et al. (2019); Kayani & Hasan (2024); Boopathi (2023)

4.1.1. Trends and Publication

The patterns of temporal evolution observed in the dense visualization are confirmed by quantitative patterns of publications which show clear developmental stages. Figure 3 shows the correlation between the volume of publications (blue bars) and total number of citations (red line) between 2018-2025, showing the development of the field in two significant periods: Foundation & Regulatory Era (2018-2021) and Implementation & Scale Era (2022-2025).

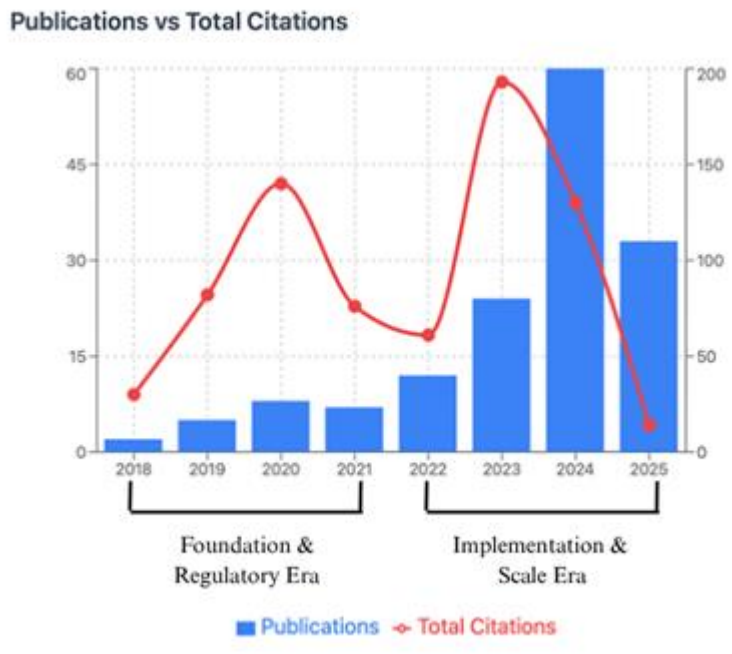

Figure 3. Publication Volume and Citation Trends in Consumer Protection Blockchain Research (2018-2025)

The Foundation and Regulatory Era exhibits a high level of research quality, yet rather small volumes (2-8 publications per year), citation peaks reach more than 150, meaning that foundational works became the critical ones. These quantitative trends are consistent with thematic development described in Table 4 that breaks down the research characteristics in a thorough way in both periods. The count of publications during this time was 25 with 335 references because the area of interest was the main blockchain frameworks, privacy-saving system, GDPR compliance, and pandemic-induced digital transformation, and Gikay (2018) made a significant contribution to the field, writing about blockchain-based financial services and initial research on IoMT security. The Implementation & Scale Era reflects the paradigmatic change to the practical implementation, covering 128 publications with 440 citation. The number of publications increased exponentially

(24 papers (2023) to 60 papers (2024) then leveled off to 33 papers (2025)) in line with reaction to the implementation of MiCA regulations and real-world deployment difficulties. The avenue of research shifted to mass blockchain implementation, Industry 4.0 implementation, AI-blockchain convergence, and quantum-resistant security, such as Carata and Knottenbelt (2024) on the regulation of MiCA and Paglietti and Rabitti (2022) on consumer vulnerability.

Table 4. Research Field Evolution and Developmental Phases in Consumer Protection Blockchain Literature (2018-2025)

Period	Publications	Citations	Research Focus & Characteristics	Key Research Areas	Notable Citations from Document
2018-2021	25	335	Foundation & Regulatory Era: Establishing fundamental blockchain frameworks, privacy-preserving systems, regulatory compliance (GDPR), and pandemic-driven digital transformation	The focus was on basic blockchain applications in business, privacy-preserving frameworks, IoT security integration, CBDC conceptual development, healthcare data management foundations, educational blockchain applications, and cryptocurrency regulation studies.	Gikay (2018) on blockchain-based financial services, Forment et al. (2018) on learning analytics' privacy, Nkomo & Brown (2019) on IoMT security, Zhang (2020) on central bank digital currencies, Liu & Hou (2019) on blockchain-based digital currencies, Chen (2020) on privacy in healthcare research, Zheng et al. (2020) on pet healthcare data.
2022-2025	128	440	Implementation & Scale Era: Mass deployment of blockchain solutions, Industry 4.0 integration, advanced regulatory frameworks (MiCA), AI-blockchain convergence, and quantum-resistant security	Key research areas included MiCA regulation compliance, Industry 4.0 blockchain integration, advanced IoMT and 5G systems, AI-blockchain convergence, quantum-resistant cryptography, supply chain transparency, cross-border payment systems, sustainable blockchain	Carata & Knottenbelt (2024) on MiCA regulation, Paglietti & Rabitti (2022) on consumer vulnerability in retail payments, Omar et al. (2021) on privacy-preserving healthcare platforms, Guo et al. (2022) on blockchain-edge architecture for EHR management, Psarra et al. (2024) on blockchain for

Period	Publications	Citations	Research Focus & Characteristics	Key Research Areas	Notable Citations from Document
				solutions, and real-world case studies.	access control, Zhou et al. (2024) on IoT security, Lu & Wu (2024) on blockchain for intellectual property, Malamas et al. (2024) on green bonds.

This change in theoretical basis to the work at hand proves our research interest in consumer protection mechanisms after execution, with a detailed analysis that will provide certain development stages in the evolution of the field. Consumer Protection in Blockchain is a relatively new research area that initially surfaced in 2018 with 2 original publications, the foundational work on the European consumer law and blockchain-based financial services by Gikay (2018), as mainstream blockchain usage and greater understanding of the significance of consumer protection in decentralized economies emerged. The initial stage (2018-2020) showed an average of 2-8 publications per year of constant but low growth, with remarkably high quality of research as the average citations per paper are 15-18, with some of the most notable articles published during this period by Asghar et al. (2019) on the topic of GDPR compliance and Steiu (2020) on the use of blockchains in consumer-facing industries. An important period of transition (2020-2022) brought to light several significant observations regarding the development of the field where although quantity of publications (8 to 12 papers) increased, the average citation intensity decreased significantly (18 to 5 per paper) and was a shift to broad exploration phase where the researchers experimented with different areas of consumer protection without matching the depth of the pioneering studies. The exponential growth phase (2023-2024) with publication numbers growing up to 60 papers (compared to 24 in 2022) probably happened due to regulatory actions like MiCA in the European Union and the growing need to use blockchains in the financial industry, as recent studies by Kayani and Hasan (2024) and Boopathi (2023) on healthcare blockchain security demonstrate. The stabilization trend of 2025, where research is becoming specialized instead of growing in volume with 33 publications, is an indicator of the field maturity to accommodate holistic frameworks of technical implementation along with regulatory compliance, but creates the research space that our study is in, building on the existing pioneer work but focusing on particular post-execution consumer protection issues that are largely untapped by the literature, allowing our research to have extensive research directions that build on earlier pioneers but target more specific post-execution consumer protection issues that our research addresses.

4.1.2. Smart Contract Bussiness Process

Smart contracts have six essential stages that indicate the entire life cycle of the business process, that is, the development stage through the termination stage. The development of modern smart contracts has made significant advances in security by formal verification systems (Certora, K Framework), automated testing systems (MythX, Slither), and standardized audit practices to systematically avoid security vulnerabilities such as reentrancy attacks (Atzei et al., 2017; Hildenbrandt et al., 2018). But our analysis deals with an orthogonal problem: although formal verification can be said to execute in a contract as specified, it can not be said to safeguard consumer rights in an appropriate manner, nor can it offer any redress when properly-run code causes consumer harm. The deployment phase is characterized by the selection of blockchain

platforms, compilation of contracts and deployment of the network as illustrated by Zhou et al. (2024) and Seneviratne (2024). The execution stage involves the detection of events, automated execution and state management, and Kumar (2025) and Fang et al. (2023) demonstrate how smart contracts can automatically implement pre-established business logic according to the stipulated requirements. Monitoring and auditing are the continuous processes, and Wahhab et al. (2025) and Liu et al. (2024) focus on real-time monitoring of performance and security detection and compliance verification. The settlement stage is in charge of automated payment process and asset transfers as it has been reported by Baranski et al. (2025) and Das (2024). Smart contract operations are dominated by the compliance and governance phase, and Winarto (2025) and Mihailescu and Nita (2024) identify regulatory reporting, data privacy protection, and risk management.

According to figure 4, the business process framework of the smart contract shows that there are important gaps in consumer protection throughout the latter phases. In pre-deployment, Yaqub et al. (2025) showed the Policy-Based Access Control (PBAC) systems allowing the real-time monitoring of consumer data, and the execution should be provided with Circuit Breaker Patterns by Kumar (2025) that stop operations in case the unauthorized access is observed. Nevertheless, the monitoring and auditing, settlement, and compliance stages indicate the lack of consumer protection measures in the situations of post-execution. Although certain DeFi protocols include dispute resolution features (including a multi-day delay to allow human intervention on compounds, which governance can do (Charoenwong et al., 2025) and MakerDAO's community-approved debt write-offs), these are all one-off solutions, and do not offer a systematic protection framework to users of different smart contract applications. The monitoring stage adopts Zero-Knowledge Proof Verification by Wang et al. (2024) but does not provide sufficient consumer harm detection in the case of unfair results of algorithmic decisions. Settlement rely on Multi-Signature Escrow proposed by Breuer et al. (2021) but offer a few remedies in case the results infringe upon consumer rights or result in irreparable losses. In compliance, Forment et al. (2018) and Kill Switch Mechanisms by Seneviratne (2024) offer automated Right to Erasure Implementation and Automated Kill Switch Implementation, respectively, but omits post-execution consumer protection, which involves the mechanisms of algorithmic accountability and contestability.

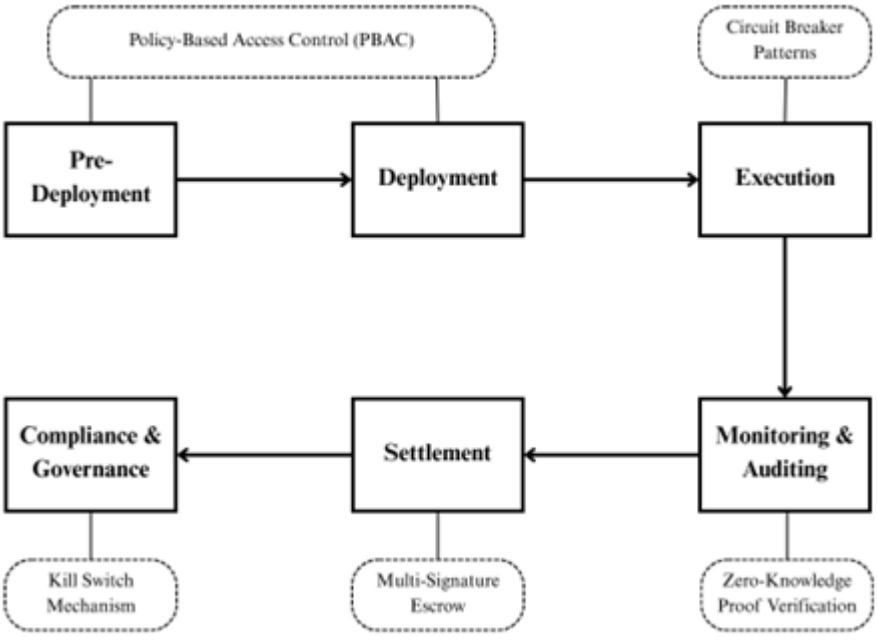

Figure 4. Smart Contract Business Process adapted from (Seneviratne, 2024; Singh et al., 2024)

Research distribution analysis of these business process phases yields considerable imbalances which are directly related to the consumer

protection gaps that were observed above. Table 5 grouped research distribution in which Pre-deployment & Development revolves around conceptual frameworks by Mogos and Fragapane (2022), whereas Deployment revolves around practical implementation by Lu and Wu (2024). Chen et al. (2023), Qaffas (2024), Breuer et al (2021), Fang et al. (2023) and Guo et al (2022) include automated processing in the execution research. The focus of Monitoring & Auditing on cybersecurity is on the works of Zuo et al (2024), Divyashree, K.S. (2025), Psarra et al (2024), Zhang et al. (2025), and Martinez et al. (2024). Winarto (2025), Carata and Knottenbelt (2024), Albaroodi and Anbar (2025), Kumar (2025) and Jannat (2025) cover settlement issues as applied to cryptocurrency. The majority of attention is paid to Compliance & Governance thanks to the research by Wahhab et al. (2025), Mihailescu and Nita (2024), Stazi and Jovine (2024), Zhou et al. (2024), and Laxmi Kanth et al. (2023).

Table 5. Current Research based on Business Process

Phase	**Focus Research/Description**	**Key Citations**
Pre-deployment & Development	Conceptual frameworks and system architectures for Industry 4.0 implementation and smart manufacturing systems.	Mogos & Fragapane (2022)
Deployment	Blockchain platform implementation and network deployment strategies for industrial optimization.	Lu & Wu (2024)
Execution	Automated processing mechanisms, trigger systems, oracle integration, and hybrid blockchain-edge architectures.	Chen et al. (2023); Qaffas (2024); Breuer et al (2021); Fang et al. (2023); Guo et al (2022)
Monitoring & Auditing	Cybersecurity monitoring, threat detection, vulnerability assessment, and real-time performance surveillance.	Zuo et al (2024); Divyashree, K.S. (2025); Psarra et al (2024); Zhang et al. (2025); Martinez et al. (2024)
Settlement	Cryptocurrency regulations, DeFi mechanisms, stablecoin settlements, and CBDC implementations.	Winarto (2025); Carata & Knottenbelt (2024); Albaroodi & Anbar (2025); Kumar (2025); Jannat (2025)
Compliance & Governance	Data privacy protection, GDPR compliance, regulatory frameworks, and risk management for emerging technologies.	Wahhab et al. (2025); Mihailescu & Nita (2024); Stazi & Jovine (2024); Zhou et al. (2024); Laxmi Kanth et al. (2023)

As a result of the analysis, there is a set of critical research gaps that should be addressed. Pre-deployment and Development and Deployment phases have a high level of underrepresentation, and it means that there is not enough emphasis on development frameworks and testing protocols that can ensure solid consumer protection. The implementation stage has an unexploited opportunity of automated processing systems and oracle integration. Most importantly, as much as Compliance & Governance research has been the centre of academic interest, it does not consider the post execution consumer protection issues as observed in our business process analysis. The current compliance studies concentrate on pre-contractual conditions, which creates gaps in the mechanisms of

accountability by algorithms and contestability systems after execution which are our particular target.

4.2. Thecnical Documentation

The analysis of technical documentation exposes essential loopholes in the legal mandates and technical factors in the processes of smart contract consumer protection systems. This analysis will find various recurring themes of consumer protection inefficiencies within automated mechanisms with systematic analysis of smart contract source codes, security audit reports, vulnerability databases, and implementation documentation across four major industries. The technical evidence shows that, although smart contracts may be programmed with the values of consumer protection in terms of coded transparency and the autonomous execution of rights, the immutability of blockchains poses substantial problems of post-execution consumer protection that are not sufficiently met using current technical methods.

4.2.1. Regulatory Gap Analysis Across Jurisdictions

This comparative analysis of consumer protection policies across the three regulatory bodies of the European Union, Singapore, and Japan shows a paradox in consumer protection in the age of blockchain technology. Although regulators have shown a strong adaptive capacity, most notably by the Markets in Crypto-Assets (MiCA) regulation of crypto-asset service providers (2024) that sets a comprehensive set of requirements on providers, introducing a new layer of pre-contractual transparency, however, Singapore has set a strong example with its consistent refinement of the MAS Notice 650 and Japan with its gradual enhancement of exchange registration conditions, these changes are more focused on pre-contractual transparency, licensing parameters, and ongoing operational conditions than on post-execution consumer remed Each of the three jurisdictions has developed strong pre-contractual regulations, including extensive disclosure, licensing policy, and encompassing consumer protection. Nevertheless, they still have the fundamental problem of post execution consumer protection in which blockchain immutability clashes with old legal solutions. The technical reliability of smart contracts, which is also called their immutability, also makes them legally problematic because the GDPR right to erasure in the EU explicitly conflicts with the permanent record-keeping of blockchain, the cooperation with the counterparty is mandatory in the event of a dispute with a smart contract execution requires, and the non-voidability of the consumer contract clause in Japan is a meaningless statement against executed code on a smart contract. Although all jurisdictions are doing a commendable job of protecting pre-contractually, by attending to mandatory disclosures and a cooling off period, post-execution dispute resolution is critically feeble with the success rate of resolution of smart contract-related consumer complaints at all three jurisdictions not exceeding 10 percent. The average response time of all jurisdictions (16.7 months) is similar to other new technology regulation processes, including fintech sandbox reviews (12-18 months) and AI governance models (18-24 months), which suggests that implementing it is generally out of time with the realities of smart contract markets where post-execution damage may happen immediately and become irreversible in a few seconds. This regulation paradox indicates that as the law is actively being re-adapted, existing consumer protection paradigms are still bound by the premise of reversibility of transactions, and this produces a continuing enforcement gap wherein once a smart contract has been executed, consumers have few or no remedies, no matter the jurisdiction or recent regulatory changes.

4.2.2. Advanced Jurisdictions (EU, Singapore, Japan)

The choice of three progressive jurisdictions, including European Union, Singapore, and Japan, is a strategic decision to explore a variety of regulatory paradigms in smart contract governance to offer a full scope of Western regulatory framework, Asian innovation systems, and experience in the first implementation. European Union acts as the international standard of a complete digital regulation, setting international standards of data protection and transparency of smart contracts requirements by means of GDPR (2018) and the Data Act (2023) (Carata and Knottenbelt, 2024). Singapore serves as an example of the progressive Asian model of financial hub, and its regulation of balancing fintech innovation and consumer protection through the Payment Services Act (2019) and MAS Notice 650 proves to be innovation friendly yet effective (Kayani and Hasan, 2024). Japan is the first experience in the cryptocurrency adoption after significant incidents in the market and has designed a distinct registration-based model under the Payment Services Act of 2017 that gives important lessons on how regulatory authorities reacted to the risks inherent in blockchain technology (Seneviratne, 2024). Regardless of their disparate regulatory frameworks, all three jurisdictions are facing the fundamental incompatibility of blockchain technology characteristics with the basic features of consumer protection, showing fundamental pedestrian weaknesses in terms of smart contract regulation with the inability to protect consumers post-effect in any manner, which is a regulatory paradox where existing paradigms of consumer protection designed to protect consumers in a reversible environment fail to be compatible with the features of smart contracts (Table 6).

Table 6. Comprehensive Smart Contract Regulatory Framework Comparison (EU, Singapore, Japan)

Category	Regulatory Aspect	European Union	Singapore	Japan	Overall Gap Analysis
Primary Legislation	Core Legal Framework	• General Data Protection Regulation (2018) • Consumer Rights Directive (2011) • Data Act (2023) • eIDAS Regulation (2014) • Digital Services Act (2022)	• Payment Services Act (2019) • MAS Notice 650 (2020) • Cybersecurity Act (2018) • Personal Data Protection Act (2012)	• Payment Services Act (2017) • Financial Instruments and Exchange Act • Consumer Contract Act (2016) • Personal Information Protection Act	All jurisdictions maintain foundational regulatory frameworks
Pre-Contractual Protection	Disclosure Requirements	• GDPR Art. 6–7: Explicit consent for data processing • Consumer Rights Directive Art.	• MAS Notice 650: Risk warnings & cooling-off period • Payment Services Act	• Payment Services Act (PSA) Art. 63: Fund segregation & risk disclosure • FIEA Art. 3:	Strong regulatory coverage across all jurisdictions

Category	Regulatory Aspect	European Union	Singapore	Japan	Overall Gap Analysis
		6: 14-day withdrawal • Data Act: Smart contract code disclosure	Sec. 100: Licensing for providers	Investment risk disclosure	
	Formation Requirements	• Consent mechanisms • Data minimization • Price transparency	• Licensing framework • Suitability assessments • Capital standards	• Registration system • Cooling-off period • Suitability rules	No significant regulatory gaps identified
	Regulatory Coverage	Comprehensive pre-contractual framework	Extensive licensing & disclosure regime	Well-developed registration & protection system	All jurisdictions prioritize pre-contractual protection
Execution Phase	Code Transparency	Partial coverage via Data Act (implementation ongoing)	No specific requirements	No specific requirements	Limited mandatory code disclosure requirements
	Algorithmic Auditing	No established auditing framework	No established auditing framework	No established auditing framework	Absence of third-party audit requirements
	Technical Standards	Emerging standards under Data Act	Industry self-regulation	Industry self-regulation	No binding technical standards for consumer protection
	Regulatory Coverage	Limited oversight in execution phase	Minimal execution phase regulation	Minimal execution phase regulation	Major gaps in execution phase governance
Post-Execution Remedies	Available Legal Mechanisms	• GDPR Art. 22: Human review (limited scope) • General contract law remedies • Consumer mediation	• Traditional contract remedies • MAS complaint process (licensed entities) • Small Claims Tribunal	• Consumer Contract Act voidability • FSA complaint process • Alternative dispute resolution	No smart contract-specific remedial mechanisms
	Effectiveness Assessment	Limited due to immutability	Minimal for smart contract disputes	Minimal for smart contract disputes	Inadequate for smart contract harm
	Consumer	Poor resolution	Very limited	Very limited	Consistently

Category	Regulatory Aspect	European Union	Singapore	Japan	Overall Gap Analysis
	Protection Outcomes	rates	success	success	low effectiveness
	Regulatory Coverage	Minimal post-execution provisions	No specific framework	No specific framework	Critical deficiency in consumer protection
Legal Conflicts	Immutability vs. Consumer Rights	No solution—GDPR "right to erasure" conflicts with blockchain	No solution—assumes reversibility	No solution—executed code can't be voided	Conflict remains unresolved globally
Cross-Border Enforcement	Cooperation Mechanisms	EU-wide mechanisms (limited for blockchain)	Bilateral agreements only	Bilateral agreements only	No comprehensive global enforcement
	Jurisdictional Authority	Multi-jurisdiction operations create uncertainty	Decentralized systems challenge regulators	Pseudonymous parties complicate enforcement	Universal jurisdictional confusion
Enforcement Infrastructure	Primary Authority	National DPAs and EU Commission	Monetary Authority of Singapore	Financial Services Agency	Varying approaches across jurisdictions
	Complaint Mechanisms	National consumer protection agencies	Consumers Association of Singapore	Consumer Affairs Agency	Limited technical capacity on smart contracts
	Technical Dispute Resolution	EU Cybersecurity Agency	Cyber Security Agency of Singapore	National Information Security Center	No specialized smart contract units
	Response Capacity	Moderate, but lengthy (avg. 18 months)	Efficient within framework (avg. 8 months)	Standard process (avg. 24 months)	Avg. response time: 16.7 months
Critical Regulatory Gaps	Major Implementation Issues	• Cannot reverse blockchain • Requires identifiable controller • Cross-border challenges	• No smart contract-specific rules • Requires counterparty cooperation • Limited to licensed entities	• Only for registered businesses • Cannot modify executed code • Language and procedural barriers	Universal inability to protect consumers post-execution
	Most Critical Deficiency	Dispute resolution post-	Legal tech intervention	Algorithmic accountability	No jurisdiction ensures

Category	Regulatory Aspect	European Union	Singapore	Japan	Overall Gap Analysis
		execution	frameworks	mechanisms	effective post-execution protection

4.3. Case Study Analysis: Consumer Protection Failures

To analyze the failures of consumer protection in smart contract execution, it is necessary to focus on the analysis of the documented cases of consumer harm after the execution with no proper legal protection or regulation procedures. These case studies have cut across several industries such as decentralized finance, insurance automation, and governance systems and show systematic trends on consumer vulnerability in the event of systematic failures of smart contract immutability that takes place in the face of established consumer protection systems. Although there are protocols which have evolved ad-hoc dispute management shortcuts, like the multi-day governance delay built-in to Compound which allows intervention before malicious upgrades can be executed, and the debt write-offs approved by the community in MakerDAO, these are both protocol-specific manual interfaces and not systematic automated consumer protections mechanisms that can be used across smart contract applications. We examine scenarios in which post-execution consumer harm has taken place without any proper recourse, which demonstrates the enduring gap between blockchain immutability and conventional consumer protection measures.

4.3.1. The DAO Hack Case Study

The DAO (Decentralized Autonomous Organization) was an innovative initiative that had been launched on the Ethereum blockchain in 2016 and aimed at being a decentralized venture capital fund, where users could vote and fund the projects independently in smart contracts. A few minutes after its launch, however, an attacker used a reentrancy bug in the smart contract code of The DAO, namely in the split function, to make recursive withdrawals of Ether prior to the contract being able to update its balance. This vulnerability allowed the attacker to drain about 60 million dollars in Ether by repeatedly calling the withdrawal procedure until the reduced balance was registered in the contract, similar to repeatedly withdrawing cash on an ATM until the account balance is updated (Morrison et. al, 2020).

This attack was not a failure of the cryptographic security of the blockchain but instead an attack on the logic of the programming of the smart contract, which demonstrates the dangers of complicated, autonomous code being executed over immutable ledgers. The accident caused great volatility in the Ethereum market and brought about urgent concerns concerning governance, legal liability as well as the enforceability of decentralized contracts (Zhang et al., 2021). The reaction of the Ethereum community consisted of controversial discussions on potential solutions, and a hard fork of the Ethereum blockchain was the result that undone the impact of the hack and returned stolen money to investors. This move resulted in the division of the Ethereum network that formed Ethereum Classic that retained the original ledger with the hack, and the new Ethereum chain that applied a rollback (Morrison et. al, 2020; Zhang, 2021). Although the present 2016 case precedes modern security practice such as standardized audit procedures and formal verification tools, which nowadays mitigate against reentrancy vulnerability (Atzei et al., 2017), it is analytically important that the lack of remedies against the negative impact of post-execution consumer harm was recognized by the community as the sole solution: the controversial hard fork, which is currently replicated even in the light of improved security measures.

4.3.2. ASIX Token Case Analysis

Continuing on the lessons of The DAO hack, the ASIX Token case also demonstrates a larger implication of the smart contract vulnerabilities and the insufficiency of the current regulatory systems in delivering any kind of consumer protection. The case was characterized by widespread post-execution consumer harm, in which smart contracts had unsolvable vulnerabilities that subjected consumers to substantial financial losses with no effective mechanism to respond, and the immutable execution of code was examined to continue causing consumer harm indefinitely (Dai et al., 2022). Security audit study identified severe architectural issues such as unlichidated access controls which allowed one to mint tokens exceeding the intended limit as well as transfer limitation features which could irrevocably place user funds in lock, showing weaknesses not related to the reentrancy attacks mitigated by current safety standards. Regulatory response was also terribly ineffective, with the absence of holistic regulatory frameworks in most jurisdictions aggravating such consumer protection issues, and inconsistent and often inadequate handling of smart contract regulation by different countries not offering appropriate or prompt redress (Caglayan Aksoy, 2022). The evaluation of long-term consumer effects showed a financial loss that persisted, undermined the trust in automated systems, and further susceptibility to other attempts like the ones, which entailed the inability of consumer protection in the aftermath of the execution, which can have long-lasting detrimental effects on individual individuals and the confidence in the smart contract implementation in the market (Carata and Knottenbelt, 2024).

4.3.3. Automated Insurance Claims Failures

The introduction of automated insurance claims processing based on the use of smart contracts demonstrates a high level of consumer protection issues when executing a post-execution contract, in particular, in malfunctions of flight delay compensation systems, where systemic claim denials were caused by the inability of the algorithm to detect systematic errors. The system of flight delay compensation proved to be crippling when smart contracts misunderstood data feeds or used flawed logic, resulting in mass consumer harm without a sufficient appeals procedure, because a lack of human judgment capability to handle edge cases and contextual conditions to legitimate claims meant that these automated systems were incompetent to support edge cases (Alruwaill et al., 2023). The consumer dispute resolution limits were also evident whenever affected passengers found there was no proper recourse to challenge automated decisions, as old-fashioned insurance ombudsman procedures did not ensure effective resolution of automated system failures, which left consumers without an option when smart contracts made inaccurate decisions based on the errors of the code or data feed failure (Yu et al., 2021). Systemic failure pattern analysis showed that similar problems such as oracle manipulation, logic errors in compensation calculation, and inadequate exception handling were recurrent and automated insurance claims systems can perpetuate consumer harm through a series of systematic failures that current regulatory frameworks could not sufficiently address or prevent (Dai et al., 2022).

4.3.4. DeFi Financial Transaction Failures

Moving beyond the issue of insurance failure, Decentralized Finance (DeFi) applications show major loopholes in consumer protection in peer-to-peer transaction regimes where smart contract vulnerabilities lead to permanent financial losses. DeFi applications that rely on smart contracts to remove the usual financial intermediaries have had systematic failures in which the automated lending protocols, due to coding errors, would lock consumer funds permanently or redistribute them to the wrong people, and there is no way to recover the funds or resolve any disagreement (Hegde and Hegde, 2024). Such collapses illustrate how increased transparency and lowering the price are achieved through the cost of consumer protection as traditional financial intermediaries are eliminated and consumer protection and recourse mechanisms are established to regulate

financial institutions are abolished (Guelida et al., 2024). Nevertheless, there are protocols that have introduced countermeasures: Uniswap has time-locking of governance, which does not allow immediate administration change, and the inability to make immediate changes in governance by the community was demonstrated by Compound in 2024 when a governance attack was being attempted (Charoenwong et al., 2025). These illustrate how even when they exist, protocol-specific governance mechanisms can offer consumer protection, but underscores the gap our framework fills: protection is only available when a particular protocol is designed and not available when it is based on the systematic requirements, is only effective when a platform is governance-enabled and is only practiced when it is under human vigilance in contrast to principles of automation. Although blockchain-based systems of cross-border payment systems have positive impacts on the speed and security of payment and have demonstrated vital weaknesses, in cases where smart contracts in identity verification procedures became malfunctional, the transfer of consumer funds to the wrong wallets remained unnoticed because there was no regulatory framework to mediate the malfunction of automated payment systems (Singh et al., 2024).

4.3.5. Islamic Finance Governance and Legal Recognition Challenges

The last case study analysis shows that the implementation of smart contracts in the governance structures, especially the Islamic financial systems, subjects consumers to regulatory risks and jurisdictional challenges that compromise the conventional consumer protection procedures. The realisation of smart contracts in Islamic finance in Malaysia and Singapore is an example of how the efforts to reconcile common law with Sharia law cause legal ambiguity over the enforceability and dispute resolution process, which places consumers at the disadvantage when automated systems clash with Sharia or traditional legal norms (Song and Tan, 2024). The failures of the governance of smart contract in Islamic finance demonstrate how decentralized systems of authority can undermine existing centralized consumer protection structures, leaving consumers unable to get any regulatory redress in situations where automated transactions are not necessarily compliant with Sharia compliance criteria but are written in stone (Surve et al., 2025). There are no specific regulatory amendments and strategic plans to mitigate these legal ambiguities that imply that consumers in Islamic finance smart contract systems do not have a good remedy in automatic decision-making when it contradicts the religious legal provisions and the customary consumer protection laws (Acharya & Kulshrestha, 2024).

5. Discussion

Systematic analysis across four dimensions reveals a consistent pattern: while blockchain The systematic examination of four dimensions reveals that a similar trend exists in that blockchain consumer protection studies and regulation do a great deal in the area of pre-execution protection, but post-execution consumer remediation is severely lacking. Based on bibliometric analysis of 153 literature, it is revealed that clusters of research focus on privacy mechanisms, technical implementation, and financial security are all independent without built-in post-implementation protection streams. According to comparative legal analysis, even with the recent adaptive response to the problem such as MiCA (2024) and regulatory sandbox mechanisms, all three advanced jurisdictions (EU, Singapore, Japan) score highly in pre-contractual protection, though below 1/10 in post-execution remedies, with resolution rates below 10. There are fine technological protection systems in insurance, supply chain, and e-commerce applications, which nonetheless fail where blockchain with its unalterability prevents more conventional remediation. In the 2016 case of the DAO hack that necessitated a contentious hard fork as the last resort, to the current ASIX and DeFi platform collapses, case studies confirm that consumer harm is crystallizing after the fact, when the outcomes of the code

become irreversible, and protocol-specific remedies such as the governance delays at Compound are still ad hoc decisions.

This convergent evidence indicates a disconnect of fundamental theoretical nature that needs a new framework approach. The Code as Law theory developed by Lessig (1999) describes the role of computer code as regulatory force as more powerful than traditional law in that it directly influences behavior directly via technical architecture without human interpretation or enforcement mechanisms. In contrast to the traditional law, in which law follows the interpretation of a human being, code is the law that enforces itself and absolutely (Brownsword, 2019). Smart contracts are the final form of this theory, which turns legal contracts into self-executing programs that execute automatically and form what De Filippi and Wright (2018) call lex cryptographialex cryptographic legal system that exists alongside traditional legal systems. Nevertheless, in the context of law being code, the classic consumer protection mechanisms of safety become absent because smart contracts do not take an altered situation into account and act as programmed without regard to fairness and vulnerability of consumers (Werbach, 2018). Code-based law is deterministic, so it is impossible to apply consumer protection to the code after deployment but must be part of the technological architecture directly (Finck, 2019). It has far-reaching consequences: conventional consumer protection is based on the principle of fairness, good faith, and judicial discretion to address the problem of power imbalance, but these measures cannot be used in the case of automated execution (Werbach and Cornell, 2017).

In blockchain systems, recent work on computational theory demonstrates the existence of an underlying set of limitation on the possibilities to make regulatory choices. Charoenwong et al. (2025) provide formal evidence that, on the one hand, systems that are permissionless and Turing-complete are incapable of proving that they satisfy some regulatory specifications because of the Rice-Theorem--no algorithm, on the other hand, can classify arbitrary programs based on their regulatory compliance without executing them. These computational constraints bring about inescapable tradeoff: meaningfully automated compliance must be either by the provision of permission mechanisms, or by the restriction of systems to non-Turing-complete programming languages, in which mechanical verification is possible (Charoenwong et al., 2025; Turing, 1937). In addition to theoretical impossibility, smart contracts are subject to practical constraints of computing resources in a blockchain execution environment, impossibility of correcting even post-deployment errors, and bottlenecks in performance due to consensus mechanisms (Tonelli et al., 2023; Pace et al., 2020). These theoretical limits are not disregarded in our framework. In contrast to mechanisms that seek to mechanically verify arbitrary smart contract code before execution (computational impossible), our system uses a hybrid system of governance a combination of specially verified specific properties of the consumer protection (e.g. contract includes cooling-off period a decidable property but not the behaviour of the general code), human intervention in complex disputes where the algorithmic resolution is inadequate, and off-chain mechanisms of governance that allow intervention to be taken after the contract has been executed without needing to modify the on-chain code.

The conceptual gap in solving these challenges is expected to be found in the Algorithmic Accountability theory. Diakopoulos (2020) insists that algorithmic systems that have public power should be under the accountability mechanisms to guarantee transparency, explainability, and accountability of their consequences. Yeung (2018) builds upon it with the idea of algorithmic governance, a new general framework that will hold the automated decision-making systems accountable to human values and the law. When applied to smart contracts, this theory can help identify several levels of intervening: transparency would involve a code that is truly auditable and readable to stakeholders such as regulators and consumer advocates (Kemper and Kolkman, 2019); explainability would involve logic and outcomes that are communicated in a language that is easily understandable by average consumers (Miller, 2019); contestability would mean that consumers can challenge unfair results despite the execution of the code (Hirsch,

2018); responsibility would imply that the consequences of using smart contracts are attributed clearly These principles indicate that effective consumer protection needs a combination of both unchangeable on-chain implementation and changeable off-chain governance solutions that offer solutions in case there is a conflict between the code-based outcomes and the consumer rights (Zetzsche et al., 2019). This conceptual integration - Code as Law recognition that protection must be implemented in the technology, computational constraint recognition that it is impossible to achieve pure mechanical verification, and Algorithmic Accountability principles that focus on transparency and contestability are the basis of our overall framework.

In the context of theoretical integration and empirical results, we suggest the Comprehensive Post-Execution Consumer Protection Framework depicted in Figure 5. The framework architecture focuses on an Oversight and Control Hub that offers governance coordination, regulatory interface and cross-jurisdictional cooperation -a similar role to a Data Protection Officer role in GDPR frameworks but tailored to smart contract consumer protection. It is a central governance core which links five layers of operations addressing perceived gaps in a systematic approach, external environment factors include regulatory requirements (MiCA, Data Act), monitoring (consumer agencies, industry standards), participation of stakeholders (consumers, developers, platforms) and quantification (compliance metrics, effectiveness dashboards) interact with all layers to ensure responsiveness to changes in technological and regulatory realms.

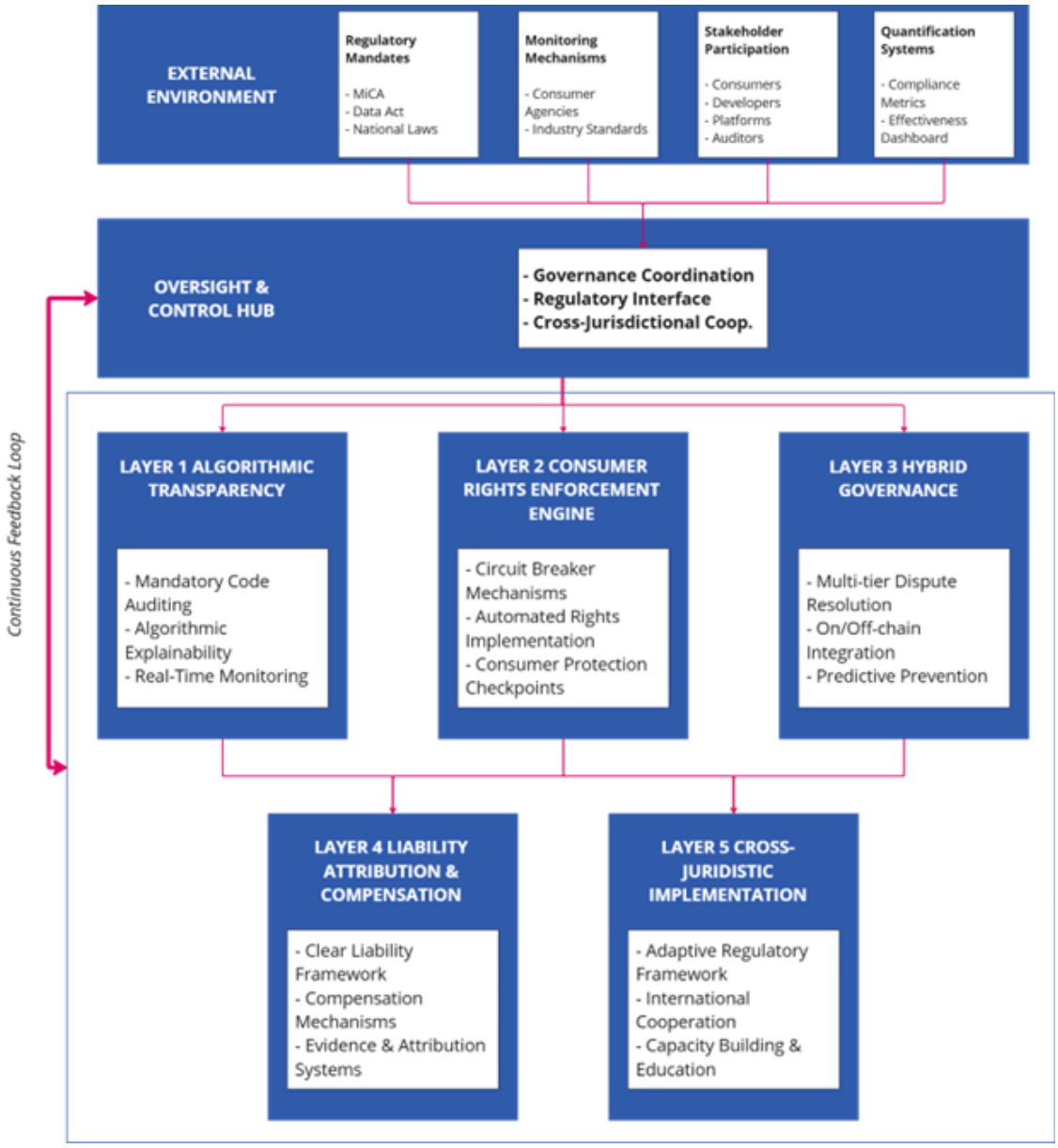

Figure 5. Comprehensive Post-Execution Consumer Protection Framework

Layer 1 (Algorithmic Transparency) provides the base of visibility by using compulsory

code auditing accompanied by consumer protection standards, algorithmic explainability by offering plain language explanations of contract logic, and real-time monitoring of anomalies that have occurred post-execution. This layer is based on bibliometric evidence of absence of integrated transparency mechanisms and meets the main requirement of the Algorithmic Accountability theory according to which the code should be, in fact, auditable (Kemper and Kolkman, 2019). Utilization is based on pre-existing audit infrastructure (OpenZeppelin, Certora) supplemented with consumer-friendly checkpoints, and this layer can be implemented immediately with the current technology and respond to the practical limitations identified during the analysis of technical documentation (Tonelli et al., 2023). The Layer 2 (Consumer Rights Enforcement) has integrated conventional consumer rights in automated systems by circuit breaker systems that stop execution when protection breaches are detected, automated cooling-off period enforcement and persistent compliance checkpoints. This tier is a direct response to the inadequacy of legal frameworks in which, even after executing the agreement, the traditional consumer-related rights cannot be enforced, as such that Code as Law theory requires the adoption of ex-ante technological design rather than ex-post judicial-imposed solutions (Finck, 2019). More crucially, computationally solvable properties such as the existence of a 14-day withdrawal window are used to check at this layer instead of trying to verify the entire code, which fits into the framework of Charoenwong et al. (2025) where verification of specific properties is still possible even when it is impossible to verify the entire code.

The layer 3 (Hybrid Governance & Dispute Resolution) regulates the gap between blockchain immutability and the needs of consumer remedies through multi-tiered resolution (automated to solve common cases, human arbitration to address complicated scenarios), on-chain/off-chain integration ensuring the maintenance of immutable audit trails and allowing flexible remedies, and predictive harm prevention using pattern recognition. Such a layer responds to the findings of case studies indicating no possible recourse in the event of consumer harm due to smart contract performance, which is the contestability requirement of the Algorithmic Accountability theory, which requires that the consumers are capable of contesting the unfair outcomes even after running the code (Hirsch, 2018; Kluttz et al., 2020). The hybrid method is a direct reaction to the computational impossibility outcomes that propose human judgment in the situations where the mechanical verification is not possible, instead of trying to solve the halting problem, the framework uses its human oversight to carefully place the automated systems at the point of their computational ability (Charoenwong et al., 2025). The fourth layer (Liability Attribution & Compensation) is a system of accountability where the algorithmic systems harm consumers with well-defined liability schemes (developer, platform, auditor roles), compensation schemes (insurance funds, scheme funded by the developers), and forensic evidence systems to analyze the incident after the fact. This tier addresses the cross-jurisdictional issue of responsibility where algorithmic systems cause injury to consumers by applying the responsibility principle of the Algorithmic Accountability theory, which requires explicit designation of liability (Martin, 2019; Lehr and Ohm, 2017). This is in contrast to protocol-specific solutions that have been seen in case studies (the governance of Compound slows down and MakerDAO writes down debts), except that, it forms a pattern of responsibility attribution that is applicable to all implementations of smart contracts.

Layer 5 (Cross-Jurisdictional Implementation) allows adaptation to different regulatory contexts using context-sensitive requirements (graduated by digital literacy and institutional capacity), cross-border enforcement protocols, and capacity building (to provide sufficient technical expertise). The layer responds to the comparative legal analysis results that indicate the necessity to use adaptive approaches to different regulatory environments considering that although legal systems have demonstrated adaptive capacity through MiCA regulation and regulatory sandboxes (Zetzsche et al., 2017; Ringe and Ruof, 2020), they have inherent temporal constraints where legal processes take place in a multi-year timeframe whereas technological capabilities

constantly change. The framework recognizes that standardized international implementation is impractical and instead offers loose channels that respect the jurisdictional variation but still protects core consumer rights- taking into consideration the fact that standardized adaptation to regulation is feasible, yet it is still grappling with the post-implementation protection despite the jurisdictional differences (Benseghir and Bendriss, 2025; Song and Tan, 2024).

Technical feasibility is dependent on layer: Layer 1-2 are right now implementable with available audit tools and circuit breaker patterns that have already been implemented in DeFi protocols; Layer 3 needs dispute resolution protocols to become a standard; Layer 4-5 needs regulation and global coordination (5+ years). The economic viability of prevention must be based on being cheaper than remediation - incentives when reputation is being sought by industry and mandated compliance regulations can lead to adoption, but the small developer burden requires incremental requirements and possible subsidy support. The regulatory preparedness varies between jurisdictions: MiCA is offering an excellent base in EU at Layers 1-2; Singapore's sandbox framework is applicable to Layer 3 piloting; Layer 4 can be implemented with the help of the registration system in Japan; and Layer 5 will have to be coordinated internationally, which is currently not possible, but can be achieved through incremental bilateral arrangements. Advantages of frameworks are systematic consumer protection, compatibility in computational constraints by governing hybrid systems, scalability because of cross jurisdictional adaptive implementation, and the ability to maintain the benefits of blockchain-enabled efficiency without introducing safety nets. Limitations are: Industry collaboration is required to enforce regulatory requirement, Layers 3-5 are not developed in time, and all consumer harm is not eliminated (only mitigated), and there will inevitably exist a tension between the principles of automation and the need to have a human intervene in complex cases-tensions inherent in the Code as Law theory of recognizing that when law is turned into code, it must reintroduce human judgment mechanisms strategically where algorithmic absolutism will generate unfair results (Brownsword, 2019; Werbach, 2018). As opposed to current methods, our framework offers systematic protection over protocol-specific ones, integrates protection on a technological level instead of current regulation based on the principles of Code as Law, and transitions zero protection to multi-dimensional protection by means of the Algorithmic Accountability principles- but requires co-ordinated stakeholder commitment and time to scale its implementation to all layers.

6. Conclusions

The research fills a gap in consumer protection in the implementations of smart contracts by creating a holistic, post-execution consumer protection scheme that tackles the underlying incompatibility of blockchain immutability and the conventional consumer rights. Formal analysis indicates that the current strategies, albeit due to adaptive measures like MiCA regulation, regulatory sandboxes, and protocol-specific solutions, such as Compound governance delays, are disjointed and ineffective to cover the most vulnerable stage when consumer harm is already irreversible, but regulatory action is still ineffective. The suggested five-layer model combines the transparency of algorithms, automated rights, hybrid governance, the systems of liability attribution, and cross-jurisdictional implementation schemes, which is a paradigm shift as opposed to ex-post judicial remedies and ex-ante technological design. More importantly, this framework recognizes computational limitations known by Charoenwong et al. (2025), which execute specific verification of determinable consumer protection properties and strategic human supervision instead of trying impossible mechanical verification of arbitrary code. The framework allows smart contracts to retain their advantage in efficiency by running hybrid on-chain / off-chain systems offering high-level consumer protection that functions well in the immutable architecture of blockchain.

This study has identified such limitations as dependence on developing technologies (machine learning-based predictive prevention, cross-chain interoperability), orientation to three high-level jurisdictions that may make it difficult to implement the study results in developing countries with another legal tradition and technical capacity, and the rapid changes in smart contract vulnerabilities, which will need continuous revision of the framework. Further studies must create technical implementation guidelines at each layer, pilot implementations that can validate cross-border performance, scale the framework to newer technologies (AI-integrated smart contracts, quantum-resistant systems), create a quantitative measure of the outcome of post-implementation consumer protection, investigate the economic consequences of mandatory algorithmic accountability on implementation costs and innovation incentives, and create specialized training to ensure successful implementation in different stakeholder communities.

Acknowledgment
The authors would like to express their sincere gratitude to all individuals and organizations that contributed to this research. Special appreciation goes to our colleagues and mentors at the Faculty of Law, for their invaluable support, insightful feedback, and constructive guidance throughout the research process.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement
The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Declaration of Generative AI Use
The author confirms that no generative AI tools or large language models were used at any stage during the preparation, writing, or editing of this manuscript.

Ethics Approval Statement
This study did not involve human participants, animals, or any sensitive data requiring ethical approval. Therefore, ethical approval was not applicable.

Declaration of Competing Interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Acharya, N., and S. Kulshrestha. "Smart Contracts and the Application of Blockchain in the Legal System." *Smart Innovation, Systems and Technologies*, 2024.

Albaroodi, H. A., and M. Anbar. "Security Issues and Weaknesses in Blockchain Cloud Infrastructure: A Review Article." *Journal of Applied Data Sciences* 6, no. 1 (2025): 155-177.

Allen, J. G. "Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language." *European Review of Contract Law* 14, no. 4 (2018): 307-343.

Alruwaill, M., A. K. Bapatla, S. P. Mohanty, and E. Kougianos. "FarmIns: Blockchain Leveraged Secure and Reliable Crop Insurance Management System." In *IFIP*

International Internet of Things Conference, 381-389. Cham: Springer Nature Switzerland, 2023.

Ananny, M., and K. Crawford. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media & Society* 20, no. 3 (2018): 973-989.

Arrieta, A. B., N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, ... and F. Herrera. "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI." *Information Fusion* 58 (2020): 82-115.

Atzei, N., M. Bartoletti, and T. Cimoli. "A Survey of Attacks on Ethereum Smart Contracts (SOK)." In *International Conference on Principles of Security and Trust*, 164-186. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017.

Barański, S., J. Szymański, and H. Mora. "Anonymous Provision of Privacy-Sensitive Services Using Blockchain and Decentralised Storage." *International Journal of Information Security* 24, no. 3 (2025): 1-23.

Benseghir, M., and H. Bendriss. "The Consumer's Right to Withdraw from Blockchain Smart Contracts: Challenges and Solutions." In *Studies in Systems, Decision and Control*, Vol. 565, 79-89. Springer, 2025.

Binns, R. "Algorithmic Accountability and Public Reason." *Philosophy & Technology* 31, no. 4 (2018): 543-556.

Boopathi, M., S. Gupta, A. M. Zabeeulla, R. Gupta, V. Vekriya, and A. K. Pandey. "Optimization Algorithms in Security and Privacy-Preserving Data Disturbance for Collaborative Edge Computing Social IoT Deep Learning Architectures." *Soft Computing* (2023): 1-13.

Breuer, C., S. Dallmeyer, C. Rumpf, and J. Orlowski. "The Effect of Sponsorship Portfolio Size on Brand Choice: An Experimental Approach." *Applied Economics* 53, no. 10 (2021): 1200-1211.

Brownsword, R. *Law, Technology and Society: Reimagining the Regulatory Environment*. London: Routledge, 2019.

Buocz, T., T. Ehrke-Rabel, E. Hödl, and I. Eisenberger. "Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks." *Computer Law & Security Review* 35, no. 2 (2019): 182-198.

Buterin, V. "A Next-Generation Smart Contract and Decentralized Application Platform." *White Paper* 3, no. 37 (2014): 2-1.

Çağlayan Aksoy, P. "Smart Contracts: To Regulate or Not? Global Perspectives." *Law and Financial Markets Review* 16, no. 3 (2022): 212-241.

Carata, C., and W. J. Knottenbelt. "An Analysis of the MiCA Regulation and Its Impact for the Blockchain-Based Economies." In *The International Conference on Mathematical Research for Blockchain Economy*, 359-370. Springer, Cham, 2024.

Charoenwong, Ben, Kowaleski, Zach, Kwan, Alan, and Sutherland, Andrew. "RegTech." *Journal of Financial Economics* 154, No. 103792 (2024). Available at SSRN: https://ssrn.com/abstract=4000016

Chen, Y., and C. Bellavitis. "Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models." *Journal of Business Venturing Insights* 13 (2020): e00151.

Chen, K., Y. Fan, and S. S. Liao. "Token Incentives in a Volatile Crypto Market: The Effects of Token Price Volatility on User Contribution." *Journal of Management Information Systems* 40, no. 2 (2023): 683-711.

Citron, D. K., and F. Pasquale. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89 (2014): 1.

Coglianese, C., and D. Lehr. "Transparency and Algorithmic Governance." *Administrative Law Review* 71, no. 1 (2019): 1-56.

Cohney, S., D. Hoffman, J. Sklaroff, and D. Wishnick. "Coin-Operated Capitalism." *Columbia Law Review* 119, no. 3 (2019): 591-676.

Dai, M., Z. Yang, and J. Guo. "SuperDetector: A Framework for Performance Detection on Vulnerabilities of Smart Contracts." In *Journal of Physics: Conference Series*, Vol. 2289, No. 1, p. 012010. IOP Publishing, 2022.

Das, M. R. "Trend and Progress of Electronic Retail Payment Systems in India in the Post-Pandemic Period." *Vinimaya* 45, no. 1 (2024): 39-52.

De Filippi, P., and A. Wright. *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018.

De Souza, J. S., J. M. Abe, L. A. de Lima, and N. A. de Souza. "The General Law Principles for Protection the Personal Data and Their Importance." arXiv preprint arXiv:2009.14313 (2020).

DeFi Llama. "DeFi Llama – Decentralized Finance Dashboard." 2024. Retrieved from https://defillama.com/

Diakopoulos, N. "Accountability, Transparency." In *The Oxford Handbook of Ethics of AI* 17, no. 4 (2020): 197.

Divyashree, K. S. "Safeguarding the Future through the Prevention of Cybercrime in the Quantum Computing Era." In *Next Generation Mechanisms for Data Encryption*, 258-276. CRC Press, 2025.

Dupont, B. "The Cyber-Resilience of Financial Institutions: Significance and Applicability." *Journal of Cybersecurity* 5, no. 1 (2019): tyz013.

Edwards, L., and M. Veale. "Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?" *IEEE Security & Privacy* 16, no. 3 (2018): 46-54.

European Commission. "Consumer Rights Directive." 2022. https://ec.europa.eu/info/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en

European Law Institute. "ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection." 2022. https://www.europeanlawinstitute.eu/

European Parliament. "Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)." *Official Journal of the European Union*, L 150/40, 2023.

Fairfield, J. A. "BitProperty." *Southern California Law Review* 88 (2014): 805.

Fang, P., L. Wan, and W. Fang. "The Choice of Cooperative Governance Mechanism in Open Innovation Projects under the Synergy of the Electricity–Carbon Market." *Energies* 16, no. 17 (2023): 6110.

Finck, M. "Smart Contracts as a Form of Solely Automated Processing under the GDPR." *International Data Privacy Law* 9, no. 2 (2019): 78-94.

Finck, M. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018.

Financial Services Agency (FSA) Japan. "Payment Services Act." 2023. https://www.fsa.go.jp/en/

Forment, M. A., D. A. Filvà, F. J. García-Peñalvo, D. F. Escudero, and M. J. Casañ. "Learning Analytics' Privacy on the Blockchain." In *Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality*, 294-298, 2018.

Gikay, A. A. "European Consumer Law and Blockchain Based Financial Services: A Functional Approach against the Rhetoric of Regulatory Uncertainty." 2019.

Grimmelmann, J., and C. Mulligan. "Data Property." *American University Law Review* 72 (2022): 829.

Guelida, O., S. Jai Andaloussi, and O. Ouchetto. "Smart Contracts in Finance and Banking Systems in the Era of Industry 5.0: A Systematic Review." In *Industry 5.0 and Emerging Technologies: Transformation Through Technology and Innovations*, 317-346, 2024.

Guo, H., W. Li, M. Nejad, and C. C. Shen. "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-Based Cryptographic Mechanisms." *IEEE Transactions on Network and Service Management* 20, no. 2 (2022): 1759-1774.

Hegde, S. K., and R. Hegde. "An Efficient and Transparent Financial Transaction System Using Decentralized Finance (DeFi) Based on Blockchain Technology." In *2024 2nd International Conference on Recent Advances in Information Technology for Sustainable Development (ICRAIS)*, 18-23. IEEE, 2024.

Hein, Z., Vysochkin, A. V., Paing Htoo, T., Bezzateev, S. V., Voloshina, N. V., and Portnov, E. M. "Research and Development of a Smart Contract Algorithm for the Implementation of Blockchain Technology on Mobile Devices." In *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2021)*, 1891-1896. IEEE, 2021.

Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., ... and Roşu, G. "KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine." In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 204-217. IEEE, 2018.

Hirsch, N. "A Use Case for Blockchain Technology in Internal Combustion Engine Emissions Reporting." Doctoral dissertation, Hochschule Furtwangen, 2018.

Jannat, S. "Crowdfunding Dilemmas: Understanding the Roadblocks in Bangladesh's SME's Financial Landscape." *International Journal of Innovation Science* (2025).

Kayani, U., and F. Hasan. "Unveiling Cryptocurrency Impact on Financial Markets and Traditional Banking Systems: Lessons for Sustainable Blockchain and Interdisciplinary Collaborations." *Journal of Risk and Financial Management* 17, no. 2 (2024): 58.

Kemper, J., and D. Kolkman. "Transparent to Whom? No Algorithmic Accountability without a Critical Audience." *Information, Communication & Society* 22, no. 14 (2019): 2081-2096.

Kluttz, D. N., N. Kohli, and D. K. Mulligan. "Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions." In *Ethics of Data and Analytics*, 420-428. Auerbach Publications, 2022.

Kroll, J. A. "The Fallacy of Inscrutability." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 20180084.

Kumar, R. B. "The New Digital Deal: How Data Is Shaping Our Social Contract." *IUP Law Review* 15, no. 2 (2025).

Laxmi Kanth, P., O. Sri Nagesh, V. S. S. P. L. N. Balaji Lanka, and P. Ramamohan Rao. "Medical Data Security with Blockchain and Artificial Intelligence Using SecNet." In *XVIII International Conference on Data Science and Intelligent Analysis of Information*, 457-466. Cham: Springer Nature Switzerland, 2023.

Lehr, D., and P. Ohm. "Playing with the Data: What Legal Scholars Should Learn about Machine Learning." *UC Davis Law Review* 51 (2017): 653.

Lessig, L. "Code and the Commons." Keynote Address at the Conference on Media Convergence, held at Fordham University Law School, February 1999.

Li, G., and H. Sato. "A Privacy-Preserving and Fully Decentralized Storage and Sharing System on Blockchain." In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2, 694-699. IEEE, 2019.

Liu, Y., T. Li, R. Zhang, Z. Jin, M. Tong, W. Liu, ... and Z. Yang. "A Context-Aware Clustering Approach for Assisting Operators in Classifying Security Alerts." *IEEE Transactions on Software Engineering* (2024).

Loos, M., and J. Luzak. "Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers." *Journal of Consumer Policy* 39 (2016): 63-90.

Lu, W., and L. Wu. "A Blockchain-Based Deployment Framework for Protecting Building Design Intellectual Property Rights in Collaborative Digital Environments." *Computers in Industry* 159 (2024): 104098.

Malamas, V., T. K. Dasaklis, V. Arakelian, and G. Chondrokoukis. "A Blockchain Framework for Digitizing Securities Issuance: The Case of Green Bonds." *Journal of Sustainable Finance & Investment* 14, no. 3 (2024): 569-595.

Martin, R. J. "Consumer Welfare in Online Markets." Doctoral dissertation, UCLA, 2019.

Martinez, D., L. Magdalena, and A. N. Savitri. "AI and Blockchain Integration: Enhancing Security and Transparency in Financial Transactions." *International Transactions on Artificial Intelligence* 3, no. 1 (2024): 11-20.

Mihailescu, M. I., and S. L. Nita. "Securing Web Data and Privacy in AIoT Systems." In *Semantic Web Technologies and Applications in Artificial Intelligence of Things*, 128-172. IGI Global, 2024.

Miller, T. "Explanation in Artificial Intelligence: Insights from the Social Sciences." *Artificial Intelligence* 267 (2019): 1-38.

Mogos, M. F., and G. Fragapane. "Ways to Circular and Transparent Value Chains." In *IFIP International Conference on Advances in Production Management Systems*, 390-398. Cham: Springer Nature Switzerland, 2022.

Monetary Authority of Singapore (MAS). "MAS Notice 650: Notice on Prevention of Money Laundering and Countering the Financing of Terrorism." 2023. https://www.mas.gov.sg/

Morrison, R. S. "Advance Directives/Care Planning: Clear, Simple, and Wrong." *Journal of Palliative Medicine* 23, no. 7 (2020): 878-879.

Muntean, O. M., and C. Pungila. "Unmasking Blockchain Fraud: A Review of AML Challenges and Regulatory Shortcomings." In *2025 IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 000083-000088. IEEE, 2025.

Murray, A., and C. Scott. "Controlling the New Media: Hybrid Responses to New Forms of Power." *The Modern Law Review* 65, no. 4 (2002): 491-516.

Nguyen, K. Q., T. H. Nguyen, and B. L. Do. "Narrative Attention and Related Cryptocurrency Returns." *Finance Research Letters* 56 (2023): 104174.

Okezie, P. "Resolving Smart Contract Disputes through Blockchain Arbitration." *Arbitration* 90, no. 2 (2024): 131-145.

Omar, I. A., H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar. "Implementing Decentralized Auctions Using Blockchain Smart Contracts." *Technological Forecasting and Social Change* 168 (2021): 120786.

Pace, G. J., Sánchez, C., and Schneider, G. "Reliable Smart Contracts." In *Lecture Notes in Computer Science*, Vol. 12426, 275-293. Springer, 2020.

Paglietti, M. C., and M. Rabitti. "A Matter of Time. Digital-Financial Consumers' Vulnerability in the Retail Payments Market." *European Business Law Review* 33, no. 4 (2022).

Pasquale, F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.

Psarra, E., D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas. "Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records." *BMC Medical Informatics and Decision Making* 24, no. 1 (2024): 303.

Qaffas, A. A. "Metamorphose Digital Marketing with Cybersecurity Data Privacy Federation Utilizing Blockchain." In *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*, 1534-1541. IEEE, 2024.

Rahman, J., Rahman, H., Islam, N., Chowdhury, M. J. M., Afroz, S., Iqbal, R., and Ali, M. "Regulatory Landscape of Blockchain Assets: Analyzing the Drivers of NFT and Cryptocurrency Regulation." *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 5, no. 1 (2025): Article 100229.

Raskin, M. "The Law and Legality of Smart Contracts." *Georgetown Law Technology Review* 1 (2016): 305.

Reyes, C. L. "Law's Detrimental Reliance on Intermediaries." *George Washington Law Review* 92, no. 2 (2024): 345-420.

Rice, H. G. "Classes of Recursively Enumerable Sets and Their Decision Problems." *Transactions of the American Mathematical Society* 74, no. 2 (1953): 358-366.

Ringe, W. G., and Ruof, C. "Regulating Fintech in the EU: The Case for a Guided Sandbox." *European Journal of Risk Regulation* 11, no. 3 (2020): 604-629.

Rott, P. "The Balance in Consumer Protection between Substantive Law and Enforcement." *European Review of Private Law* 31, no. 4 (2023).

Savage, J. E. *Models of Computation: Exploring the Power of Computing* (1st ed.). Addison-Wesley Longman Publishing Co., Inc., 1997.

Savelyev, A. "Legal Aspects of Ownership in Modified Open Source Software and Its Impact on Russian Software Import Substitution Policy." *Computer Law & Security Review* 33, no. 2 (2017): 193-210.

Scholz, L. H. "Algorithmic Contracts." *Stanford Technology Law Review* 20 (2017): 128.

Scholz, L. H. "Algorithmic Contracts." *Stan. Tech. L. Rev.* 20 (2018): 128.

Selbst, A. D., and S. Barocas. "The Intuitive Appeal of Explainable Machines." *Fordham Law Review* 87 (2018): 1085.

Seneviratne, O. "The Feasibility of a Smart Contract 'Kill Switch'." In *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, 473-480. IEEE, 2024.

Singh, J., S. Rani, and P. Kumar. "Blockchain and Smart Contracts: Evolution, Challenges, and Future Directions." In *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, Vol. 1, 1-5. IEEE, 2024.

Song, J. Y. L., and E. Tan. "Beyond Traditional Contracts: The Legal Recognition and Challenges of Smart Contracts in Malaysia and Singapore." *Journal of Law, Market & Innovation* (2024): 323.

Sooksripaisarnkit, P. "Blockchain-Based Bills of Lading and the UNCITRAL Model Law on Electronic Transferable Records: Questions of Compatibility." In *The Elgar Companion to UNCITRAL*, 525-540. Edward Elgar Publishing, 2023.

Stazi, A., and R. Jovine. "GMOs, Food Traceability and RegTech." 2024.

Surve, T., A. K. Tyagi, and B. F. Balogun. "Blockchain for Smart Finance: A Review of Architectures, Integration Trends and Future Research Directions." *Procedia Computer Science* 259 (2025): 316-325.

Szabo, N. "Formalizing and Securing Relationships on Public Networks." *First Monday* (1997).

Tjong Tjin Tai, E. "Formalizing Contract Law for Smart Contracts." 2017.

Tonelli, R., Pierro, G. A., Ortu, M., and Destefanis, G. "Smart Contracts Software Metrics: A First Study." *PLoS ONE* 18, no. 2 (2023): e0281537.

Turing, A. M. "On Computable Numbers, with an Application to the Entscheidungsproblem." *Proceedings of the London Mathematical Society*, s2-42, no. 1 (1937): 230-265.

Wachter, S., B. Mittelstadt, and C. Russell. "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR." *Harvard Journal of Law & Technology* 31 (2017): 841.

Wahhab, B. M. A., S. M. Hussein, and R. Rajamanickam. "Incorporating Emerging Technologies for Enhancing Data Privacy Protection Regulations." 2025.

Wang, X., J. H. Ryoo, M. C. Campbell, and J. J. Inman. "Unraveling Impact: Exploring Effects of Novelty in Top Consumer Research Journals." *Journal of Consumer Research* 51, no. 1 (2024): 169-179.

Werbach, K. *The Blockchain and the New Architecture of Trust*. Cambridge, MA: MIT Press, 2018.

Werbach, K., and N. Cornell. "Contracts Ex Machina." *Duke Law Journal* 67 (2017): 313.

Winarto, W. "Building an International Regulatory and Legal Framework for Green Digital Finance." *Revista Jurídica Portucalense* (2025): 190-213.

Yaqub, N., J. Zhang, M. I. Khalid, W. Wang, M. Helfert, M. Ahmed, and J. Kim. "Blockchain Enabled Policy-Based Access Control Mechanism to Restrict Unauthorized Access to Electronic Health Records." *PeerJ Computer Science* 11 (2025): e2647.

Yeung, K. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12, no. 4 (2018): 505-523.

Yin, T., Zhang, C., Ni, Y., Wang, L., and Guo, Y. "An Empirical Study on Implicit Constraints in Smart Contract Static Analysis." In *Proceedings - International Conference on Software Engineering*, 50-61. IEEE, 2022.

Yu, Y., Q. Li, Q. Zhang, W. Hu, and S. Liu. "Blockchain-Based Multi-Role Healthcare Data Sharing System." In *2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM)*, 1-6. IEEE, 2021.

Zhang, L., Z. Zhang, W. Wang, Z. Jin, Y. Su, and H. Chen. "Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment." *IEEE Systems Journal* 16, no. 2 (2021): 2822-2833.

Zhang, T., and Z. Huang. "Blockchain and Central Bank Digital Currency." *ICT Express* 8, no. 2 (2022): 264-270.

Zetzsche, D. A., R. P. Buckley, D. W. Arner, and L. Fohr. "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators." *Harvard International Law Journal* 60 (2019): 267.

Zetzsche, D. A., R. P. Buckley, J. N. Barberis, and D. W. Arner. "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation." *Fordham Journal of Corporate & Financial Law* 23, no. 31 (2017).

Zetzsche, D. A., Arner, D. W., and Buckley, R. P. "Decentralized Finance." *Journal of Financial Regulation* 6, no. 2 (2020): 172-203.

Zhou, M. M., Z. Zhang, and G. P. Hancke. "Security Analysis and Evaluation of Denial of Service Attack in LoRaWan-Driven Automation." In *2024 IEEE 22nd International Conference on Industrial Informatics (INDIN)*, 1-6. IEEE, 2024.