INSEAD The Business School for the World®

Working Paper

2025/46/FIN

Blockchain Compliance: A Framework for Evaluating Regulatory Approaches

Ben Charoenwong
INSEAD, ben.charoenwong@insead.edu
Corresponding author

Pratik Soni
University of Utah, psoni@cs.utah.edu

Varun Shankar
University of Utah, shankar@cs.utah.edu

Robert M. Kirby
University of Utah, mike.kirby@utah.edu

Jonathan Reiter
ChainArgos, jonathan@chainargos.com

This article provides a systematic framework for evaluating blockchain regulatory approaches, bridging technical, economic, and legal analysis. Traditional financial oversight operates through intermediaries like banks and exchanges that implement compliance programs under regulatory supervision. Blockchain systems eliminate these gatekeepers, creating fundamental mismatches between regulatory design and technological reality. Traditional regulatory frameworks encounter three fundamental limitations in decentralized contexts: jurisdictional constraints, absence of intermediaries, and technical surveillance limits. We develop a novel taxonomy categorizing five compliance approaches across multiple dimensions and provide a technical evaluation of cryptographic mechanisms, including zero-knowledge proofs. Our analysis demonstrates that hybrid regulatory frameworks, combining automated ex ante compliance with appropriate human oversight, achieve more balanced outcomes than singular approaches. This framework provides practical guidance for regulators and technologists while identifying key legal questions requiring further scholarship. Our contribution lies in creating structured tools for evaluating regulatory trade-offs across technical feasibility, regulatory effectiveness, and economic efficiency.

JEL Classification: K23, K24, G28, O33, O38
Keywords: Blockchain Regulation; Regulatory Compliance; Decentralized Finance; Cryptographic Privacy; Financial Technology; Hybrid Regulatory Frameworks; Automated Compliance; Smart Contracts; Zero-Knowledge Proofs.
History: Current Draft: October 2025 ; First Draft: March 2025

We thank Yusang He for excellent research assistance. Anthropic Claude Sonnet 3.7 and 4 was used for copy-editing and LATEXand BiBTeX formatting, and Grammarly was used for copy-editing. Word count: 14,048 words (text, headers, and references).

Blockchain Compliance: A Framework for Evaluating Regulatory Approaches

Ben Charoenwong*, Pratik Soni, Varun Shankar, Robert M. Kirby, Jonathan Reiter

Current Draft: October 2025
First Draft: March 2025

Abstract

This article provides a systematic framework for evaluating blockchain regulatory approaches, bridging technical, economic, and legal analysis. Traditional financial oversight operates through intermediaries like banks and exchanges that implement compliance programs under regulatory supervision. Blockchain systems eliminate these gatekeepers, creating fundamental mismatches between regulatory design and technological reality. Traditional regulatory frameworks encounter three fundamental limitations in decentralized contexts: jurisdictional constraints, absence of intermediaries, and technical surveillance limits. We develop a novel taxonomy categorizing five compliance approaches across multiple dimensions and provide a technical evaluation of cryptographic mechanisms, including zero-knowledge proofs. Our analysis demonstrates that hybrid regulatory frameworks, combining automated *ex ante* compliance with appropriate human oversight, achieve more balanced outcomes than singular approaches. This framework provides practical guidance for regulators and technologists while identifying key legal questions requiring further scholarship. Our contribution lies in creating structured tools for evaluating regulatory trade-offs across technical feasibility, regulatory effectiveness, and economic efficiency.

JEL Classification: K23, K24, G28, O33, O38
Keywords: Blockchain Regulation; Regulatory Compliance; Decentralized Finance; Cryptographic Privacy; Financial Technology; Hybrid Regulatory Frameworks; Automated Compliance; Smart Contracts; Zero-Knowledge Proofs.

*Ben Charoenwong (Corresponding Author), Email: ben.charoenwong@insead.edu, INSEAD, Asia Campus, 1 Ayer Rajah Ave #621, Singapore 138676. Pratik Soni, Email: psoni@cs.utah.edu, Kahlert School of Computing, University of Utah, Salt Lake City, United States. Varun Shankar, Email: shankar@cs.utah.edu , Kahlert School of Computing and Stena Center for Financial Technology, University of Utah, Salt Lake City, United States. Robert M. Kirby, Email: mike.kirby@utah.edu, Kahlert School of Computing, University of Utah, Salt Lake City, United States. Jon Reiter, Email: jonathan@chainargos.com , ChainArgos, Singapore, Singapore. We thank Yusang He for excellent research assistance. Anthropic Claude Sonnet 3.7 and 4 was used for copy-editing and LaTeXand BiBTeX formatting, and Grammarly was used for copy-editing. Word count: 14,048 words (text, headers, and references).

1 Introduction

The emergence of blockchain technology and decentralized finance (DeFi) presents distinctive regulatory challenges that existing financial regulatory frameworks struggle to address effectively. Traditional financial oversight primarily operates through intermediaries like banks, exchanges, and payment processors that implement compliance programs under regulatory supervision. Blockchain systems eliminate these gatekeepers, creating networks that often lack clearly defined accountable entities, thereby creating a fundamental mismatch between regulatory design and technological reality. This paper examines this tension and proposes that thoughtfully designed hybrid regulatory approaches—combining elements of automated *ex ante* compliance mechanisms with selective human oversight—may offer more balanced and effective paths forward for blockchain regulation than singular approaches applied in isolation.

Our central thesis is that hybrid regulatory frameworks that integrate technical mechanisms with appropriate legal safeguards and governance structures can achieve more balanced outcomes than pure implementations of any single oversight model. These hybrid approaches can leverage automated compliance for well-defined, stable regulatory requirements. At the same time, they maintain necessary human oversight for complex, context-dependent judgments that require interpretive flexibility. Importantly, designing these approaches to operate within constitutional and administrative law boundaries, as interpreted by courts and legal scholars, is essential to their legitimacy and effectiveness.

Blockchain systems exist on a spectrum of transparency and privacy, ranging from public ledgers that enable unprecedented visibility into financial flows to privacy-focused protocols that intentionally obscure transaction details. This technical diversity—combined with the global, borderless nature of blockchain networks—renders traditional jurisdiction-based regulatory frameworks increasingly strained. Current regulatory responses have often struggled to navigate this complexity effectively, either hindering innovation through broadly restrictive requirements or creating regulatory gaps through frameworks that cannot adequately adapt to decentralized architectures.

We employ an interdisciplinary methodology that bridges technical cryptography, regulatory theory, and legal doctrine. Our analysis focuses on U.S. constitutional and administrative law frameworks with comparative analysis of approaches in the European Union, Singapore, and other key jurisdictions. The nature of the challenge itself necessitates this interdisciplinary approach: effective blockchain regulation requires expertise across domains that have traditionally operated in isolation from one another.

By analyzing blockchain compliance through these complementary lenses, we identify potential solutions that may satisfy technical requirements while remaining within constitutional boundaries and respecting principles of due process, privacy, and appropriate delegation of authority. Our contribution lies in developing an integrated analytical framework that systematically maps technical design choices to their legal and regulatory implications, a perspective that requires combining

technical, economic, and legal analysis in ways that single-discipline approaches cannot achieve.

Rather than resolving contested legal questions, we provide structured tools for evaluating tradeoffs across constitutional compatibility, technical feasibility, and economic efficiency. This framework enables legal scholars, policymakers, and technologists to identify which technical approaches merit deeper legal analysis and where legal doctrine may need to evolve to address novel technological capabilities.

This paper examines both the technical feasibility and legal implications of embedding compliance directly into blockchain protocols and applications. Our taxonomic analysis (Section 3) demonstrates that no single regulatory approach adequately addresses all dimensions of the blockchain compliance challenge, with each approach offering distinct advantages while facing significant limitations when applied in isolation.

Automated compliance approaches face three categories of challenges. First, governance challenges: embedding compliance into protocols requires mechanisms for updating requirements as regulations evolve, a non-trivial design challenge given blockchain's immutability (Azgad-Tromer et al., 2023b). Second, due process concerns: fully automated enforcement without human oversight may raise constitutional issues, as illustrated by *State v. Loomis, 881 N.W.2d 749 (Wis. 2016)*, where courts held algorithmic tools should inform rather than determine outcomes. Third, technical constraints: cryptographic techniques impose substantial computational overhead (Goldwasser et al., 1989). These limitations, examined in detail in Sections 2 and 4, motivate our focus on hybrid approaches combining automated mechanisms with appropriate human oversight.

This paper makes three contributions to the emerging literature on blockchain regulation. First, we develop a novel taxonomy (Section 3) that systematically categorizes five blockchain compliance approaches across multiple dimensions including cost structure, timing, decision authority, and system resilience. The taxonomy addresses a significant gap in existing literature, which has approached blockchain regulation from either purely legal (Zetzsche et al., 2020; Alkadri, 2018) or technical (Buterin et al., 2024; Beal and Fisch, 2023) perspectives without sufficient integration. Second, we provide an evaluative framework (Section 4) for assessing automated compliance solutions across technical effectiveness, regulatory compatibility, and economic considerations, offering structured analytical tools for policymakers, legal scholars, and technologists. Third, we apply this framework to identify hybrid regulatory approaches (Section 5) that warrant further legal and policy analysis regarding their potential to balance innovation with legitimate regulatory objectives.

This interdisciplinary analysis proceeds systematically from legal foundations through technical mechanisms to practical implementation. Sections 2-3 establish how traditional financial regulation encounters fundamental limitations in blockchain contexts and develop a taxonomic framework for evaluating alternative approaches. Section 4 examines three cryptographic tools: zero-knowledge proofs, threshold encryption, and compliance oracles. These tools enable novel regulatory architectures. Legal practitioners will find essential precedential analysis in Sections 2-3, while technologists

and compliance professionals require the integrated technical-legal framework spanning Sections 3-4. Section 5 synthesizes these perspectives into concrete hybrid regulatory proposals, including addressing constitutional constraints and implementation pathways, and Section 6 concludes and provides an overview of future research.

While our analysis engages with relevant legal precedents, we acknowledge important gaps in administrative law scholarship on algorithmic governance. Recent work by legal scholars on administrative procedure and algorithmic accountability (Calo and Citron, 2021; Citron, 2008; Coglianese and Lehr, 2017) offers deeper doctrinal analysis than we provide here. Our framework is designed to complement rather than substitute for such scholarship, identifying where technical capabilities and constraints create novel questions for administrative law doctrine to address.

2 Background: Traditional Financial Regulation and Blockchain Systems

Traditional financial regulatory frameworks must be understood before evaluating novel blockchain compliance approaches. This section examines how traditional regulation functions, its application to blockchain systems, and its fundamental limitations in decentralized contexts. This legal environment constrains both enforcement mechanisms and cost allocation across the compliance frameworks enumerated in Table 1. Figure 1 illustrates how these five regulatory approaches create different oversight pathways. Traditional approaches operate through financial institution intermediaries. In contrast, blockchain-native approaches can bypass intermediaries entirely, creating direct regulator-participant relationships. This architectural shift underlies many of the economic and technical trade-offs we analyze.

2.1 Centralized Regulation

Under centralized regulation, government agencies directly monitor and enforce rules through inspections and reporting requirements. Centralized regulation offers significant advantages in terms of regulatory flexibility, as agencies can adapt requirements quickly as technologies and markets evolve without requiring consensus from multiple stakeholders (Hughes and Middlebrook, 2016). Agencies can also leverage existing legal frameworks and regulatory expertise, reducing implementation costs relative to entirely novel approaches.

Table 1: Economic and Technical Analysis of Regulatory Frameworks for Blockchain Systems

Dimensions	**Centralized Regulation**	**Gatekeeper Regulation**	**RegTech**	***Ex Ante* Automated DeFi**	**Ex Post DeFi**
Economic Cost Structure					
Fixed Costs	Moderate (agency establishment)	Moderate (framework creation)	High (technology development)	Very High (protocol design, verification)	Very High (tech & regulatory apparatus)
Variable Costs	High (case-by-case assessment)	Moderate (supervisory oversight)	Low (automated monitoring)	Very Low (computational costs)	High (enforcement actions)
Marginal Cost Pattern	Convex (increases with complexity)	Linear (scales with intermediaries)	Sublinear (economies of scale)	Sublinear for oversight; Linear for computation	Convex (increases with scale)
Cost Bearer	Regulator & Regulated Entities	Primarily Regulated Entities	Initially Regulator, then Regulated Entities	Protocol Developers & Users	Protocol Developers & Regulator
Enforcement Mechanism					
Timing	Ex Post	Mixed	Ex Post with real-time monitoring	*Ex Ante* (preventive)	Ex Post
Decision Authority	Human Judgment	Human Judgment	Algorithmic with Human Oversight	Algorithmic	Human Judgment
System Resilience	Single point of failure (regulatory authority)	Multiple potential failures (intermediaries)	Technology infrastructure failures	Smart contract vulnerabilities; Oracle dependencies	Multiple (technical & regulatory)

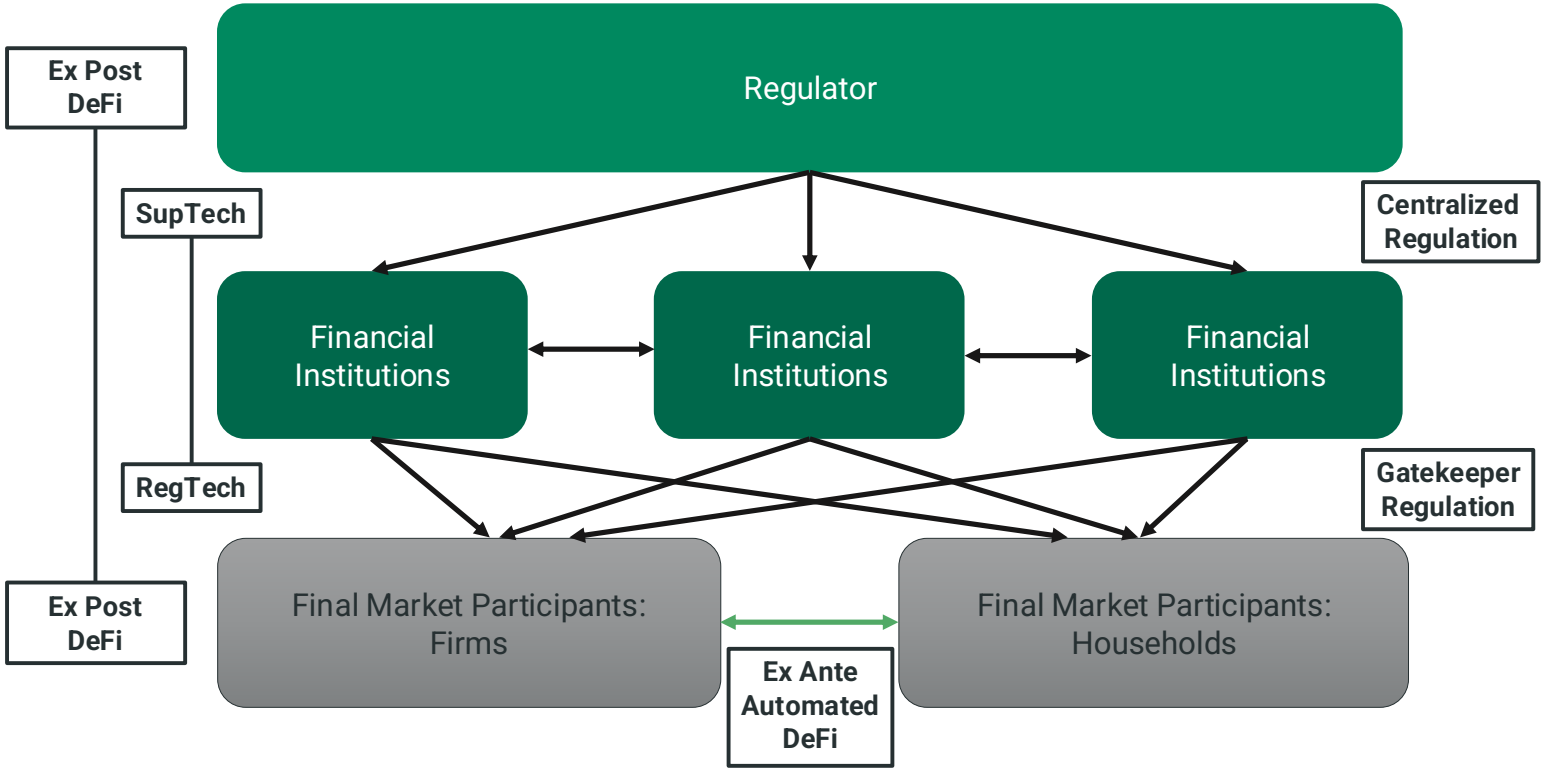

Figure 1: Regulatory approaches across market participants

New York's BitLicense exemplifies centralized regulation applied to blockchain systems.[1] This comprehensive licensing regime requires virtual currency businesses operating in New York to maintain capital reserves, implement cybersecurity programs, and conduct transaction monitoring. While providing regulatory clarity, the regime has faced legal and practical challenges, including litigation questioning its statutory basis in *Chino v. N.Y. Dep't of Fin. Servs.*,[2] where the court ultimately upheld the NYDFS's authority.

The BitLicense implementation illustrates regulatory arbitrage, where regulated entities strategically relocate to jurisdictions with more favorable treatment.[3] This forum shopping demonstrates how territorial regulations applied to inherently global technologies may inadvertently incentivize jurisdiction-shopping without necessarily achieving regulatory objectives.

Judicial Development of Securities and Commodities Law Applications

Courts increasingly define the scope of centralized regulation through the interpretation of existing securities and commodities laws. The most significant precedent emerged in *SEC v. Ripple Labs*, where the court distinguished between tokens sold as investment contracts, falling under securities laws, and those used for other purposes.[4] The court's analysis focused on the economic realities of token sales rather than technical characteristics, emphasizing that regulatory status depends on the circumstances of offer, sale, and reasonable expectations of purchasers rather than technology alone. Similarly, in *Commodity Futures Trading Commission v. McDonnell*, the court affirmed the CFTC's jurisdiction over virtual currencies as commodities under the Commodity Exchange Act, establishing a parallel regulatory track alongside securities law.[5] These judicial interpretations

[1] N.Y. Comp. Codes R. & Regs. tit. 23, § 200 *et seq.* (2015), promulgated under authority of N.Y. Financial Services Law § 102. The licensing regime requires companies handling virtual currency to obtain comprehensive licenses, maintain capital reserves, implement cybersecurity programs, and submit regular reports. See generally Brito et al. (2014).

[2] *Chino v. N.Y. Dep't of Fin. Servs.*, 2017 N.Y. Slip Op. 31908(U) (N.Y. Sup. Ct. 2017). The court rejected constitutional challenges and upheld NYDFS authority to promulgate the BitLicense regulations under state financial services law, finding that the agency acted within its statutory mandate to regulate money transmission activities.

[3] Attorney General James Proposes Nation-Leading Regulations on Cryptocurrency Industry, N.Y. State Attorney General (May 5, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-proposes-nation-leading-regulations-cryptocurrency. Accessed August 2025.

[4] *SEC v. Ripple Labs, Inc.*, No. 20-cv-10832 (S.D.N.Y. July 13, 2023). Judge Analisa Torres applied the *Howey* test, holding that "XRP, as a digital token, is not in and of itself a 'contract, transaction, or scheme' that embodies the Howey requirements of an investment contract." The court distinguished three categories of transactions: (1) Institutional Sales to sophisticated investors under written contracts constituted securities because purchasers reasonably expected Ripple to use proceeds to develop XRP functionality; (2) Programmatic Sales on exchanges were not securities because buyers could not identify Ripple as the seller and thus had no expectation of profits from Ripple's efforts; (3) Other Distributions as compensation did not involve investment of money. The decision challenges the SEC's position that digital assets are inherently securities, requiring instead a transaction-specific analysis under *Howey*. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

[5] *Commodity Futures Trading Comm'n v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018). The court reasoned that "virtual currencies can be regulated by CFTC as a commodity" despite not being physical commodities because they function as "a store of value" and "a medium of exchange." This establishes dual regulatory jurisdiction with the SEC, creating potential conflicts where the same digital asset might be considered both a security (under *Howey*) and a commodity (under the CEA), depending on the specific transaction context and regulatory theory applied.

highlight the fragmented nature of current regulatory approaches and reinforce the need for more coherent frameworks acknowledging blockchain-based assets' unique characteristics.

2.2 Gatekeeper Regulation

Beyond direct governmental oversight, regulatory frameworks often delegate enforcement responsibilities to private intermediaries. The dominant paradigm in financial regulation delegates regulatory responsibilities to private entities like banks and broker-dealers. These institutions implement their own compliance systems while remaining under regulatory supervision. Gatekeeper regulation offers several advantages over direct centralized regulation. Distributing compliance responsibilities across the industry achieves greater coverage without proportional increases in regulatory resources (Gilad, 2010). It also allows for specialization, with regulated entities developing compliance expertise specific to their business models and customer bases.

However, this approach introduces principal-agent problems. When compliance costs are borne by private entities while benefits accrue largely to the public, misaligned incentives may lead to minimal compliance rather than robust implementation (Jackson, 2007). This dynamic requires careful calibration of enforcement mechanisms and penalties to maintain effectiveness.

The Financial Action Task Force's "Travel Rule" exemplifies gatekeeper regulation in blockchain contexts.[6] This framework requires virtual asset service providers (VASPs) to exchange customer information when transferring virtual assets, mirroring requirements long imposed on traditional financial institutions under BSA/AML regulations.

Implementation has spurred industry collaboration through initiatives like the Travel Rule Information Sharing Alliance (TRISA) and the OpenVASP protocol (Greenberg and Goldstein, 2020). However, unlike traditional wire transfers that occur through a limited number of regulated financial institutions, individuals can initiate cryptocurrency transactions using non-custodial wallets, creating fundamental challenges for traditional 'gatekeeper regulatory models. The Travel Rule illustrates both the potential and limitations of this delegated enforcement approach. While effectively leveraging existing compliance infrastructures at centralized exchanges, the framework struggles to address transfers involving non-custodial wallets outside the regulated perimeter (Pavlidis, 2023).

[6] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021). The rule requires virtual asset service providers to collect and transmit customer information for transfers exceeding certain thresholds, mirroring requirements for traditional wire transfers under the Bank Secrecy Act. U.S. implementation derives from 31 C.F.R. § 1010.410(f) and FinCEN Guidance FIN-2019-G001, which extends existing suspicious activity reporting and customer due diligence requirements to virtual currency transmittals. See Financial Action Task Force (2019).

Decentralized Autonomous Organization Liability

Courts consistently find that collective schemes to manage software can qualify as traditional partnerships even if management occurs through blockchain and participants did not intend to create partnership-like arrangements. In *CFTC v. Ooki DAO*, the Commission argued that DAO governance token holders could be held jointly and severally liable under federal commodities law.[7] This novel approach suggests that participation in governance decisions may create regulatory liability even in decentralized contexts, with significant implications for compliance system design and governance.

Both *Houghton v. Leshner* and *Samuels v. Lido DAO* are civil class actions with claims made against DAOs and their alleged members for damages suffered by tokenholders.[8] While not regulatory actions, both cases pivoted on questions of membership and liability in DAO contexts, and both found that claims against some purported members could proceed. This establishes that investment in, and participation in governance of, a DAO can plausibly create legal liability at least sometimes.

These precedents suggest that geographically disparate pseudonymous groups are already "deputized" in the sense described above, whether or not participants want, expect, or even know this to be the case. Supervising financial institutions that explicitly opt into regulatory regimes fundamentally differs from relying on gatekeepers that do not want, and may actively resist, directives from regulatory authorities.

2.3 RegTech

While centralized regulation and gatekeeper regulation rely on human judgment for compliance decisions, regulatory technology introduces algorithmic monitoring and analysis. Regulatory technology and supervisory technology automate monitoring and reporting within existing financial

[7] *CFTC v. Ooki DAO*, No. 3:22-cv-5416 (N.D. Cal. June 8, 2023). Judge William H. Orrick granted a default judgment, holding that Ooki DAO constituted an "unincorporated association" under the Commodity Exchange Act and California law. The court found that the DAO violated the CEA by: (1) conducting unlawful off-exchange leveraged commodity transactions; (2) operating as an unregistered futures commission merchant; and (3) failing to implement required anti-money laundering procedures. Critically, the court established that DAOs can be "persons" under federal law and that governance token holders may face joint and several liability for DAO violations. The decision imposed a $643,542 penalty and ordered shutdown of the platform, establishing that a decentralized structure does not immunize participants from regulatory liability. The CFTC emphasized that "founders created the Ooki DAO with an evasive purpose, and with the explicit goal of operating an illegal trading platform without legal accountability."

[8] *Houghton v. Leshner*, No. 3:22-cv-07781 (N.D. Cal. filed Dec. 8, 2022) (class action against Compound DAO and its members alleging that governance token holders form a general partnership liable for protocol decisions); *Samuels v. Lido DAO*, No. 23-cv-06492-VC (N.D. Cal. decided Nov. 18, 2024) (holding that claims against DAO members could proceed where plaintiffs sufficiently alleged that governance participants formed a general partnership under state law). Both courts found that DAOs lacking formal corporate structure may constitute general partnerships under state law, exposing governance token holders to joint and several liability for partnership debts and obligations. The decisions establish that investment in, and governance participation of, decentralized protocols can create traditional partnership liability regardless of participants' intent or awareness.

infrastructure. Transaction monitoring systems exemplify this approach, using algorithms to flag suspicious activities for review. RegTech focuses on post-transaction detection and reporting, offering substantial advantages in cost-effectiveness and adaptability. By automating routine compliance tasks and enhancing human analyst capabilities, these solutions significantly reduce enforcement costs while improving effectiveness (Treleaven, 2017). They can also adapt relatively quickly to emerging threats and regulatory changes without requiring consensus from multiple stakeholders.

Blockchain analytics platforms like Chainalysis, Dune, Elliptic, and TRM Labs represent prominent examples of RegTech solutions for blockchain compliance (Gerard, 2017). These tools leverage public blockchain transparency to identify suspicious transaction patterns, map wallet relationships, and assess counterparty risk (Mohanta et al., 2019). Their legal status received important clarification in *United States v. Gratkowski*, where the Fifth Circuit held that government agencies' use of blockchain analytics to trace Bitcoin transactions did not constitute a search requiring a warrant under the Fourth Amendment, distinguishing blockchain data from the cell phone records protected in *Carpenter v. United States*.[9]

However, blockchain analytics face significant limitations when applied to privacy-enhancing technologies. As Kappos et al. (2018) demonstrate in their analysis of Zcash's shielded transactions, privacy-focused cryptocurrencies can render traditional analytics approaches ineffective. Tools like Tornado Cash and other mixing services present substantial challenges for transaction tracing (Guillen et al., 2023), highlighting tensions between traditional regulatory approaches and privacy-preserving technologies.

Fourth Amendment Constraints on Blockchain Surveillance

The *Gratkowski* decision offers one judicial perspective on RegTech approaches while raising questions about privacy expectations in blockchain systems. The Fifth Circuit's reasoning that Bitcoin users voluntarily disclose information to all network participants potentially expands government surveillance capabilities, though how broadly this reasoning applies across different blockchain contexts remains uncertain. The court's distinction from *Carpenter* suggests that different types of blockchain data might receive varying levels of Fourth Amendment protection, though the precise contours of these distinctions require further judicial development and legal scholarship.

This evolving jurisprudence creates legal uncertainty for blockchain surveillance. Outcomes depend on the type of blockchain system involved (public versus private, pseudonymous versus anonymous), the comprehensiveness of analysis performed, the nature of information revealed, and

[9] *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020). The court applied the third-party doctrine, holding that Bitcoin users voluntarily disclose transaction information to the global Bitcoin network and exchanges like Coinbase, thereby eliminating any reasonable expectation of privacy. The court distinguished *Carpenter v. United States*, 138 S. Ct. 2206 (2018), finding that Bitcoin blockchain records are more analogous to bank records than to the comprehensive, intimate cell phone location data protected in *Carpenter*. The decision establishes that blockchain analytics tools can be used without warrants for tracing cryptocurrency flows, significantly expanding government surveillance capabilities over digital asset transactions.

investigative techniques used to link blockchain activities to real-world identities. For regulatory compliance systems relying on government monitoring, this suggests the value of warrant procedures for more intrusive analyses, even when basic blockchain information may be accessible without such protection.

2.4 Automated *Ex Ante* Compliance

The surveillance limitations identified above, combined with privacy-enhancing technologies that defeat monitoring, motivate a fundamentally different approach: preventing non-compliant transactions rather than detecting them after the fact. While not prevalent in traditional finance, automated compliance approaches represent an emerging paradigm enabled by blockchain technology. Smart contracts are self-executing agreements with terms directly written into code that automatically enforce compliance rules without human intervention. These approaches embed regulatory requirements directly into blockchain protocols or smart contracts, preventing non-compliant transactions through *ex ante* design (Schrepel, 2021). This approach shifts from post-facto detection and punishment to preventive design, fundamentally altering the relationship between regulation and regulated activities. As Azgad-Tromer et al. (2023a) note, embedded compliance "shifts the regulatory paradigm from retrospective enforcement to preemptive assurance, enabling compliance by design rather than through after-the-fact sanctions."

Recent developments in privacy-preserving compliance mechanisms demonstrate this approach's potential. Privacy Pools, as described by Buterin et al. (2024), enable users to demonstrate compliance with specific regulatory requirements without compromising overall transaction privacy. By allowing users to prove that their funds originate from non-sanctioned sources without revealing their complete transaction history, these protocols create a "separating equilibrium" between compliant and non-compliant uses. However, the legal status of such mechanisms has not been definitively resolved, as they have not yet been tested in court or explicitly addressed by regulatory guidance.

Regulatory Authority Over Blockchain Code and Protocols

The extent to which regulators can directly control blockchain code and protocols remains contested, creating uncertainty for compliance system design. The Tornado Cash sanctions case provides the most prominent example of these contested boundaries. In August 2022, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash smart contracts, including specific Ethereum addresses containing immutable code.[10] Acting under authority granted by the International Emergency Economic Powers Act (IEEPA), OFAC took the unprecedented step of designating smart contract addresses as Specially Designated Nationals, effectively prohibiting U.S. persons from interacting with the associated code.

[10] U.S. Treasury Dep't, Office of Foreign Assets Control, *Tornado Cash Designation* (Aug. 8, 2022).

This action faced legal challenge in *Van Loon v. Department of the Treasury*, raising novel questions about regulatory authority over code itself, including whether code constitutes "property" under IEEPA and whether such restrictions implicate First, Fourth, or Fifth Amendment protections regarding free expression, search warrant procedures, and due process requirements respectively.[11] The Fifth Circuit found that OFAC lacked authority to sanction Tornado Cash as it existed at the time of sanctioning because technical features, namely that the code had no owner and could no longer be modified, rendered it outside the scope of OFAC's sanctioning power. How broadly this reasoning applies to other automated compliance systems and regulatory approaches remains an open question for courts and legal scholars.

However, in *United States v. Storm*, a developer of the system was convicted after a jury trial of concerning activities related to developing, deploying, and maintaining Tornado Cash.[12] Around the same time, in *United States v. Rodriguez*, the operator-developers of Samourai Wallet pled guilty to the same conspiracy charge in similar circumstances. [13] These cases demonstrate the legal uncertainty and complexity surrounding regulatory approaches to privacy-preserving blockchain technologies and the need for more nuanced frameworks.

Heterogeneity of Frameworks

This uncertainty and complexity extend beyond just privacy-related technologies. Consider a project where the holders of some collection of tokens vote on governance decisions that have achieved compliance in a given jurisdiction. That jurisdiction might, for example, impose requirements on certain named parties or anyone holding over some fixed percentage of voting power. How

[11] *Van Loon v. Dep't of the Treasury*, No. 23-50669 (5th Cir. Nov. 26, 2024). The Fifth Circuit reversed the district court, holding that OFAC exceeded its statutory authority by sanctioning Tornado Cash's immutable smart contracts. The court reasoned that "property" under IEEPA must be capable of ownership, control, or exclusion, which immutable smart contracts lack because they are "self-executing and cannot be altered or controlled, even by their creators." Applying *Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244 (2024), the court rejected agency deference and applied plain meaning interpretation. The decision noted that "[p]erhaps Congress will update IEEPA, enacted during the Carter Administration, to target modern technologies like crypto-mixing software," but declined to expand executive authority through judicial interpretation. The Treasury Department subsequently removed Tornado Cash sanctions on March 21, 2025, citing the court's ruling.

[12] *United States v. Storm*, No. 1:23-cr-00430 (S.D.N.Y. filed Aug. 21, 2023, decided Aug. 6, 2025). Roman Storm, co-founder of Tornado Cash, was convicted of conspiracy to operate an unlicensed money transmitting business, while the jury deadlocked on charges of conspiracy to commit money laundering and conspiracy to violate the International Emergency Economic Powers Act. The case focused on allegations that Tornado Cash facilitated over $1 billion in money laundering, including funds from the North Korean Lazarus Group. The partial verdict demonstrates how individual developers may face criminal liability even when the underlying protocol is deemed unsanctionable, creating significant legal uncertainty for blockchain developers and highlighting the distinction between protocol sanctions and individual criminal responsibility.

[13] *US v Rodriguez*, No 124-cr-00082 (S.D.N.Y 2024). Samourai Wallet is a service broadly similar to Torando Cash. The team was initially charged with the same money transmission and money laundering conspiracy charges as Roman Storm but not sanctions violations. In pre-trial motions the defandants and government disputed the meaning and importance of "custody" as opposed to merely controlling software that processes funds and which of those actions could constitute a necessary element of the charged crimes. Ultimately the defendants pled guilty during Roman Storm's trial and before their own trial began.

does this project handle a second jurisdiction with a different threshold? Or no threshold at all? Or a jurisdiction that imposes conditions on the developers as well? There is but one governance mechanism as a technical matter, but there can be an arbitrary number of supervisory regimes.

Traditional financial regulatory compliance, generically, silos these questions within a legal entity structure that maps to legal requirements. For products without traditional legal representation,[14] and where it is not even clear within a single jurisdiction who is accountable for what, conflict of laws questions abound. However, these problems are not without precedent in the law. Imagine an unincorporated general partnership operating across two jurisdictions, where all members are jointly and severally liable for everything. Legal frameworks exist to assign liability within and across jurisdictions. These frameworks do not, of course, guarantee equivalent treatment across heterogeneous legal systems. Furthermore, all manner of intricate and complex questions can arise in even seemingly simple contexts. It is not our intention here to address any of those questions. To the extent we touch on these problems, our goal is merely to indicate where the interfaces between law and the technology under examination lie and to categorize broad classes of solutions in a way that helps clarify the questions all the practical work necessary to address them must answer.

2.5 Fundamental Limitations in Decentralized Contexts

Having described how traditional regulatory approaches function (centralized oversight, gatekeeper regulation, and RegTech solutions), we now examine why each encounters fundamental limitations when applied to blockchain systems. The regulatory approaches described above each encounter distinct but interconnected limitations when applied to blockchain systems. These limitations are not merely implementation challenges but fundamental mismatches between traditional regulatory paradigms and blockchain technology's novel characteristics.

2.5.1 Jurisdictional Constraints and Conflicts

Unlike traditional financial institutions with clear geographic ties, blockchain networks operate globally with distributed nodes across multiple jurisdictions (Alkadri, 2018). This creates significant challenges for territorial regulatory frameworks. The BitLicense case study demonstrates how such approaches create inefficiencies and opportunities for regulatory arbitrage, as service providers simply relocate to more favorable jurisdictions. Blockchain networks' global and borderless operations create significant challenges for traditional territorial regulatory frameworks (Zetzsche et al., 2020).

Courts and regulators have developed varying approaches to establishing jurisdiction over blockchain activities, creating a complex and sometimes contradictory legal landscape. The effects-

[14] For example, compare the regulatory challenges faced by decentralized autonomous organizations (DAOs), which often lack traditional corporate structures. See CFTC v. Ooki DAO, No. 3:22-cv-5416 (N.D. Cal. June 8, 2023) (treating DAO as unincorporated association); Houghton v. Leshner, No. 3:22-cv-07781 (N.D. Cal. filed Dec. 8, 2022) (alleging DAO token holders form general partnership under state law).

based jurisdiction model is exemplified by cases like *SEC v. PlexCorps*, where the court asserted U.S. jurisdiction over a Canadian ICO based on its effects on U.S. investors.[15] The node-based jurisdiction model, emerging in cases like the BitMEX prosecution, focuses on the physical location of network infrastructure. In *CFTC v. HDR Global Trading Limited*, the court upheld jurisdiction based partly on the presence of BitMEX trading servers in the U.S., despite the company's nominal offshore registration.[16]

The enterprise-engagement model, developed in cases like *SEC v. Telegram Group Inc.*, focuses on blockchain projects' entirety rather than isolated technical components.[17] Under this approach, courts evaluate jurisdiction based on the collective activities of the enterprise, including development, promotion, and ongoing operations. These varying jurisdictional approaches create significant challenges for designing compliant blockchain systems. Privacy-preserving compliance techniques potentially offer advantages by enabling jurisdiction-specific disclosure without exposing all transaction details globally.

And for products and protocols that operate simultaneously across multiple jurisdictions, there is the further problem that different systems may impose dramatically different or contradictory rules. One technology may be simultaneously regulated as a commodity trading platform in one country and a payment services provider in another. Similarly, one regulator may require fund seizures under certain circumstances incompatible with another's concept of end-user property rights. Technology is sometimes, even often, designed to be composable in a way that sovereign legal systems are not. A "court of final appeal" exists to dispense a finality that may not apply here.

The introduction of globally active networks can expose this conflict in novel ways. Imagine a product built and maintained by an identifiable legal entity that achieves compliance in one jurisdiction. This is a common situation where a company develops a product with a token and releases that token on a decentralized network. Now, the development company wishes to achieve compliance with different requirements in a second jurisdiction. Then the software must be upgraded, and both regulators must approve the new version.

For a second jurisdiction, this may prove workable. However, incorporating requirements from regulator $n+1$ requires approval from the first n, noting that this is the "good" scenario when all of those rules are compatible. As the product is simultaneously active in all of these jurisdictions, we have an emergent problem akin to driving in a manner consistent with several countries' traffic laws simultaneously. Even when this is possible, it can prove exceptionally challenging.

Our framework simplifies the scope within the context of a given approach. For example, in a scenario where we rely on centralized regulation, these inter-jurisdictional conflicts must be settled among the centralized regulators. New regulators will, consequently, be forced to negotiate with

[15] *SEC v. PlexCorps*, No. 17-cv-7007 (E.D.N.Y. 2017).
[16] *CFTC v. HDR Global Trading Limited*, No. 20-cv-8132 (S.D.N.Y. filed Oct. 1, 2020).
[17] *SEC v. Telegram Group Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020).

the incumbents if they wish to enact novel rules. Alternatively, for an ex ante automated system to achieve global scale, it must be designed to accommodate rule sets as heterogeneous as the world's financial regulatory regimes. As it is unlikely a short and simple block of immutable code can achieve that for anything but the most trivial of requirements, designers must be aware of the scale of these conflicts when scoping their products.

2.5.2 Absence of Clearly Defined Intermediaries

Traditional regulatory frameworks rely heavily on identifiable entities, such as banks, broker-dealers, and exchanges, who can be held accountable for compliance failures. However, as Walch (2019) notes, truly decentralized protocols may lack any single entity with both the authority and capability to implement compliance programs. The Travel Rule implementation illustrates this limitation, as it struggles to address transfers involving non-custodial wallets outside the regulated perimeter.

The possibility of removing intermediaries also introduces a new type of misrepresentation: false claims that software is not an intermediary. This resembles determining what constitutes money transmission but focuses more heavily on analyzing technology rather than traditional financial transactions. Existing frameworks consider the facts and circumstances of bank and cash transfers,[18] hawala,[19] and various other value transfer methods.[20] But historically, none required determining to what extent a software system's developer or operator exercises control over funds by analyzing that system's code.

Nonetheless, practical cryptocurrency implementation and adoption through exchanges permit the same intermediary/deputized approach. Although existing exchanges, including both those acknowledging operation as intermediaries and those rejecting the premise, appear to want to shun that responsibility due to additional compliance burdens.

2.5.3 Technical Limitations of Transparency

While public blockchains offer unprecedented visibility into transaction flows, privacy-enhancing technologies can render traditional surveillance approaches ineffective. The OFAC sanctions against Tornado Cash starkly illustrate the limitations of post-facto monitoring approaches when confronted with privacy-preserving technologies.

The Tornado Cash case also demonstrates the limits of traditional record-keeping requirements. Even if that system had a central operator, the operator could not de-anonymize withdrawals. The system's design ensures that records pairing deposits and withdrawals cannot be reconstructed from information in the system. Tension exists in insisting on a controlling intermediary that cannot produce useful records, serving little purpose beyond perhaps punishing that intermediary

[18] *United States v. Velastegui*, No. 99-1362 (S.D.N.Y. June 8, 1999).
[19] *United States v. Banki*, No. S1 10 Cr. 08 (JFK) (S.D.N.Y. July 30, 2010).
[20] *United States v. Bah*, No. 07-4370-cr (S.D.N.Y. July 31, 2009).

for running the system in the first place.

If such an approach effectively banned the design, it might serve a purpose. However, since it is possible to build working intermediary-free versions, banning certain forms of anonymizers while allowing other equally effective variants would seem to be an odd public policy.

This tension generalizes. A regulatory system in which every decision involves public dissemination of all the details of everyone and every related act would be radically more transparent than any current system. In practice, transparency must mean something less than that. And we know it is possible to develop systems that make and publish provably-correct judgements without also publishing all the information required to reach those judgements using cryptographic techniques like interactive ZKPs Goldwasser et al. (1989).

But there are limitations. Automated prover systems can only prove statements expressible in code. This brings in more than computational limits akin to Turing Charoenwong et al. (2025). Automated systems can only automate the enforcement of sufficiently precise laws that can be reduced to mathematical statements.

Crootof and Ard (2021) describe this problem as "the fundamental challenge of techlaw is not how to best regulate novel technologies, but rather how to best address familiar forms of legal uncertainty in new sociolegal contexts." Such legal uncertainty exists, necessitating systems that are less stiff than formal mathematics. When facing a rule that a computer cannot reliably evaluate, a designer must choose between an unreliable implementation and reliance on non-automated mechanisms. Threshold cryptography schemes can ensure non-automated decision-making authority is sufficiently diffuse, but they cannot automate that authority. Further, many techniques offer promising solutions but impose substantial computational overhead that may affect scalability and user experience.

This integrated analysis of regulatory frameworks and judicial developments reveals that traditional binary classifications (public versus private enforcement, rules versus standards) prove insufficient for blockchain contexts. The courts' varied approaches to jurisdiction (PlexCorps, BitMEX), liability allocation (Ooki DAO, Lido DAO), surveillance boundaries (Gratkowski), and code regulation (Van Loon, Storm) demonstrate this insufficiency, creating a fragmented landscape requiring more nuanced taxonomic frameworks. Recent scholarship has similarly emphasized that blockchain regulation requires novel frameworks rather than simple extensions of existing approaches (Azgad-Tromer et al., 2023b; Burleson et al., 2022).

Having established the fundamental limitations of traditional regulatory frameworks (jurisdictional constraints, absence of intermediaries, and technical limitations of surveillance), we now develop such a framework. Section 3 provides a taxonomy for comparing five distinct regulatory strategies across multiple dimensions, enabling identification of complementarities and potential hybrid solutions.

3 A Taxonomy of Regulatory Approaches for Blockchain Systems

Developing effective regulatory frameworks for blockchain systems requires systematically understanding various approaches and their relative strengths and weaknesses. Traditional financial regulation has evolved over decades through trial and error, with limited need to consider fundamental design choices across multiple dimensions simultaneously. In contrast, blockchain technology presents a rare opportunity and challenge to reconsider the regulatory architecture from first principles (Zetzsche et al., 2020).

Our taxonomy provides a structured framework for evaluating five regulatory approaches across multiple dimensions including cost structure, timing, decision authority, and system resilience. By systematically comparing these approaches, we can identify complementarities, trade-offs, and potential hybrid solutions that may offer superior outcomes to any single paradigm. Table 1 summarizes this analysis from economic and technical perspectives.

3.1 Centralized Regulation: Government Takes Direct Control

Government agencies directly monitor blockchain activities and enforce rules through traditional legal mechanisms. Agencies write rules, investigate violations, and impose penalties. This approach mirrors traditional financial regulation, where agencies like the SEC or CFTC directly oversee market participants (Hughes and Middlebrook, 2016).

Centralized regulation offers significant advantages in regulatory flexibility. Agencies can adapt requirements quickly as technologies evolve without requiring consensus from multiple stakeholders. They can leverage existing legal frameworks and regulatory expertise, reducing implementation costs relative to entirely novel approaches.

However, the economic structure creates escalating challenges. Implementation involves the government bearing moderate setup costs but facing escalating expenses as blockchain adoption grows. Each new cryptocurrency or DeFi protocol requires separate analysis. Companies face compliance costs, including legal fees, reporting systems, and ongoing regulatory relationships. The cost pattern becomes convex, with expenses increasing disproportionately as system complexity grows. Centralized regulation faces fundamental scalability limitations. Blockchain networks' global, borderless nature makes territorial regulatory frameworks increasingly strained. Enforcement becomes challenging across multiple legal systems, creating regulatory arbitrage opportunities that undermine effectiveness.[21]

New York's BitLicense exemplifies these trade-offs (analyzed in Section 2). While providing regulatory clarity for compliant businesses, the compliance costs drove cryptocurrency businesses

[21] Administrative law constraints may limit centralized approaches. The Administrative Procedure Act's notice-and-comment requirements for substantive rules create potential tensions with rapid technological development, though how courts will balance these considerations remains to be seen. Due process requirements may also constrain automated enforcement systems, as suggested by recent jurisprudence analyzed in Section 2, though the precise scope of these constraints in blockchain contexts requires further legal analysis.

from New York entirely.[22] This demonstrates how territorial regulations applied to inherently global technologies create economic incentives for jurisdiction shopping without necessarily achieving regulatory objectives.

3.2 Regulation through Financial Intermediaries

Government delegates enforcement responsibility to private financial intermediaries while maintaining supervisory oversight. This approach dominates traditional finance and extends to blockchain through anti-money laundering requirements (Gilad, 2010).

Gatekeeper regulation offers distinct economic advantages over centralized regulation. By distributing compliance responsibilities across the industry, this approach achieves broader coverage without proportional increases in regulatory resources. Implementation spreads costs across industry participants rather than concentrating them in government agencies. Costs scale linearly with the number of intermediaries rather than system complexity, making this approach more scalable than pure centralized regulation.

However, the cost structure creates different incentive problems. When compliance costs are borne by private entities while benefits accrue largely to the public, misaligned incentives may lead to minimal compliance rather than robust implementation (Jackson, 2007). Regulated companies must invest in compliance systems and staff, while the government maintains supervisory oversight expenses. The economic efficiency of gatekeeper regulation depends critically on the availability of suitable intermediaries. When blockchain systems eliminate traditional gatekeepers, the entire model faces structural challenges that cannot be resolved through better implementation alone.[23]

The Travel Rule implementation exemplifies this approach (detailed in Section 2). Coordination gains have spurred industry collaboration through initiatives like TRISA and OpenVASP protocols (Takei and Shudo, 2024). Major exchanges exchange customer information for large transfers, while smaller platforms struggle with implementation costs. However, as analyzed in Section 2, this creates fundamental limitations when applied to non-custodial wallets outside the regulated perimeter.

3.3 RegTech: Algorithms Watch the Blockchain

Technology enhances traditional regulation through automated monitoring and analysis. Sophisticated algorithms scan blockchain transactions for suspicious patterns while human analysts investigate flagged cases (Treleaven, 2017).

[22] See, for example, https://www.coindesk.com/markets/2015/08/13/the-real-cost-of-applying-for-a-new-york-bitlicense. Accessed August 2025

[23] The non-delegation doctrine constrains agencies' ability to outsource rulemaking functions without clear statutory authorization. See *West Virginia v. EPA*, 142 S. Ct. 2587 (2022). The DAO liability cases discussed in Section 2 further complicate this delegated enforcement model by creating involuntary regulatory responsibility for governance participants.

RegTech approaches offer substantial economic advantages through cost-effectiveness and scalability. Implementation involves high up-front costs for developing monitoring systems, but low marginal costs for analyzing additional transactions. Technology scales efficiently, with monitoring millions of transactions costing little more than monitoring thousands. The sublinear cost pattern creates substantial economies of scale. Companies typically purchase analytics services rather than building internal capabilities, while regulators leverage these tools for investigation and enforcement. This creates a viable market structure where specialized firms develop sophisticated monitoring capabilities that benefit multiple users. RegTech systems enable unprecedented visibility into financial flows at scale, with analytics companies processing billions of transactions daily.

However, the economic model faces fundamental limitations when confronted with privacy-enhancing technologies. As Kappos et al. (2018) demonstrate, privacy-focused cryptocurrencies can render traditional analytics approaches ineffective. This creates an arms race dynamic where each privacy innovation potentially undermines existing RegTech investments, requiring continuous technological adaptation.[24]

Blockchain analytics platforms like Chainalysis, Dune, Elliptic, and TRM Labs exemplify RegTech in practice (analyzed in Section 2). The legal framework for these tools was established in the *Gratkowski* decision, which held that blockchain analytics do not constitute searches requiring warrants. However, as analyzed in Section 2, this creates fundamental limitations when applied to privacy-preserving technologies like mixing services.

3.4 *Ex Ante* Automated Compliance: Rules Built Into the Code

Regulatory requirements embed directly into blockchain protocols through smart contracts and cryptographic mechanisms. Non-compliant transactions cannot occur because the underlying technology prevents them (Schrepel, 2021). This fundamentally alters the relationship between regulation and regulated activities by making violations technically impossible rather than merely detectable.

This approach offers substantial economic advantages. The economic structure reverses traditional regulatory costs: implementation requires large upfront costs for protocol development, formal verification, and security auditing, but incurs very low ongoing costs for compliance verification. Once implemented, the marginal cost of compliance verification approaches zero. The approach enables global reach without territorial limitations, consistent enforcement across all transactions, and automatic operation without regulatory staff. The elimination of human bias or corruption in compliance decisions provides additional value.

[24] Fourth Amendment constraints may limit RegTech expansion beyond current applications. While *Gratkowski* permits basic blockchain analysis, more comprehensive surveillance might trigger heightened constitutional scrutiny. Courts increasingly require transparency and appeal mechanisms for algorithmic enforcement systems.

However, the economic model faces significant governance challenges. Updating compliance requirements as regulations evolve represents a major coordination challenge. The massive upfront investment becomes economically problematic when regulatory requirements change frequently, potentially requiring substantial system modifications or complete rebuilds. Users bear minimal transaction fees while protocol developers invest heavily in initial design, creating questions about long-term sustainability.

Recent developments in privacy-preserving compliance mechanisms, such as Privacy Pools and Derecho, demonstrate technical progress in reconciling privacy with regulatory oversight (examined in Section 2). However, the legal status of such mechanisms has not been definitively resolved, as highlighted by the regulatory authority questions in the Tornado Cash cases.[25]

3.5 Ex Post DeFi: Automated Monitoring with Human Enforcement

This approach combines automated compliance technology with traditional human oversight. Sophisticated algorithms monitor blockchain activities while human regulators make final enforcement decisions. The model attempts to leverage technological capabilities for detection while maintaining human judgment for complex determinations.

This hybrid model offers some theoretical advantages. Ex post timing maintains traditional reactive enforcement while introducing algorithmic analysis capabilities. The approach preserves human judgment for enforcement decisions, allowing regulators to consider context and exercise discretion. It also enables deployment of sophisticated monitoring tools without requiring complete protocol redesigns.

However, the economic structure creates the most challenging cost profile. Implementation combines high costs for developing sophisticated technology with high costs for maintaining the human regulatory apparatus. Both technical and regulatory complexity create multiple cost centers without clear efficiency gains. This model represents essentially the worst of both worlds from a cost perspective. The distributed responsibility structure lacks clear accountability mechanisms when systems fail. Traditional regulation assigns clear accountability for failures, but hybrid ex post systems often lack such structures, devolving to loose forms of collective responsibility that undermine economic efficiency.[26]

[25] Due process concerns may significantly constrain automated compliance systems. Courts have required transparency, explanation, and appeal mechanisms for algorithmic decision-making that affects property rights in some contexts. See *State v. Loomis, 881 N.W.2d 749 (Wis. 2016)* addressing due process concerns with proprietary algorithmic risk assessment tools, and *Houston Federation of Teachers v. Houston Independent School District, No. 4:14-cv-01189 (S.D. Tex. 2017)* finding due process violations where teachers could not verify accuracy of algorithmic evaluations used for employment decisions. The *Van Loon v. Dep't of the Treasury, No. 23-50669 (5th Cir. Nov. 26, 2024)* decision further addresses limits on regulatory authority over immutable code. How these precedents apply to blockchain compliance systems requires deeper legal analysis.

[26] Administrative constraints compound the economic inefficiencies. The APA's rulemaking requirements create delays in implementing technical standards, while judicial review standards for complex algorithmic systems remain uncertain. These procedural requirements add significant costs without corresponding benefits.

The practical economic challenges become evident in responses to major incidents. Despite sophisticated monitoring tools and extensive coordination efforts involving multiple analytics firms and exchanges, significant funds regularly escape recovery in major thefts. This highlights fundamental problems with hybrid ex post systems where successful efforts receive credit while failures generate finger-pointing about responsibility. The coordination costs may exceed the benefits of combining technical and human elements.

3.6 Economic Analysis and Trade-offs

Table 1 reveals fundamental trade-offs between approaches that shape their practical viability. No single model adequately addresses all dimensions of the blockchain compliance challenge from an economic perspective.

Traditional approaches minimize upfront investment but face escalating operational costs as blockchain adoption grows. Centralized regulation requires hiring technical experts and expanding enforcement capabilities with each new application. The convex cost pattern means expenses increase disproportionately with system complexity. Gatekeeper regulation spreads costs across industry participants but scales linearly with regulated entities.

Technology-focused approaches reverse this pattern. Automated compliance requires massive initial investment but minimal ongoing operational costs. *Ex ante* systems achieve very low variable costs for compliance verification, though computational costs for cryptographic operations scale with transaction volume. The challenge involves justifying enormous upfront expenses when regulatory requirements continue evolving.

RegTech solutions occupy a middle ground with high initial development costs but sublinear scaling that creates significant economies of scale. Monitoring additional transactions becomes increasingly efficient as capabilities expand, making this approach attractive for large-scale deployment.

The timing dimension creates fundamental trade-offs between adaptability and enforceability. Ex post enforcement maintains flexibility for addressing novel situations that resist predefined categorization but struggles with blockchain's global, instantaneous nature, where harmful activities can complete before detection occurs. *Ex ante* prevention offers comprehensive coverage and consistent enforcement but faces adaptation challenges when regulatory changes require modifying underlying protocols. This represents a fundamental trade-off between adaptability and enforceability that shapes the entire regulatory architecture.

Innovation protection requires careful calibration of regulatory intensity. Heavy-handed regulation stifles beneficial innovation by imposing excessive compliance burdens, as demonstrated by BitLicense. Insufficient oversight enables harmful activities that undermine market integrity. Effective regulation must distinguish between innovations that genuinely improve financial services and those that primarily facilitate harmful activities.

These trade-offs are not mutually exclusive choices. The five approaches examined above represent distinct regulatory strategies, but in practice they need not be implemented in isolation. Centralized regulation can coexist with RegTech monitoring tools. Gatekeeper frameworks can incorporate automated compliance mechanisms. Each approach faces fundamental limitations: jurisdictional constraints for centralized models, adaptability challenges for automated systems, and privacy vulnerabilities for surveillance approaches. These limitations suggest that effective regulation may require strategic combinations rather than singular implementations.

Understanding which combinations are viable and effective requires examining the technical mechanisms that enable automated compliance. Section 4 provides this technical foundation, analyzing the cryptographic tools (zero-knowledge proofs, threshold encryption, and compliance oracles) that make certain hybrid configurations possible. This technical analysis then informs Section 5's development of specific hybrid regulatory frameworks.

4 Technical Approaches to Automated Blockchain Compliance

As discussed in Section 3, automated compliance approaches mark a shift from reactive, post-facto enforcement to proactive, preventive mechanisms, made possible through advanced cryptographic tools. As noted in Azgad-Tromer et al. (2023a), embedded compliance realizes "compliance by design," embedding enforcement into system behavior rather than relying solely on external sanctions. For legal practitioners and regulators, understanding these technical mechanisms becomes essential as they may fundamentally alter how financial regulations are implemented and enforced. This section introduces the key cryptographic primitives that enable such automated compliance and assesses their technical, regulatory, and economic tradeoffs.

4.1 Overview of Cryptography-Enabled Compliance Mechanisms

Before examining specific compliance mechanisms, it is essential to understand the cryptographic tools that enable them. Recent cryptographic advances have made it possible to reconcile the seemingly conflicting goals of transaction privacy and regulatory compliance. These tools provide the foundation for protocols that preserve confidentiality while enabling the verification of legal constraints. We discuss three such tools here: zero-knowledge proofs, threshold cryptography, and compliance oracles.

Zero-knowledge proofs (ZKPs), introduced in Goldwasser et al. (1989), stand out as one of the most powerful tools as a novel approach to the longstanding tension between regulatory oversight and privacy rights. Technically, ZKPs allow a party to prove that a transaction satisfies specific properties without revealing the transaction itself; an encrypted version of the transaction is instead revealed. From a legal perspective, ZKPs enable compliance verification without the broad information disclosure that traditionally accompanies financial regulation. In regulatory contexts,

this means a user could prove their transaction complies with anti-money laundering rules without revealing their identity, transaction amount, or counterparty, analogous to proving you are over 21 without showing your birthdate. Systems like Privacy Pools (Buterin et al., 2024), Derecho (Beal and Fisch, 2023), and zkFI Sahu et al. (2024a) use ZKPs to allow privacy-preserving transactions, where users can demonstrate compliance without disclosing full transaction histories.

While theoretically effective, ZKPs can be computationally intensive, particularly in generating proofs for complex compliance logic. However, recent advances have significantly improved performance. A wide range of ZKP protocols now exist, each offering distinct trade-offs in the proving time, proof size, verification time, and mathematical hardness assumptions that underpin security Groth (2016); Setty (2019); Ben-Sasson et al. (2018a); Bowe et al. (2019); Kothapalli et al. (2021); Gabizon et al. (2019); Chen et al. (2022); Ben-Sasson et al. (2018b); Bünz et al. (2019); Block et al. (2020, 2021). The emergence of domain-specific languages like Circom iden3 (2025) has lowered the barrier to encoding high-level regulatory predicates into efficient ZKP circuits. Meanwhile, production-grade ecosystems such as zkSync Matter Labs (2025), Polygon zkEVM Polygon Labs (2025), and RiscZero RISC Zero (2025) are enabling practical deployment of ZKP-based compliance tools. With continued research into faster proving, recursive composition, and hardware acceleration, ZKPs are rapidly maturing into a viable foundation for scalable, privacy-preserving, regulatory frameworks.

Threshold cryptography requires multiple parties to cooperate to perform cryptographic operations, similar to requiring multiple keys to open a safety deposit box, ensuring no single party has unilateral control over sensitive compliance decisions. It provides a complementary approach by enabling selective disclosure of transaction data. In systems designed per this principle, sensitive information is encrypted and can only be revealed through cooperation among trusted guardians or authorities. For instance, the SeDe protocol Sahu et al. (2024b) (designed based on guidelines outlined in Burleson et al. (2022)) uses threshold decryption to allow selective unmasking of user identities in suspected cases of abuse or fraud. This offers a middle ground: information remains private by default but becomes available under defined legal or compliance conditions.

Duffie et al. (2025) propose similar mechanisms to preserve privacy while automating simple compliance rules and falling back on threshold cryptography and a form of guardian set for not-currently-automatable rules. Such mechanisms, however, depend in the limit on the integrity of and coordination within the guardian set; this dependence naturally raises questions about resilience and trust assumptions. We discuss this tension as it relates to framing the compliance problem in Section 2.5.3 and then how it constrains hybrid solution implementations in Section 5.5.

Compliance oracles represent a third category of tools that help bridge on-chain transactions with off-chain compliance requirements. These oracles attest to real-world properties such as KYC status or sanctions screening and can certify addresses as compliant by signing digital credentials. Users can then prove possession of such credentials (*e.g.*, via ZKPs) when executing

transactions. While oracles reduce on-chain logic complexity, they introduce data accuracy, centralization, and potential manipulation concerns. Such oracle-based attestation is gaining traction with the launch of initiatives like the *Ethereum Attestation Service (EAS)* (Ethereum Attestation Service, 2023), which provides a public infrastructure for issuing and verifying attestations using standardized schemas. By combining oracles with verifiable credentials and ZKPs, users can demonstrate compliance without revealing personal information, paving the way for privacy-preserving identity protocols and regulatory proofs.

Combining these three tools, ZKPs for privacy, threshold encryption for selective access, and compliance oracles for external verification, enables rich architectures for automated compliance. However, the secure and efficient integration of these tools into blockchain protocols presents challenges. Trusted setup phases in ZKP parameter initialization, multi-party key management in threshold systems, and centralized control in oracle networks can each undermine decentralization if not handled carefully.

It is worth noting that these mechanisms, despite their promise to balance privacy and compliance, introduce important legal complexities. ZKPs, though secure from a cryptographic standpoint, may not satisfy conventional evidentiary standards in judicial settings. Similarly, the distribution of authority in threshold-based systems complicates accountability and raises unresolved questions about liability in the event of compliance failures. As a result, these systems must be assessed not only for their technical soundness but also for their alignment with legal frameworks and institutional requirements.

Having introduced the three core cryptographic tools, we now develop a comprehensive framework for evaluating how these tools combine in automated compliance systems.

4.2 Technical Taxonomy for Automated Compliance

Building upon the five regulatory approaches in Section 3, we now examine the technical mechanisms enabling automated compliance, particularly *ex ante* approaches embedding requirements into protocols. The design space is multidimensional: invasive implementations enforce strong compliance but reduce adaptability; privacy-preserving systems require advanced cryptography to prove compliance without disclosure. Understanding these trade-offs is essential for evaluating solutions within legal and constitutional frameworks.

We introduce a structured taxonomy for evaluating cryptographic compliance approaches across four categories: *technical effectiveness*, *stakeholder burdens*, *regulatory effectiveness*, and *deployment considerations* (Figure 2). This framework enables comprehensive evaluation of emerging solutions and identifies gaps requiring resolution for full legal and operational compliance.

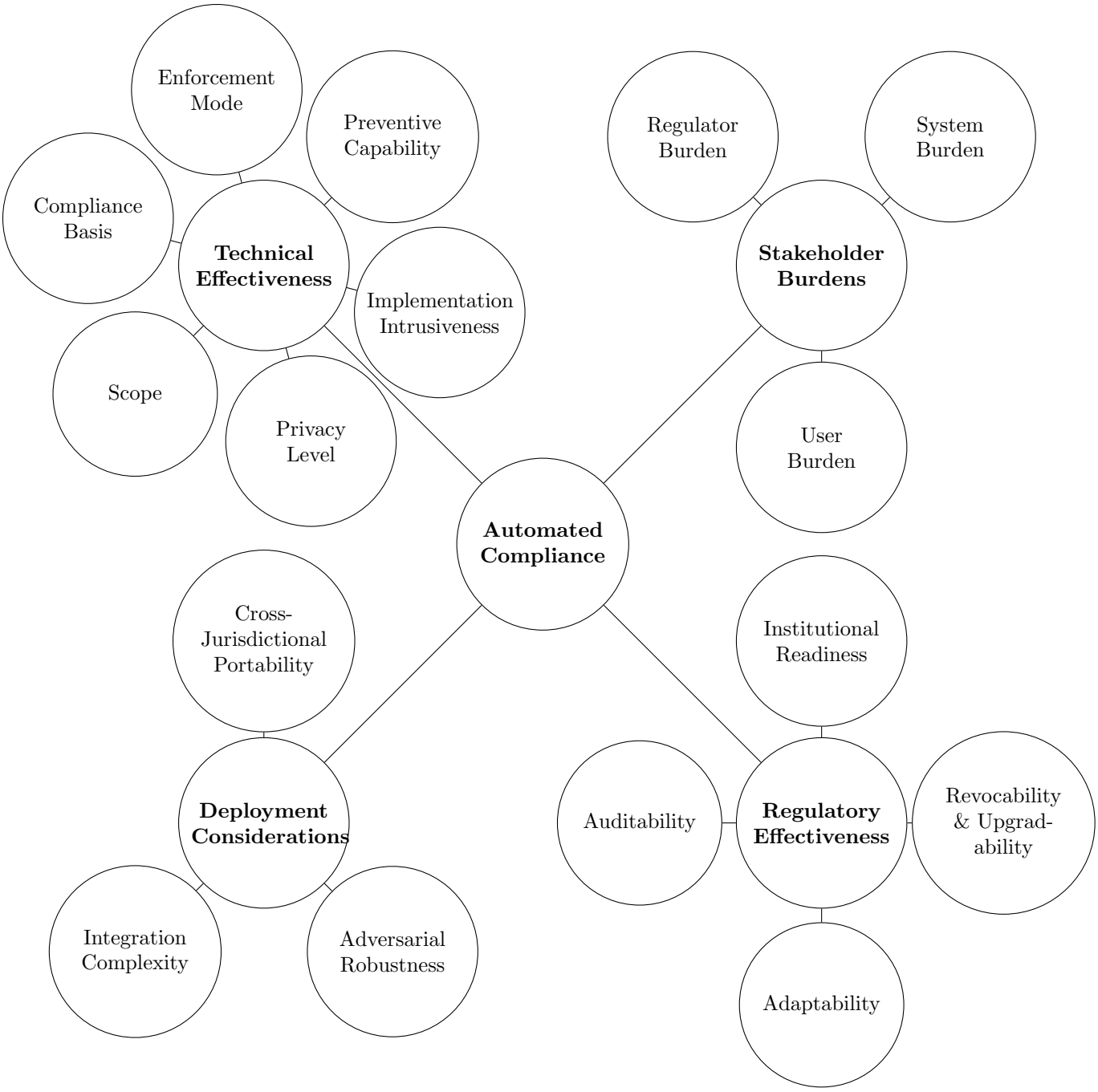

Figure 2: A taxonomy for comparing automated compliance approaches

4.2.1 Technical Effectiveness

These dimensions characterize how different compliance mechanisms address core legal and regulatory requirements:

Scope: Captures whether the solution applies only to programmable blockchains with smart contract functionality (*e.g.*, Ethereum), or can extend to more constrained platforms (*e.g.*, Bitcoin). Systems utilizing execution environments with a rich feature set may achieve greater expressivity and push a significant burden onto stakeholders.

Privacy Level: Assesses the degree to which transaction data and user identities remain confidential. High-privacy systems, often based on ZKPs, reveal only the fact that transactions meet compliance conditions, without exposing underlying details (even to regulators). Lower-privacy systems, such as those based on threshold encryption, may disclose limited information to designated authorities, balancing transparency with confidentiality. The Tornado Cash case illustrates the risks of designing systems that prioritize only privacy and have opaque compliance behavior Pertsev et al. (2019).

Compliance Basis: Defines what constitutes a compliant transaction. Systems may use fixed allowlists (*e.g.*, Privacy Pools), programmable on-chain predicates, or attestations issued off-chain (*e.g.*, zkFi, Derecho). This axis distinguishes between different compliance models and whether enforcement depends on centralized or decentralized authorities.

Enforcement Mode: Describes who enforces compliance logic. Enforcement may be embedded in smart contracts (on-chain blocking), delegated to off-chain actors (e.g., guardians), or depend on user behavior (e.g., attestations). Each mode implies different trust assumptions and levels of automation.

Preventive Capability: Evaluates whether the system proactively blocks illicit behavior (*ex ante*) or merely supports post-facto (ex post) verification. Preventive systems offer stronger assurances but often require tighter integration into the system (or occasionally system redesign). Reactive approaches enable flexibility but rely on post-hoc enforcement mechanisms.

Implementation Intrusiveness: Distinguishes between invasive designs that require core protocol changes and add-on solutions layered on existing infrastructure. Invasive systems can provide stronger guarantees but face higher deployment costs. Add-on approaches (*e.g.*, middleware or SDKs) are easier to adopt but may limit enforceability.

4.2.2 Stakeholder Burdens

Compliance designs distribute technical and operational burdens across users, systems, and regulators. Understanding this distribution is essential for predicting adoption and ensuring usability.

User Burden: Captures the computational load that compliance places on end users. Compliance that requires complex proof generation or user-managed credentials while simultaneously requiring interaction with external certified authorities may hinder adoption if not offset by strong incentives or usability improvements.

System Burden: Measures the infrastructure required to support compliance, including the maximum-allowed complexity of smart contracts, the possible need for off-chain services (*e.g.*, guardian networks, oracles), and the specific nature of cryptographic requirements. Systems that shift verification off-chain may reduce on-chain costs but increase complexity elsewhere. An exact categorization of such costs is necessary to inform adopters of tradeoffs across different system designs.

Regulator Burden: Reflects the effort required for regulators to verify compliance. Most agencies cannot support resource-intensive tasks like large proof verification or threshold decryption. Systems with a high computational cost for verification may be infeasible to audit at scale. Verifier-efficient designs, such as succinct SNARKs, reduce this load and improve auditability. Even off-chain attestations (e.g., via EAS Ethereum Attestation Service (2023)) can impose oversight burdens around credential management and revocation.

4.2.3 Regulatory Effectiveness

Technical sophistication alone cannot ensure regulatory compliance. These systems raise questions about conformity with established legal standards including due process, evidentiary requirements, and constitutional constraints, questions that require legal expertise to resolve definitively. The failure of traditional surveillance methods against privacy-preserving technologies (Kappos et al., 2018) underscores the need for compliance mechanisms that preserve regulatory visibility while respecting privacy rights.

Adaptability: Reflects how easily systems can accommodate evolving laws or policy priorities. Protocol-level changes (e.g., hard forks) impose high coordination costs, while modular middleware approaches (e.g., Privacy Pools, Derecho) enable updates without altering base protocol logic.

Auditability: Describes the system's capacity to produce evidence suitable for regulatory inspection. Legal admissibility often requires explanatory metadata and human-interpretable records, not just cryptographic validity. Designs should support compliance visibility without undermining user privacy.

Revocability and Upgradability: Addresses the ability to modify or revoke attestations and policies over time. As legal frameworks evolve, systems must adapt without compromising integrity.

Transparent and cryptographically sound mechanisms for updating credentials and compliance logic are essential.

Institutional Readiness: Assesses whether regulators, law enforcement, and institutions can feasibly adopt and operate the system. Approaches that require deep cryptographic expertise or non-standard tooling face steep institutional learning curves, potentially delaying deployment and limiting impact. Importantly, effective compliance must not come at the cost of innovation. Regulatory mechanisms that overly constrain design space may inadvertently suppress valuable experimentation or decentralization. Hybrid models that align enforcement strength with risk sensitivity offer promising paths forward.

4.2.4 Deployment Considerations

This final category evaluates the practical deployability, interoperability, and robustness of compliance mechanisms.

Integration Complexity: Measures the difficulty of incorporating compliance mechanisms into existing applications and infrastructure. Developer tooling, SDK availability, and compatibility with standards (e.g., ERC protocols) reduce integration friction.

Cross-Jurisdictional Portability: Measures the ability to navigate divergent regulatory regimes, particularly around AML/KYC and data protection. Highly tailored solutions may be efficient locally but difficult to scale globally. Portability demands modular designs that accommodate regional variation.

Adversarial Robustness: Evaluates the system's resilience to manipulation, forgery, or misuse. Key risks include replayed attestations, dishonest oracles falsifying compliance data, or guardian collusion in flagging mechanisms. Robust systems must withstand standard cryptographic and blockchain adversaries, with careful attention to both implementation flaws and systemic vulnerabilities. Compliance mechanisms may introduce new attack surfaces, such as deanonymization in selective disclosure or centralization in off-chain attestations, raising concerns about censorship resistance and adversarial robustness.

Having established the evaluative framework across four dimensions, we now apply this taxonomy to existing automated compliance proposals.

Dimension	**Privacy Pools** Buterin et al. (2024)	**Derecho** Beal and Fisch (2023)	**SeDe** Sahu et al. (2024b)	**zkFi** Sahu et al. (2024a)	**On-Chain Compliance** Azgad-Tromer et al. (2023b)	**a16z Position** Burleson et al. (2022)
Focus / Use Case	Mixers	Mixers + transfers	Any dApp	Any dApp	Any dApp	Any dApp
Privacy Level	Low (depends on anonymity set)	High (Regulator learns nothing)	Medium (High until flagged)	Medium	High	High
Compliance Basis	Whitelist of good Txs	Whitelist of good IDs	Flagging + Guardian-Gated Decryption	Programmable Proofs + Attestations	Whitelist	Off-chain attestations
Enforcer	Users	Users	Guardians	Guardians	Blockchain contracts	Certifiers + users
User Burden	Medium (proof + set choice)	Medium–High (ZK proving)	Low (unless flagged)	Low (unless flagged)	Medium–High (must follow contract logic)	Medium–High (varies by certifier)
System Burden	Low (off-chain logic)	Low	Low	Low	High (complex rules)	High
Regulator Burden	Medium (maintain sets + verify)	Medium (verify attestations)	High (coordinate with guardians)	High (coordinate with guardians)	Medium (code audit + allowlist)	Low (verifies attestations only)
Preventative of Illicit Txs	No	No	No	No	Yes	Yes
Implementation Intrusiveness	Low (backward compatible)	Low	Medium (dApp changes)	Medium	Medium–High (smart contract + chain-level)	Medium-High

Table 2: Comparison of Privacy & Compliance Approaches on Technical Effectiveness and Stakeholder Burdens. Here, "dApp" stands for decentralized application; "mixers" is used in the usual sense of services that mix potentially identifiable cryptocurrency funds with others.

4.3 Comparison of Existing Approaches

We evaluate several representative automated compliance architectures. Each system embodies trade-offs among privacy preservation, enforcement capability, stakeholder burden, and legal robustness. This section presents a structured comparison of six prominent approaches: Privacy Pools Buterin et al. (2024), Derecho Beal and Fisch (2023), SeDe Sahu et al. (2024b), zkFi Sahu et al. (2024a), and conceptual frameworks introduced in Azgad-Tromer et al. (2023a) and Burleson et al. (2022). We evaluate each approach across four major categories: technical effectiveness, stakeholder burdens, regulatory effectiveness, and deployment considerations. In particular, we summarize the technical effectiveness and stakeholder burdens imposed by Privacy Pools, Derecho, SeDe, zkFi, On-Chain Compliance models, and the a16z position paper in Table 2.

Details for Table 2. We classify user, system, and regulator burden as "low", "medium", or "high", with explanations provided in the table and use a similar classification for privacy levels. We assume that by default, all systems already encrypt all transactions.

Users in Derecho/a-16z/embedded compliance establish compliance by using ZKPs to prove that both parties in an encrypted transaction are "good." The certificate of being "good" is implemented differently in different systems, but this is the highest level of privacy achievable. Privacy pools use ZKPs slightly differently, wherein users establish compliance through a ZKP-type proof by showing that their encrypted transaction is among a set of already deemed good (possibly unencrypted) transactions called association sets. In this context, the privacy level depends on the size of the the association set; for instance, if an association set is 1, then all transaction details are revealed. The association sets are kept small to ensure efficiency of ZKP-proving. We characterize this as "low" privacy. In SeDe/ZkFI, the privacy is "high" until a transaction is flagged; at this point, the guardians completely decrypt the transaction, allowing the regulator to learn all transaction details. While this might seem befitting of a label of "low" privacy, no party other than the guardians and regulators sees this information. Consequently, we classified this system as having "medium" privacy.

Finally, we also label implementation intrusiveness similarly (low/medium/high) based on whether the protocol implementation requires changing the underlying code for smart contracts or the blockchain itself. For instance, Derecho and Privacy Pools do not require these changes and are hence labeled as having "low" intrusiveness. All other systems require some changes to the underlying blockchain.

4.3.1 Technical Effectiveness and Stakeholder Burdens

Privacy Pools and Derecho both exemplify non-invasive designs that achieve incremental compliance by requiring users to prove –through off-chain proofs and allowlists– that their interactions involve only legitimate entities. Both systems achieve privacy-preserving compliance using ZKPss (*e.g.*, ZK-

SNARKs), allowing users to prove that their transactions meet compliance criteria without revealing underlying data. Privacy Pools centers on a whitelist of "good" transactions, while Derecho builds around whitelists of "good" entities (possibly maintained by a regulatory body). These designs enable flexible, incremental deployment without protocol changes but do not proactively block illicit activity, relying instead on a "separating equilibrium" where only compliant users can interact meaningfully.

SeDe and zkFi instead adopt a guardian-mediated model. In these systems, transactions are private by default but may be selectively unmasked if flagged by regulatory bodies. Guardians collectively control decryption keys or trigger audit mechanisms. These designs reduce user and system burden under normal conditions, but shift substantial operational load to guardians when disputes or anomalies arise. Although these systems maintain a degree of intrusiveness, they support broad applicability and adaptability across decentralized applications.

In contrast, embedded compliance takes an invasive approach by encoding regulatory rules directly into smart contracts or the consensus layer. This allows for *ex ante* blocking of non-compliant transactions, offering the strongest preventive guarantees. However, it comes with significant implementation and governance challenges, particularly around rule updates and adapting to shifting regulatory requirements. Conceptual foundations for such systems have been proposed by Azgad-Tromer et al. (2023b) and Burleson et al. (2022), with a recent implementation seen in Ethereum Verified Pools (Coinbase, 2025).

Azgad-Tromer et al. (2023b) advocate for embedding compliance logic at the protocol level, enabling strong enforcement but introducing high complexity for users and developers, and regulatory burdens related to audits, allowlist management, and contract governance. These systems are well-suited to jurisdictions that demand strict preemptive control but often lack flexibility due to the rigidity of on-chain enforcement.

By contrast, the model outlined in Burleson et al. (2022) relies on off-chain attestations: trusted certifiers verify user compliance, and decentralized applications check these credentials before granting access. This design offers a significant degree of privacy for relatively low regulator-side overhead, though it depends heavily on the integrity and reliability of the certifier ecosystem. It achieves *ex ante* compliance with less architectural intrusion, but may entail varying user burden and nontrivial operational costs for managing attestation infrastructure.

In terms of scope, Privacy Pools are limited to enabling privacy-preserving compliant coin-mixing – where assets from multiple users are pooled and redistributed to obscure sender-receiver links – making them the most functionally restricted. Derecho extends this model by supporting compliant asset transfers within the pool. In contrast, the other solutions in Table 2 generalize compliance mechanisms to arbitrary decentralized applications (dApps).

Different compliance architectures impose varying burdens across three stakeholder groups: users, system operators, and regulators, as summarized in Table 2. Add-on systems like Privacy

Pools and Derecho keep system and user burdens relatively low by offloading logic to off-chain servers. However, they place moderate demands on regulators by requiring that they maintain and verify compliance sets. Guardian-based models like SeDe and zkFi minimize routine burdens but require significant coordination and oversight when flagging occurs. Invasive designs like On-Chain Compliance introduce high system and user complexity due to embedded logic. Meanwhile, off-chain attestation models (e.g., a16z's approach) shift operational complexity to certifier infrastructure, resulting in a moderate user burden (but low regulator overhead).

Together, these case studies illustrate a continuum of design choices reflecting tradeoffs among privacy preservation, regulatory assurance, implementation burden, and system adaptability. Add-on systems like Privacy Pools and Derecho emphasize minimal disruption and composability, while more invasive systems like On-Chain Compliance maximize regulatory enforcement at the expense of flexibility and simplicity. Middleware approaches like zkFi and selective disclosure systems provide nuanced tradeoffs, supporting hybrid models where enforcement is escalated only when necessary.

Ultimately, no single solution optimally satisfies all dimensions of effectiveness. In practice, hybrid models–such as those that combine off-chain attestation with on-chain flagging or auditability–may provide the best balance between enforcement, privacy, and ease-of-deployability. For example, the aftermath of the Bybit hack illustrates the limits of ex post detection and the value of building accountability and responsiveness directly into protocol infrastructure. Moving toward flexible, modular compliance layers that allow optional enforcement, selective disclosure, and certifier attestations may offer decentralized systems a more robust and future-proof compliance architecture.

4.3.2 Regulatory Effectiveness

From a regulatory standpoint, existing systems differ in their ability to provide visibility, enforceability, and legal legitimacy. Below, we discuss several important aspects of regulatory effectiveness.

Interpretability and Evidence: Systems based solely on cryptographic proofs, such as ZKPs, may face challenges in legal settings that require human-readable logs or standardized metadata. For example, Privacy Pools and zkFi offer strong privacy and compliance guarantees but lack conventional audit trails.

Distributed Responsibility: In guardian-based systems like SeDe, legal ambiguity arises if guardians fail to act or collude. Questions about accountability and liability remain unresolved in these decentralized enforcement frameworks.

Single Points of Trust: Oracle-based and certifier-driven systems (Derecho, a16z model) centralize key functions in trusted third parties. These actors could become chokepoints or sources of abuse, raising governance concerns if not properly regulated.

Auditability and Standardization: Regulator-friendly APIs, metadata schemas, and documentation are still nascent in most systems. While initiatives like the Ethereum Attestation Service (EAS) help, further development is required for regulators to audit and interact with compliance tools routinely.

Revocation and Upgradability: Few systems support attestation revocation or policy updates in a cryptographically sound and transparent manner. Real-world deployments must incorporate expiration dates, update hooks, or revocation registries.

Institutional Readiness: Financial regulators often lack the technical expertise to evaluate cryptographic systems or assess decentralization. Without standardized training, interfaces, or support frameworks, adoption of these tools remains limited. Legal definitions, such as what constitutes "control" over assets, must be clarified before these technologies can operate within established regulatory regimes. Despite promising progress, full regulatory alignment will require combining these technical systems with legally grounded processes and clearer governance frameworks. Also note that the work required to achieve such alignment is likely larger than with earlier, more incremental, technology changes. Simply put: getting regulators familiar with code is a bigger step-change than updating rules and training to accommodate a new form of electronic payment or record-keeping.

4.3.3 Legal and Government Alignment

The legal alignment of blockchain compliance tools hinges on how well they map onto current statutory and institutional structures. Most current systems remain at odds with traditional legal doctrines. We identify four important aspects to this discussion:

Due Process and Rulemaking: Automated enforcement systems raise important questions about compliance with administrative law principles. Systems that block transactions automatically, without notice or recourse, may raise due process concerns that legal scholars and courts will need to address, particularly regarding what safeguards would be constitutionally sufficient.

Judicial Reviewability: Mechanisms like ZKPs can strengthen reviewability by producing cryptographic evidence that can be used to demonstrate that a transaction satisfies some pre-defined compliance criteria. Such evidence can be generated without revealing sensitive details, with the proofs being re-verifiable, allowing regulators or auditors to confirm compliance well after execution.

However, whether ZKPs alone satisfy judicial reviewability requirements remains an open legal question. Courts or regulators may find mathematical guarantees difficult to interpret without supporting metadata, human-readable logs, or attestations linking proofs to real-world entities and

events. How existing evidentiary and administrative law standards apply to cryptographic proofs requires legal analysis beyond our scope.

For ZKP-based compliance to achieve full judicial reviewability, it must integrate these supplementary elements to bridge the gap between cryptographic assurance and legally actionable evidence. Achieving this also requires institutional readiness. Legal and regulatory bodies must be prepared, both technically and procedurally, to accept cryptographic proofs as valid evidence in compliance and enforcement processes.

Authority and Accountability: In decentralized systems, it may be difficult to identify a responsible party for legal violations. Models like SeDe or a16z's certifier architecture complicate enforcement because authority is distributed or delegated without clear lines of liability.

Evolving Legal Definitions: Terms like "decentralized," "controller," or "custodian" lack standardized definitions across jurisdictions. Ongoing regulatory proposals, including MiCA in the EU and the GENIUS and STABLE Acts in the U.S., are beginning to address these gaps, but significant ambiguity remains. For automated compliance systems to achieve widespread legal legitimacy, they must interoperate with statutory definitions, support standard forms of evidence, and accommodate the institutional processes of judicial and regulatory bodies.

4.3.4 Deployment Considerations

Deployment feasibility is shaped by the technical complexity of integration of compliance, jurisdictional compatibility, and robustness under adversarial conditions.

Integration Complexity: Add-on systems like Derecho and zkFi offer ease of integration through SDKs and modular contracts. Invasive systems like On-Chain Compliance, by contrast, require consensus-level changes, making them costly to deploy and difficult to coordinate.

Cross-Jurisdictional Portability: Systems tightly coupled to one region's rules (e.g., U.S. AML compliance) may not generalize to others. Modular architectures that abstract legal logic from transaction processing, such as zkFi or Privacy Pools, offer better global portability.

Adversarial Robustness: Threat models vary across systems. Guardian-based flagging systems may face collusion risks; oracle-fed attestation systems can suffer from data poisoning or censorship. Compliance solutions must be resilient not only to technical attacks but also to social or institutional manipulation.

4.3.5 Cost-Benefit Analysis

Economic viability is a key determinant of system adoption. Costs fall into three main categories:

Implementation Costs: These arise due to development effort, protocol changes, testing, and integration. Invasive systems (e.g., On-Chain Compliance) are resource-intensive, while middleware solutions (e.g., Derecho, zkFi) offer quicker deployment paths.

Operational Costs: Zero-knowledge systems require ongoing proof generation and verification, which may tax network or user devices. Off-chain infrastructure (e.g., certifier nodes, oracles, guardians) requires maintenance and governance, adding recurring overhead.

Indirect Market Effects: Compliance systems that introduce friction–for instance, higher gas costs, longer latencies, or poorly-designed user interfaces–may reduce user participation or currency liquidity. Conversely, systems that explicitly seek to increase trust and reduce enforcement costs may attract institutional adoption and enhance market stability. Ultimately, benefits must be weighed against direct and indirect costs. Gains may include reduced enforcement burdens, increased compliance rates, reputational assurances, and broader access to regulated financial infrastructure. However, quantifying these benefits remains challenging, especially without standardized performance benchmarks.

4.4 Summary and Future Directions

While compliance architectures have advanced considerably in the last decade, several key challenges remain. First, ZKPs still impose substantial computational costs, especially for complex logic. Improving proving efficiency through hardware acceleration, recursive proofs, and streaming verification remains a priority.

Second, systems must accommodate varying legal standards across jurisdictions. Modular and policy-aware designs will be critical to avoid infrastructure duplication. Similarly, compliance logic must be updatable while preserving the blockchain's integrity, requiring secure governance mechanisms for policy changes and credential revocation.

Third, privacy-focused protocols like Zcash remain difficult to integrate with regulatory frameworks. Selective disclosure mechanisms that preserve user privacy while supporting audits are an open area of research. Systems must also guard against new threats, such as oracle manipulation or guardian collusion, while maintaining decentralization.

Finally, regulator operability is essential. Verifications must be lightweight, interfaces intuitive, and outputs legally interpretable. Standardized attestations, logs, and APIs will ease adoption. Continued interdisciplinary collaboration is needed to develop compliance systems that are efficient, privacy-preserving, and legally usable.

Solving these challenges will require interdisciplinary collaboration across cryptography, legal studies, economics, and systems engineering. A sustainable path forward likely involves hybrid designs that combine privacy-preserving proofs, modular policy enforcement, trusted attestations, and human-in-the-loop governance. Continued development of tools, standards, and education will be key to unlocking a future in which blockchain technology can serve both innovation and public accountability.

Section 4 established what can be automated (compliance verification using ZKPs, selective disclosure through threshold cryptography) and what cannot be automated: context-dependent judgments requiring human oversight, evolving regulatory interpretations, and complex liability determinations. This technical foundation now enables development of hybrid frameworks that strategically deploy automated and human mechanisms where each performs best.

5 Towards Hybrid Regulatory Frameworks for Blockchain Compliance

Having established that regulatory approaches need not be mutually exclusive (Section 3), this section develops specific hybrid frameworks that strategically combine elements from multiple models. These frameworks address a practical reality: fully decentralized compliance systems face fundamental limitations. Even sophisticated cryptographic approaches like those examined in Section 4 require centralized elements: curated datasets for user authentication (as in Derecho), allowlist management by authorities, and human judgment for complex determinations.

Effective hybrid frameworks acknowledge this reality, combining traditional legal enforcement with selective automation where appropriate. Rather than forcing a choice between centralized control and automated compliance, these approaches deploy each mechanism where it performs best: automation for well-defined, stable requirements; human oversight for context-dependent judgments; centralized processes for coordination; and decentralized verification for transparency.

5.1 Theoretical Foundations of Hybrid Regulation

Hybrid regulatory frameworks combine elements from multiple regulatory models to achieve objectives that cannot be realized through any single approach. This concept builds upon the theory of responsive regulation in Ayres and Braithwaite (1992), which advocates for regulatory strategies that adapt to industry structure, history, and culture. In blockchain contexts, hybrid approaches are particularly valuable because they can address the multifaceted challenges of regulating decentralized systems while preserving their innovative potential. Hybrid systems can also accommodate the empirical fact that decentralized technologies often support a mixture of decentralized and centralized products and services.

The theoretical justification for hybrid approaches stems from recognition that blockchain systems operate across multiple dimensions simultaneously: they are global in reach, technically complex, rapidly evolving, and often intentionally resistant to centralized control. No single regulatory paradigm, whether traditional centralized oversight, gatekeeper regulation, or purely technical solutions, can adequately address all these dimensions. Yet, a useful framework must handle this panoply of properties without significant gaps.

The concept of "smart regulation" introduced in Gunningham and Grabosky (1998) further supports hybrid approaches, advocating for complementary combinations of regulatory instruments tailored to specific contexts. Their emphasis on policy mixes that leverage the strengths of different regulatory strategies while compensating for their weaknesses provides a theoretical foundation for our hybrid framework.

5.2 Typology of Hybrid Regulatory Approaches

We identify several promising hybrid approaches for blockchain regulation, each combining different regulatory elements to address specific challenges:

Embedded Supervision with Selective Intervention. This approach, building on Lorenz (2024), combines direct monitoring of blockchain data by regulators with selective intervention based on risk thresholds. Rather than requiring regular reporting from regulated entities, regulators leverage the inherent transparency of blockchain systems to monitor aggregate market activities directly. Human intervention occurs only when specific risk thresholds are crossed or anomalies are detected, creating an efficient oversight model that minimizes compliance burdens while maintaining regulatory visibility.

The Monetary Authority of Singapore's Project Ubin exemplifies this approach, using distributed ledger technology to facilitate regulatory monitoring while streamlining compliance processes. Similarly, the Bank for International Settlements' Project Rio explores how central banks can leverage DLT systems for more efficient supervision of financial markets (Bank for International Settlements, 2023).

Privacy-Preserving Compliance Tools with Traditional Analytics. This hybrid approach combines cryptographic compliance mechanisms like zero-knowledge proofs with traditional analytics for risk-based oversight. As proposed by Buterin et al. (2024), zero-knowledge proofs can enable users to demonstrate compliance with simple requirements (e.g., the source of funds is not known to be sanctioned) while preserving privacy for other activities. Complementing these mechanisms, traditional analytics focus on identifying suspicious patterns that warrant further investigation, rather than attempting comprehensive surveillance of all transactions.

The Privacy Pools protocol implementation demonstrates this approach, allowing users to prove their funds do not originate from known non-compliant sources without revealing their complete transaction history. This creates a separating equilibrium between legitimate privacy uses and

potentially illicit activities, making more efficient use of oversight resources (Beal and Fisch, 2023). As discussed below in the context of Tornado Cash, it remains unclear to what extent such an implementation may be legally immune. Still, it may leave the initial operators or deployers of the software at risk if their deployment experiences non-compliant use.

Enhanced Gatekeeper Regulation with Technological Infrastructure. This approach strengthens traditional gatekeeper models through shared technological infrastructure that reduces compliance costs and improves effectiveness. The Travel Rule implementation, for instance, can be enhanced through standardized APIs and shared utilities that simplify compliance for regulated entities (Greenberg and Goldstein, 2020). This maintains the distributed responsibility model while addressing the practical challenges of limited adoption.

The Travel Rule Information Sharing Alliance (TRISA) and OpenVASP protocol (described in Section 2) exemplify this approach, providing shared infrastructure that reduces compliance costs while improving standardization (OpenVASP Association, 2021).

Tiered Regulatory Approaches Based on Risk Profiles. This hybrid approach applies different regulatory mechanisms based on the risk profiles of various blockchain activities. High-risk activities face more intensive oversight, including pre-approval requirements, while lower-risk activities operate under lighter-touch frameworks emphasizing ex post monitoring. This risk-based approach allocates regulatory resources more efficiently while minimizing unnecessary constraints on innovation.

Singapore's Payment Services Act exemplifies this approach, creating a tiered regulatory framework that applies different requirements based on the specific activities undertaken and their associated risks. Similarly, Japan's Financial Services Agency has developed a graduated regulatory approach for virtual asset service providers based on their risk profiles and operational characteristics (IMF, 2023).

Having described four conceptual hybrid approaches, we now examine real-world implementations that demonstrate their practical viability.

5.3 Case Studies of Emerging Hybrid Approaches

Several nascent initiatives demonstrate the potential of hybrid regulatory approaches in blockchain contexts:

EU Markets in Crypto-Assets (MiCA) Regulation. The EU's comprehensive regulatory framework for crypto-assets combines elements of traditional gatekeeper regulation (licensing requirements for service providers) with technology-specific provisions that acknowledge the unique characteristics of distributed ledger systems. MiCA creates a tiered regulatory approach based on asset classification and risk profile, with different requirements for stablecoins, security tokens, and utility tokens (European Parliament and Council, 2022).

MiCA also incorporates elements of automated compliance by requiring certain technical stan-

dards for blockchain-based assets while maintaining traditional supervisory oversight. This hybrid approach balances innovation with consumer protection and financial stability objectives, creating a framework that can adapt to evolving technologies while maintaining consistent regulatory principles.

Compliant Privacy Protocols. Recent developments in privacy-preserving blockchain protocols demonstrate how technical design can facilitate regulatory compliance without compromising core privacy objectives. Aztec Connect combines zero-knowledge proofs with selective disclosure mechanisms, allowing users to maintain transaction privacy while enabling compliance verification for specific regulatory requirements (Aztec Protocol, 2022).

Similarly, the Zcash Shielded Assets framework combines privacy-preserving transactions with compliance tools that enable appropriate regulatory visibility without compromising overall system security (Electric Coin Company, 2021). These approaches demonstrate how carefully designed protocols can reconcile seemingly contradictory objectives through integration of privacy and compliance mechanisms.

DeFi Governance Frameworks with Regulatory Integration. Decentralized finance protocols are increasingly developing governance frameworks that incorporate regulatory considerations alongside technical and economic factors. Compound's governance system, for example, includes explicit consideration of regulatory implications when evaluating protocol changes, creating a form of self-regulation guided by community governance while acknowledging external regulatory constraints (Compound Labs, 2022). Note, however, that this cuts both ways. As discussed below, Compound is party to legal actions questioning the fairness and compliance of some governance actions.

Aave's legal structure similarly combines decentralized protocol governance with traditional corporate entities that interface with regulators, creating a hybrid structure that preserves innovation while providing clear points of regulatory contact (Aave, 2023). These approaches demonstrate how decentralized governance can incorporate regulatory considerations without necessarily sacrificing autonomy or innovation.

These case studies demonstrate that hybrid approaches are implementable in practice, though they face challenges around coordination, legal authority, and governance. What principles should guide the design of effective hybrid systems?

5.4 Design Principles for Effective Hybrid Systems

Based on our analysis of existing approaches and theoretical foundations, we propose several design principles for policymakers and legal scholars evaluating hybrid regulatory frameworks in blockchain contexts:

Principled Flexibility. Hybrid frameworks should balance rule-based certainty with principled flexibility, creating systems that can adapt to technological change without sacrificing pre-

dictability or consistency, though achieving this balance raises complex administrative law questions. This approach, advocated by Black (2015), enables regulatory evolution while maintaining the certainty that market participants require for confident participation.

Appropriate Technology Integration. Hybrid frameworks could leverage technology appropriately, using automated mechanisms offering clear advantages while maintaining human oversight for complex, context-dependent judgments, subject to constitutional and due process constraints that require legal analysis. This principle recognizes the potential and limitations of technological solutions, avoiding technology skepticism and uncritical techno-optimism.

Multi-Stakeholder Governance. The development and evolution of hybrid frameworks could involve diverse stakeholders, including regulatory authorities, industry participants, technical experts, and civil society representatives, following models from internet governance. This inclusive approach, modeled on internet governance mechanisms like the Internet Engineering Task Force, can enhance legitimacy and effectiveness while preventing capture by any single interest group.

Interoperability and Standards. Hybrid frameworks can promote interoperability through open standards that enable consistent compliance across jurisdictions and platforms, though cross-jurisdictional harmonization faces political and legal challenges. Projects like the InterVASP Messaging Standard demonstrate how technical standards can facilitate compliance while reducing fragmentation and implementation costs (Joint Working Group on interVASP Messaging Standards, 2022).

Privacy by Design with Appropriate Oversight. Hybrid frameworks should incorporate privacy by design principles while enabling appropriate regulatory visibility where legitimate public policy objectives require it, subject to Fourth Amendment and privacy law constraints. This balanced approach, advocated by Cavoukian (2011), recognizes that privacy and regulatory oversight need not be mutually exclusive when systems are thoughtfully designed.

5.5 Implementation Challenges and Solutions

Despite their theoretical promise, hybrid regulatory approaches face significant implementation challenges that must be addressed for successful adoption:

Technical Complexity and Resource Requirements. Hybrid approaches often involve sophisticated technologies that may exceed the current capabilities of many regulatory authorities and market participants. Addressing this challenge requires targeted capacity building, public-private partnerships for technology development, and phased implementation approaches that allow gradual adaptation. It is also critical to ensure regulatory regimes impose only technically-feasible requirements (e.g., not expecting perfectly reliable geolocation of internet users) and reasonably manage any uncertainty derivative of technical limitations (e.g., not allowing "they used a VPN" to serve as an absolute defense).

The UK Financial Conduct Authority's regulatory sandbox addresses this challenge, creating

a controlled environment where innovative regulatory approaches can be tested and refined before broader implementation (Financial Conduct Authority, 2023). Similarly, regulatory technology accelerator programs can foster the development of tools that reduce technical barriers to compliance.

Designers of compliance systems should also recognize that when a regulator is forced to choose between ignoring a rule or adding a non-automated step, they are sometimes unable to select the former. This can be highly context-dependent, where, for example, the reliability requirements for fraud screening in domestic retail payment networks with low transaction limits vary materially from those for sanctions screening in wholesale international transfer systems. The nature of the problem at hand may, in part, dictate which technologies can be brought to bear. And lawmakers who want the compliance regimes they mandate to be regulated via automated means should consider the feasibility of automation when writing the rules.

Cross-Border Coordination. The global nature of blockchain networks necessitates international regulatory coordination, which faces both political and practical challenges. Regional approaches like the EU's MiCA regulation provide potential models for broader international cooperation, while technical standards bodies can facilitate interoperability without comprehensive regulatory harmonization.

The Financial Stability Board's work on crypto-asset regulation demonstrates how international coordination can progress through principles-based approaches that allow jurisdictional adaptation while maintaining overall consistency (Financial Stability Board, 2022). Similarly, FATF's Risk-Based Approach Guidance provides a framework for consistent regulation across jurisdictions while accommodating different legal systems and market contexts.

Regulatory Authority and Legitimacy. Questions about the legal authority for novel regulatory approaches must be addressed to ensure legitimacy and prevent legal challenges. In some jurisdictions, this may require legislative updates to explicitly recognize new regulatory tools and approaches. The Wyoming Blockchain Laws provide an example of legislative action to clarify regulatory authority and create legal certainty for blockchain applications (Wyoming Legislature, 2022).

Balancing Innovation and Stability. Hybrid approaches must balance innovation protection with financial stability and consumer protection objectives. This requires careful calibration of regulatory intensity based on risk profiles and continuous assessment of emerging technologies and business models. Singapore's regulatory approach demonstrates this balance, with a framework that differentiates retail and institutional markets while providing clear paths for innovative products to achieve regulatory compliance (Monetary Authority of Singapore, 2022).

Governance Adaptation. Effective implementation requires governance mechanisms that can evolve regulatory approaches as technologies and markets develop. Meta-governance frameworks that establish processes for regulatory evolution without requiring constant legislative intervention can address this challenge. The EU's Lamfalussy Process for financial regulation provides a poten-

tial model, separating high-level principles from technical implementation details to enable more flexible adaptation (European Commission, 2020).

5.6 Measuring Effectiveness of Hybrid Approaches

Evaluating the effectiveness of hybrid regulatory frameworks requires appropriate metrics that capture their multidimensional impacts:

Compliance Efficiency. Effective hybrid frameworks should reduce compliance costs relative to traditional approaches while maintaining or improving compliance rates. Metrics might include implementation costs, ongoing operational expenses, and compliance verification efficiency.

Innovation Impact. Regulatory approaches should minimize negative impacts on beneficial innovation while constraining harmful activities. Metrics might include new product development rates, capital formation in regulated sectors, and geographic distribution of blockchain activities (to assess regulatory arbitrage effects).

Regulatory Outcomes. Ultimate effectiveness depends on achieving legitimate regulatory objectives like financial stability, market integrity, and consumer protection. Metrics might include fraud rates, market volatility, and systemic risk indicators in blockchain-based financial markets.

Adaptability. Given the rapidly evolving nature of blockchain technology, regulatory frameworks must adapt without creating excessive uncertainty. Metrics might include time required for regulatory updates, consistency of application across similar activities, and stakeholder assessments of regulatory predictability.

By systematically evaluating hybrid approaches against these metrics, regulators and industry participants can refine implementation strategies and develop more effective regulatory models over time. Combining quantitative and qualitative assessments, this evidence-based approach provides a foundation for continuous improvement of blockchain regulatory frameworks.

Addressing these implementation challenges will require ongoing collaboration among technologists, legal scholars, and policymakers, a theme we return to in the conclusion.

6 Conclusion and Future Research Directions

The tension between blockchain innovation and regulatory compliance need not be zero-sum. By thoughtfully designing compliance mechanisms that leverage blockchain's unique properties while respecting legitimate regulatory objectives, we can create financial systems that are both more innovative and more compliant than traditional alternatives.

Our analysis demonstrates that while automated compliance approaches offer significant advantages in efficiency and jurisdictional reach, they cannot address all dimensions of the blockchain compliance challenge in isolation. The technical analysis in Section 4 shows how embedding regulatory requirements into protocols can achieve broader coverage without proportional increases

in enforcement resources, and how privacy-preserving techniques using zero-knowledge proofs can reconcile privacy with regulatory oversight. However, the taxonomic evaluation in Section 3 reveals that these approaches face substantial limitations regarding adaptability, governance, and legal authority when regulatory requirements evolve.

Our framework suggests that hybrid approaches, which combine elements from multiple regulatory models, warrant serious consideration by policymakers and legal scholars. These hybrid frameworks could leverage automated compliance for well-defined requirements while maintaining appropriate human oversight for complex determinations. Whether such approaches can successfully address the unique challenges of blockchain regulation while respecting constitutional constraints and fundamental legal principles remains a question requiring collaborative analysis across technical, legal, and policy domains.

Future research should focus on formal verification of compliance logic and developing techniques to prove the correctness of automated compliance implementations. It should also explore cross-jurisdiction compliance, creating technical standards that enable compliance across multiple regulatory regimes. Additionally, research should advance privacy-preserving regulatory reporting, developing cryptographic techniques that enable aggregate regulatory insight without compromising individual privacy. Finally, governance mechanisms for compliance updates should be designed, enabling systems to adapt to regulatory changes without centralized control. By advancing our understanding in these areas, we can unlock the full potential of blockchain technology while addressing legitimate regulatory concerns.

References

Aave (2023). Aave protocol documentation. https://docs.aave.com/. Accessed August 14, 2025.

Alkadri, S. (2018). Defining and regulating cryptocurrency: fake internet money or legitimate medium of exchange? *Duke L. & Tech. Rev.*, 17:71.

Ayres, I. and Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA.

Azgad-Tromer, S., Garcia, A., and Tromer, E. (2023a). The case for embedded regulation in blockchain technologies: A technical survey of methods and feasibility. Technical report, Columbia University.

Azgad-Tromer, S., Garcia, J., and Tromer, E. (2023b). The case for on-chain privacy and compliance. *Stanford Journal of Blockchain Law and Policy*, 6:265.

Aztec Protocol (2022). Aztec connect: Compliance framework. *Aztec Protocol Technical Documentation*.

Bank for International Settlements (2023). Project rio: Monitoring wholesale cbdc usage with data analytics. *BIS Innovation Hub Project*.

Beal, J. and Fisch, B. (2023). Derecho: Privacy pools with proof-carrying disclosures. *Cryptology ePrint Archive, Paper 2023/273*.

Ben-Sasson, E., Bentov, I., Horesh, Y., and Riabzev, M. (2018a). Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive, Paper 2018/046*.

Ben-Sasson, E., Chiesa, A., Riabzev, M., Spooner, N., Virza, M., and Ward, N. P. (2018b). Aurora: Transparent succinct arguments for R1CS. *Cryptology ePrint Archive, Paper 2018/828*.

Black, J. (2015). Decentring regulation: Understanding the role of regulation and self-regulation in a 'post-regulatory' world. *Current Legal Problems*, 54(1):103–146.

Block, A. R., Holmgren, J., Rosen, A., Rothblum, R. D., and Soni, P. (2020). Public-coin zero-knowledge arguments with (almost) minimal time and space overheads. Cryptology ePrint Archive, Paper 2020/1425.

Block, A. R., Holmgren, J., Rosen, A., Rothblum, R. D., and Soni, P. (2021). Time- and space-efficient arguments from groups of unknown order. Cryptology ePrint Archive, Paper 2021/358.

Bowe, S., Grigg, J., and Hopwood, D. (2019). Recursive proof composition without a trusted setup. *Cryptology ePrint Archive, Paper 2019/1021*.

Brito, J., Shadab, H., and Castillo, A. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Columbia Science and Technology Law Review*, 16:144.

Burleson, J., Korver, M., and Boneh, D. (2022). Privacy-protecting regulatory solutions using zero-knowledge proofs. *a16z*.

Buterin, V., Illum, J., Nadler, M., Schär, F., and Soleimani, A. (2024). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Blockchain: Research and Applications*, 5(1):100176.

Bünz, B., Fisch, B., and Szepieniec, A. (2019). Transparent SNARKs from DARK compilers. *Cryptology ePrint Archive, Paper 2019/1229*.

Calo, R. and Citron, D. K. (2021). The automated administrative state: A crisis of legitimacy. *Emory Law Journal*, 70(4):797–845.

Cavoukian, A. (2011). Privacy by design in law, policy and practice: A white paper for regulators, decision-makers and policy-makers. *Information and Privacy Commissioner of Ontario, Canada*.

Charoenwong, B., Kirby, R., and Reiter, J. (2025). Tradeoffs in automated financial regulation of decentralized finance due to limits on mutable turing machines. *Scientific Reports*, 15.

Chen, B., Bünz, B., Boneh, D., and Zhang, Z. (2022). HyperPlonk: Plonk with linear-time prover and high-degree custom gates. *Cryptology ePrint Archive, Paper 2022/1355*.

Citron, D. K. (2008). Technological due process. *Washington University Law Review*, 85(6):1249–1313.

Coglianese, C. and Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. *Georgetown Law Journal*, 105:1147–1223.

Coinbase (2025). Verified pools. https://www.coinbase.com/verified-pools. Accessed August 14, 2025.

Compound Labs (2022). Compound governance documentation. *Compound Protocol Documentation*.

Crootof, R. and Ard, B. (2021). Structuring techlaw. *Harvard Journal of Law & Technology*, 34.

Duffie, J. D., Olowookere, O., and Veneris, A. (2025). A note on privacy and compliance for stablecoins.

Electric Coin Company (2021). Shielded assets framework: Regulatory considerations. *Zcash Documentation*.

Ethereum Attestation Service (2023). Ethereum attestation service: Infrastructure public good for making attestations. https://attest.org/. Accessed August 14, 2025.

European Commission (2020). The lamfalussy process and eu financial regulation. *EC Financial Services Documentation*.

European Parliament and Council (2022). Markets in crypto-assets (mica) regulation. *Council of the European Union Position*.

Financial Action Task Force (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. *Technical Report*.

Financial Conduct Authority (2023). Regulatory sandbox: Outcomes and lessons learned. *FCA Reports*.

Financial Stability Board (2022). Regulatory and supervisory approaches to crypto-assets. *Consultative Document*.

Gabizon, A., Williamson, Z. J., and Ciobotaru, O. (2019). PLONK: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *Cryptology ePrint Archive, Paper 2019/953*.

Gerard, D. (2017). *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts*. CreateSpace Independent Publishing Platform.

Gilad, S. (2010). It runs in the family: Meta-regulation and its siblings. *Regulation & Governance*, 4(4):485–506.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, page 291–304, New York, NY, USA. Association for Computing Machinery.

Greenberg, A. and Goldstein, S. (2020). Travel rule: The path forward for virtual assets. *Financial Intelligence Report*.

Groth, J. (2016). On the size of pairing-based non-interactive arguments. *Cryptology ePrint Archive, Paper 2016/260*.

Guillen, T. G., Gale, A. D., Tanney, M. N., Reynolds, V., and Karambelas, A. (2023). Developer arrested following ofac sanctions of the tornado cash protocol. *The Journal of Robotics, Artificial Intelligence & Law*, 6.

Gunningham, N. and Grabosky, P. (1998). *Smart Regulation: Designing Environmental Policy*. Oxford University Press.

Hughes, S. J. and Middlebrook, S. T. (2016). Regulating cryptocurrencies in the united states: Current issues and future directions. *William Mitchell Law Review*, 40(2):813.

iden3 (2025). Circom 2 documentation. https://docs.circom.io/. Accessed August 14, 2025.

IMF (2023). Japan financial sector assessment program: Technical note on regulation and supervision of fintech. *IMF Country Report*.

Jackson, H. E. (2007). Variation in the intensity of financial regulation: Preliminary evidence and potential implications. *Yale Journal on Regulation*, 24:253.

Joint Working Group on interVASP Messaging Standards (2022). Intervasp messaging standard. *IVMS101 Standard Documentation*.

Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S. (2018). An empirical analysis of anonymity in zcash. In *27th USENIX Security Symposium*, pages 463–477.

Kothapalli, A., Setty, S., and Tzialla, I. (2021). Nova: Recursive zero-knowledge arguments from folding schemes. *Cryptology ePrint Archive, Paper 2021/370*.

Lorenz, G. (2024). Regulating decentralized financial technology: A qualitative study on the challenges of regulating defi with a focus on embedded supervision. *Stanford Journal of Blockchain Law and Policy*, 7:136.

Matter Labs (2025). Zksync: The elastic network. https://www.zksync.io/. Accessed August 14, 2025.

Mohanta, B. K., Jena, D., Panda, S. S., and Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, 8:100107.

Monetary Authority of Singapore (2022). Approach to regulating digital payment token services. *MAS Guidance*.

OpenVASP Association (2021). Openvasp protocol: Technical specification. *OpenVASP Technical Documentation*.

Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of fatf standards. *Journal of Economic Criminology*, 2:100040.

Pertsev, A., Semenov, R., and Storm, R. (2019). Tornado cash privacy solution version 1.4.

Polygon Labs (2025). Polygon zkevm: Scaling for the ethereum virtual machine. https://polygon.technology/polygon-zkevm. Accessed August 14, 2025.

RISC Zero (2025). Risc zero: Zero-knowledge required. https://risczero.com/. Accessed August 14, 2025.

Sahu, N., Gajera, M., and Chaudhary, A. (2024a). zkfi: Privacy-preserving and regulation compliant transactions using zero knowledge proofs. *arXiv*.

Sahu, N., Gajera, M., Chaudhary, A., and Ivey-Law, H. (2024b). Sede: Balancing blockchain privacy and regulatory compliance by selective de-anonymization. *arXiv*.

Schrepel, T. (2021). Computational antitrust: An introduction and research agenda. *Stanford Computational Antitrust*, 1.

Setty, S. (2019). Spartan: Efficient and general-purpose zkSNARKs without trusted setup. *Cryptology ePrint Archive, Paper 2019/550*.

Takei, Y. and Shudo, K. (2024). Fatf travel rule's technical challenges and solution taxonomy. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 784–799. IEEE.

Treleaven, P. (2017). Financial regulation of fintech. *Journal of Financial Perspectives*, 5(3).

Walch, A. (2019). In code (rs) we trust: Software developers as fiduciaries in public blockchains. *Regulating Blockchain: Techno-Social and Legal Challenges*, pages 58–81.

Wyoming Legislature (2022). Wyoming blockchain laws. *Wyoming State Legislature*.

Zetzsche, D. A., Arner, D. W., and Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, 6(2):172–203.