Blockchain Lawyers Forum

Review | Q2 2025
Arbitration Edition

Your go-to source for blockchain law and regulatory news

INSIDE THE BLF REVIEW

INSIDE THE BLF REVIEW

BLF ARBITRATORS LIST

As blockchain and crypto-related disputes continue to rise, arbitration is increasingly becoming the preferred mechanism for resolving complex cross-border conflicts. In response to this trend and repeated requests from our members, the **Blockchain Lawyers Forum** has launched the **BLF Arbitrators List** — a curated, independent directory of experienced arbitrators with a deep understanding of both **international arbitration** and the **blockchain ecosystem**.

BLF members address these developments in their articles below, focusing on smart contracts, decentralized justice disputes, enforcement mechanisms, and other emerging legal challenges in complex technical contexts.

The list is **not affiliated with any arbitral institution** and is **independently managed** by **Dr. Nino Sievi** and **Ms. Sophie Nappert**, ensuring a rigorous and impartial selection process.

This initiative aims to support parties, counsel, and institutions in identifying qualified professionals equipped to handle the unique complexities of Web3 disputes.

Dr. Nino Sievi

Sophie Nappert

1. **Be Included: Click here to fill out the application.**
2. **Be Connected: Contact us at director@blf.io to be referred selected crypto-arbitrators for your disputes.**

BLF ARBITRATORS LIST

Sherzod Abdulkasimov
Managing Director at PraeLegal Uzbekistan
Linkedin

Juliette Asso-Richard
Counsel at LALIVE
Linkedin

Jonatan Baier
Partner at MME
Linkedin

Chiann Bao
Partner at ArbBoutique
Linkedin

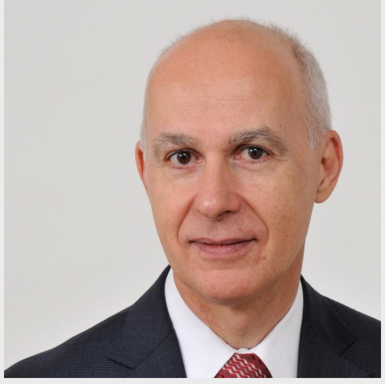
Chloë Bell
Barrister at 3 Verulam Buildings
Linkedin

Axel Buhr
Partner at Gabriel Arbitration
Linkedin

Elizabeth Chan
Legal Manager at Stevenson, Wong & Co.
Linkedin

Celso De Azevedo
Barrister and Arbitrator at Enterprise Chambers
Linkedin

Mariel Dimsey
Partner and Office Head at CMS
Linkedin



Christoph Dugué
Independent Counsel and Arbitrator
Linkedin

Zachary Figueroa
CCO at Backpack
Linkedin

Eliane Fischer
Partner at Rothorn Legal
Linkedin

Anna Guillard Sazhko
Independent Counsel and Arbitrator
Linkedin

Emily Hay
Managing Counsel at ArbBoutique
Linkedin

Ole Jensen
Managing Counsel at ArbBoutique
Linkedin

Mohammad Hossein Heidarpour
Head of Legal at Siassi Mccunn Bussard
Linkedin

Rebecca Keating
Barrister at 4 Pump Court
Linkedin

Leon Kopecky
Partner at Schoenherr Attorneys at Law
Linkedin

Panagiotis Kyriakou
Associate at Archipel
Linkedin

Matthew Lavy
Barrister at 4 Pump Court
Linkedin

Crenguta Leaua
Director at The Swiss Institute for Alternative Thinking
Linkedin

Stefan Leimgruber
Partner at Schellenberg Wittmer Ltd.
Linkedin

Aija Lejniece
Independent Counsel & Arbitrator
Linkedin

Sebastian Lukic
Attorney at Schoenherr Attorneys at Law
Linkedin

Sinem Mermer
Counsel at Balcıoğlu Selçuk Eymirlioğlu Ardıyok Keki Avukatlık Ortaklığı
Linkedin

Charlie Morgan
Partner at Herbert Smith Freehills
Linkedin

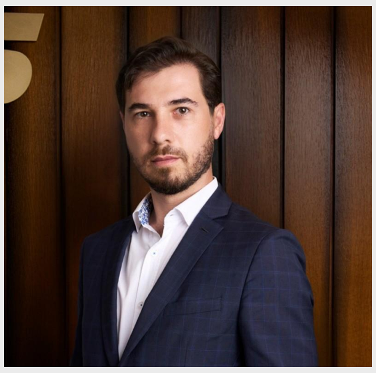
Racheal Muldoon
Barrister at 36 Commercial
Linkedin

Sophie Nappert
Independent Arbitrator
Linkedin
Selection Committee Member

Tom C. Pröstler
Partner at CMS
Linkedin

Petra Rihar
Partner at Rihar & Thouvenin Dispute Resolution
Linkedin

Joanna Rindell
Head of Legal at Trilitech Limited
Linkedin



Leonid Shmatenko
Counsel at 5Gambit Disputes
Linkedin

Nino Sievi
Partner at Nater Dallafior
Linkedin
Selection Committee Member

Matthew Townsend
Partner at Reed Smith LLP
Linkedin

Edgar J. Young Dominguez
Partner at Pacifica Legal
Linkedin

Sam Winter-Barker
Senior Associate at Wilmer Hale
Linkedin

To access laws, articles, and additional information related to each news item, simply click the underlined links.

REGULATORY NEWS

A recap of the main blockchain legal news

🇦🇷ARGENTINA:

Milei Cleared in "Cryptogate" Over LIBRA Meme Coin

- On **June 5**, Argentina's Anti-Corruption Office ruled that President Javier Milei did **not** breach ethics laws by promoting the LIBRA memecoin in a **February 14** post on X, determining he acted in a **personal capacity**, not in an official one.
- Although his endorsement preceded a dramatic spike (over **$4 billion market cap**) followed by a ~94% crash—resulting in estimated investor losses of **$250 million**—the watchdog noted **no misuse of public resources**.
- Milei subsequently **dissolved the task force** investigating the case in May via executive decree, drawing criticism that the move may obstruct proper investigation.
- Despite the administrative clearance, **criminal investigations remain ongoing** in Argentina (judicial inquiries into Milei, his sister, Karina, and close associates), with **Interpol and US authorities** also involved.

🇧🇷BRAZIL:

Key Tax & Legal Changes

1. Flat 17.5% Tax on Crypto Gains
Effective **June 12, 2025**, Brazil ended its monthly exemption (up to R$35,000 or ~$6,300) and introduced a flat 17.5 % capital gains tax on all crypto profits—domestic or offshore, exchange-held or self-custodied—under **Provisional Measure 1303**.

- Small investors now taxed where they were previously exempt; large holders may save compared to earlier progressive rates (up to 22.5%).
- Quarterly tax reporting with loss offsets allowed over the previous five quarters (subject to tighter limits in 2026).

2. Court-Authorized Crypto Asset Seizure
In **early April 2025**, Brazilian judges have been authorized to seize cryptocurrency assets from debtors who owe money and are behind on their payments, signaling a growing recognition that digital assets can be both a form of payment and a store of value.

- The court said: ""Although they are not legal tender, crypto assets can be used as a form of payment and as a store of value"

📌**Bottom Line:** Brazil now **fully taxes crypto gains** and legally acknowledges **crypto as seizable assets**—a significant tightening of both tax and creditor frameworks on digital property.

Regulatory News

To access laws, articles, and additional information related to each news item, simply click the underlined links.

🇸🇻 EL SALVADOR:

Bitcoin & AI Moves Despite IMF Deal

- **Continued Bitcoin Purchases** Since **Dec 19, 2024**, El Salvador added 240 BTC to government reserves, bringing them to **6,209 BTC**—despite IMF terms requiring a halt to public-sector accumulation and ending Bitcoin's legal tender status. The IMF has acknowledged the purchases as **technically compliant**, citing a "flexible interpretation" allowing acquisitions outside the formal fiscal sector.
- **Scaling Back Bitcoin Status** Under the IMF pact, mandatory acceptance of Bitcoin has been eliminated, and public-sector usage is now voluntary only.
- **AI Ambitions with Nvidia** On **April 21**, the National Bitcoin Office signed a **Letter of Intent** with Nvidia to build "sovereign AI"—focused on national infrastructure, workforce upskilling, health, education, environment, and meteorological models.

🇨🇦 CANADA:

Kraken Achieves Restricted Dealer Registration

Kraken secured a restricted dealer registration from the Ontario Securities Commission (OSC) on April 1. The registration reaffirms Kraken's commitment to serving Canadian investors as its platform now has more than $2 billion Canadian dollars ($1.4 billion) in combined assets under custody.

🇺🇸 USA:

Crypto Regulation Roundup

1. Stablecoin Framework Advances with GENIUS Act

- On **June 17**, the U.S. Senate passed the *GUIDING and Establishing National Innovation for U.S. Stablecoins Act* (GENIUS Act) with a **68–30** vote, marking the first major federal stablecoin regulatory bill.
- It introduces a framework requiring issuers to have 1:1 backing for their stablecoins with safe assets (e.g., U.S. Treasuries), **reserve audits**, **AML/BSA compliance**, and limited issuance to approved entities.
- Supporters see this as a path toward mainstream adoption by banks and tech firms, reinforcing dollar dominance; critics point to risk-laden precedents.
- The bill now heads to the House, where it may be reconciled with other stablecoin measures.

2. Digital Asset Market Clarity (CLARITY) Act Progresses

- The **House Financial Services Committee**, along with Agriculture, advanced the *CLARITY Act* (H.R. 3633), aiming to define regulatory jurisdiction: **CFTC for digital commodities; SEC for investment contracts**, with new registration classes for exchanges and brokers.
- A full House vote is imminent, laying groundwork for coherent U.S. market structure regulation.

3. State-Level Developments: Connecticut & California

- Connecticut **(House Bill 7082)**: Unanimously passed and signed into law, the bill titled "An Act Concerning Various Revisions to the Money Transmission Statutes, State Payments and Investments in Virtual Currency [...] **prohibits** state and local governments from accepting, holding, or investing in any cryptocurrency; kiosks and remittance agencies must comply with virtual currency regulations by **October 1, 2025**.
- California **(Assembly Bill 1180)**: The State Assembly passed the bill 68–0 on **June 2**, requiring the DFPI to enable **crypto payments** for state fees under the Digital Financial Assets Law, with implementation set for **July 1, 2026**, and a regulatory pilot through **2031**.

Regulatory News

To access laws, articles, and additional information related to each news item, simply click the underlined links.

🇩🇪 GERMANY:

Germany’s financial regulator, the Federal Financial Supervisory Authority (BaFin), granted BitGo Europe a MiCA license to provide digital asset services in the EU. The license allows BitGo to offer services to crypto-native firms and traditional finance institutions, including banks and asset managers within the EU.

🇨🇭 SWITZERLAND:

Switzerland Advances Crypto Data Transparency

- **Automatic Crypto Data Exchange**
  On **June 6, 2025**, Switzerland’s Federal Council adopted legislation to enable **automatic exchange of crypto-related tax information** with **74 partner countries**, including the UK, all EU member states, and most G20 nations—excluding the US, Saudi Arabia, and China.
- **Implementation Timeline & Oversight**
  If Parliament approves, the law takes effect **January 1, 2026**, with the **first exchanges slated for 2027**. Partner countries must comply with the OECD’s Crypto-Asset Reporting Framework (CARF) and consent to reciprocal data sharing. Periodic reviews will ensure ongoing compliance.
- **Strategic Alignment**
  This move aligns Switzerland with global standards, mirroring EU’s DAC 8 and OECD AEOI initiatives. It underscores Switzerland’s intent to elevate tax transparency and maintain a level playing field for crypto firms.

🇺🇦 UKRAINE:

Ukrainian lawmakers have introduced a draft bill that would allow the National Bank of Ukraine to include cryptocurrencies like Bitcoin in the country’s reserves.

🇬🇧 UK:

Crypto Regulatory Highlights

1. Retail Access to Crypto ETNs

On **June 6, 2025**, the FCA proposed lifting its ban on *crypto exchange-traded notes (ETNs)* for retail investors—if these are listed on FCA-recognized exchanges and marketed with full risk disclosures. The aim: balance consumer choice with protection, without extending to crypto derivatives.

2. Mandatory Transaction Reporting

Effective **January 1, 2026**, crypto firms must collect and report detailed customer and transaction data to HMRC under the OECD Crypto-Asset Reporting Framework (CARF):

- **User data**: name, DOB, address, UK NIN or foreign TIN; extends to companies, trusts, charities.
- **Transaction data**: asset type, value, amount, transaction type.
- **Penalties**: up to **£300 per user** for non-compliance.

3. Comprehensive Crypto Regulatory Regime

On **April 29**, Chancellor Rachel Reeves unveiled proposals under the *Financial Services and Markets Act 2000 (Cryptoassets) Order 2025* to regulate crypto exchanges, dealers, custody, staking, and more—applying full financial services regulations (capital requirements, governance, market-abuse rules). These measures position the UK as a global digital asset leader, diverging from the EU’s MiCA-style approach.

Regulatory News

To access laws, articles, and additional information related to each news item, simply click the underlined links.

🇹🇭 THAILAND:

Thailand Crypto: Five-Year Tax Break & Exchange Ban

1. 💰 Five-Year Tax Exemption on Crypto Gains

From **January 1, 2025 to December 31, 2029**, Thailand will waive capital gains tax on crypto sales made through **licensed crypto asset service providers**, as part of a bid to position itself as a regional financial hub.

- The Thai government estimates this measure could boost tax revenue by at least **1 billion baht (~US $30 million)** via increased economic activity.
- The exemption applies **only to transactions on SEC-regulated platforms**, supporting Thailand's commitment to AML compliance.

2. 🚫 Block on Unlicensed Exchanges

Effective **June 28, 2025**, the Thai SEC will **block access to five major** foreign exchanges—Bybit, OKX, CoinEx, 1000X, and XT.COM—for operating without a Thai license. The move aims to **protect investors** and combat money laundering.

- The SEC has referred cases to the Economic Crime Suppression Division and advises users to **withdraw assets before the ban**.
- The action follows the **Royal Decree on Technology Crimes**, which empowered regulators to swiftly block unlicensed digital platforms.

🇮🇳 INDIA

The Reserve Bank of India is set to broaden the reach of its digital rupee pilots by introducing new use cases and features for both its retail and wholesale central bank digital currencies (CBDCs), according to the central bank's Annual Report for 2024–25.

The central bank said it aims to explore programmability and offline capabilities for the digital rupee, features that may increase its applicability in areas with limited internet access and tailor payments for specific use cases such as government subsidies or corporate spending controls.

Currently, both versions of the CBDC are undergoing pilot testing. The retail CBDC pilot is being conducted with select customers and merchants through participating banks, while the wholesale pilot is targeting use in the interbank market.

🇸🇬 SINGAPORE:

Singapore Tightens DTSP Regulation & WazirX Exits

1. Strict License Requirement for Foreign-Only Crypto Services

On **June 6**, the MAS confirmed that **from June 30**, any Singapore-incorporated firm offering digital token services solely to overseas clients must hold a **DTSP license**—though such licenses will only be granted in **"extremely limited circumstances"** due to AML/CFT and supervision risks.

- Firms targeting both local and international users under existing DPT licensing remain unaffected.
- No transitional period is planned—violations could result in **fines up to SGD 250k and/or jail terms of up to 3 years**

2. Crypto Exodus: WazirX Rebrands & Relocates

Following the **June 30** deadline, WazirX—focused on the Indian market yet headquartered in Singapore—has restructured:

- A Singapore court **rejected** its revival plan, prompting its parent, Zettai, to form **Zensui Corporation** in **Panama** and shift operational control there.
- WazirX's Singapore entity **won't seek a DTSP license**, and continues operations aimed outside Singapore.

BLF COLUMN

Knowledge *from* our members, *for* our members

Home
The New York Times
Book R
Teenager's Path and a Killing Put Spotlight on Mental Care
Debt Bill S
"All the News That's Fit to Print"

Litigation Against Decentralized Autonomous Organizations (DAOs): Navigating the Legal Frontier

By Daniel Hayward-Hughes

The rise of decentralized autonomous organizations (DAOs) represents a significant evolution in how organizations can be structured and operated. DAOs leverage blockchain technology to enable decentralized decision-making, often without a central authority.

While this innovation brings numerous advantages, it also presents unique legal challenges, particularly in respect to litigation.

This article explores the complexities of litigating against DAOs, related jurisdictional issues, identification of responsible parties, and the applicability of traditional legal principles.

Many novel issues arise in the context of DAOs, such as the assessment of DAOs for tax purposes, the applicability of financial and other regulations and how a DAO might be subject to insolvency proceedings or wound up. Given the limited space available here, however, such considerations are outside the scope of this article.

For a deeper dive into the current state of DAOs, at least from an English law perspective, we recommend reading *Decentralized Autonomous Organizations (DAOs): A Scope Paper*, published by the Law Commission in July 2024. Following that publication, the Law Commission has launched a public consultation in early 2025 on potential legislative reforms aimed at giving DAOs statutory recognition under English law.

Understanding DAOs

DAOs are structures which facilitate individuals coming together with a view to realising a common interest or goal, whether commercial or otherwise. The DAO itself is governed by smart contracts—self-executing contracts with the terms of the agreement directly written into code. These smart contracts are deployed on blockchain platforms, such as Ethereum, and operate autonomously once launched. Decisions within a DAO are typically made through a voting process, where token holders vote on proposals and/or have governance rights.

Jurisdictional Challenges

One of the most significant hurdles in litigating against DAOs is determining the appropriate jurisdiction. DAOs, by design, are borderless entities that exist on the internet/decentralised blockchain. Traditional notions of jurisdiction are based on physical presence or the location of business operations, both of which are ambiguous in the context of DAOs.

Courts may need to develop new criteria for establishing jurisdiction over DAOs. Potential approaches could include the location of DAO developers, the physical location of servers hosting the blockchain, or the domicile of a significant number of DAO participants. However, each of these approaches has its limitations and complexities.

Where a DAO engages with the off-chain world, either through purporting to enter into contracts with third parties outside of the DAO or by holding real-world (off-chain) assets as well as assets held on-chain on other blockchains, it will not be able to "opt out" of the national and international laws which would otherwise apply to those contracts or assets.

As such, many DAO developers have accepted the inevitability of interacting with some national or international laws and have started to use existing legal forms, such as limited companies, foundations, or trusts, to benefit from the separate legal personality and limited liability they afford. This process is sometimes called 'wrapping' the DAO and, increasingly, developers are 'wrapping' DAOs in offshore jurisdictions such as the British Virgin Islands, the Cayman Islands, Bermuda, and more recently Liechtenstein and Guernsey, where there are also tax, strong governance and robust legal benefits. In some cases, DAOs now use multi-layered wrappers, combining legal entities with multi-signature wallet structures, to provide a hybrid of decentralised and accountable governance.

Identifying Responsible Parties

Another major issue is identifying who can be held accountable in a DAO. Traditional corporations have clear leadership structures with identified directors and officers. In contrast, DAOs lack a centralized leadership, and decision-making is distributed among token holders. This raises questions about who bears liability for the actions of the DAO.

Several possibilities exist for determining liability:

- *The wrapper*: As set out above, if a legal personality is used to 'wrap' the DAO, then the relevant company, foundation, partnership etc, would be the obvious party to look to first for liability. However, the precise nature of the wrapper and alleged dispute will have to be carefully considered in order to navigate potential issues of piercing any corporate veil to determine where liability may ultimately accrue.
- *Developers and Creators*: The individuals or entities that develop and deploy the DAO's smart contracts could be targeted for litigation. However, once the DAO is operational, developers often relinquish control, complicating this approach.
- *Token Holders*: In some cases, token holders who actively participate in the governance of the DAO might be held liable, especially if they vote for proposals that result in legal violations or breach. This raises concerns about the fairness and practicality of pursuing numerous, potentially anonymous individuals.
- *Service Providers*: Entities providing services to DAOs, such as exchanges or platforms hosting DAO tokens, might also face litigation, particularly if they facilitate activities that lead to legal disputes.

Service of Process on DAOs

Proper service of process and adequate notice to a DAO is not straightforward. Unless 'wrapped' or otherwise registered under relevant local company law, there is usually no physical location attached to a DAO, and it is even more difficult to find the domicile of an anonymous token holder. However, if it could be successfully argued that a DAO is akin to a partnership or an unincorporated association (UA), then under common law principles applicable to such partnerships and UAs, adequate service on any general partner or member may constitute service on the DAO.

Litigation Against Decentralized Autonomous Organizations (DAOs): Navigating the Legal Frontier

Therefore, even if the majority of the DAO's native token holders (in this sense, the partners) remain anonymous, if the identity of one token holder is known, then proceedings may theoretically be initiated by effective service on that individual. In many cases, the founders of a DAO will continue to hold tokens, so they may be more readily identifiable than third party token holders.

Applicability of Traditional Legal Principles

Applying traditional legal principles to DAOs involves several challenges:

- *Contract Law*: Smart contracts, the foundation of DAOs, operate differently from traditional contracts. Issues such as enforcement, interpretation, and modification of smart contracts in the eyes of the law need to be addressed.
- *Corporate Law*: The principles governing corporate entities may not easily translate to DAOs. Concepts such as fiduciary duties, corporate governance, and shareholder rights may need to be reimagined or adapted.
- *Regulatory Compliance*: DAOs operating in regulated industries, such as finance or healthcare, must navigate a complex landscape of compliance requirements. Regulatory agencies might struggle to enforce laws against decentralized and pseudonymous entities.
- *AML/KYC*: In 2025, some DAOs have started integrating compliance tools using AI-powered oracles. These tools are capable of monitoring and flagging sanction risks, financial conduct issues, and AML/KYC requirements based on predefined rule sets, but it remains to be seen how robust these are.

Case Studies and Precedents

- *The DAO Hack (2016*): One of the first major incidents involving a DAO, where a vulnerability in The DAO's smart contract code was exploited, resulting in the theft of $50 million worth of Ether. This incident led to a hard fork of the Ethereum blockchain but also raised questions about liability and legal recourse.
- *SEC v. The DAO (2017)*: The U.S. Securities and Exchange Commission (SEC) issued a report concluding that The DAO's tokens were securities and subject to federal securities laws. This case underscored the need for regulatory clarity and the applicability of securities laws to DAOs.
- *CFTC v. Ooki DAO (2022)*: In this case, service of proceedings against the DAO made through the Ooki DAO online community forum was held to be sufficient and that Ooki DAO received actual notice of the litigation because the online forum was where the majority of members, owners or token holders congregate or operate.
- *Sarcuni v. bZx DAO (2023)*: A Southern District of California federal district court held that DAOs may be deemed general partnerships if they meet the general legal criteria for such entities.
- *Samuels v. Lido DAO* (2024): A Northern District of California federal district court held that DAOs can be sued; it's not just software; and its likely a general partnership, since token holders share profits and governance.
- *Hector DAO (2024)*: Absent a head office or centralised control, where a DAO is subject to a court ordered receivership, for the purposes of Chapter 15 recognition, the main centre of interest will be the location of the receivers who were making decisions on the DAO's behalf. In this case, that was the British Virgin Islands. Chapter 15 recognition was sought to assist the receivership process generally and to protect it from interference by litigation filed against the DAO in New Jersey.

The decision also positively resolved the question of whether a DAO can be a debtor under Chapter 15, and will likely form persuasive precedent for cases emerging in other common law jurisdictions like the Cayman Islands, Bermuda and the UK.

Future Directions and Legal Innovations

The legal landscape for DAOs is still evolving. Several potential developments could shape the future of litigation against DAOs:

- *Legislative Action:* Jurisdictions may enact specific laws or regulations addressing the unique nature of DAOs, providing clearer guidelines for their operation and legal accountability. As noted above, the Law Commission in England has taken initial steps in this direction, and we would expect other English common law jurisdictions to adopt similar approaches where appropriate and where compatible with local jurisprudence.
- *Legal Recognition*: Some jurisdictions, such as Vermont, Wyoming and Tennessee in the United States, have begun to recognize DAOs as legal entities, offering a framework for their incorporation and governance. Other jurisdictions, such as Singapore, Hong Kong, and the UAE, are exploring limited recognition under sandbox regimes or bespoke VASP legislation.
- *Technological Solutions*: Advances in blockchain technology and smart contracts could enable built-in compliance mechanisms, dispute resolution systems, and more transparent governance models. DAO-native arbitration platforms, such as Kleros or Aragon Court, continue to evolve and may eventually gain broader acceptance.

Conclusion

Litigating against decentralized autonomous organizations presents novel challenges that test the boundaries of existing legal frameworks. As DAOs continue to proliferate and evolve, the legal community must adapt and innovate to address the complexities they introduce. Collaboration between technologists, legal experts, and regulators will be essential to develop a robust legal infrastructure that balances the benefits of decentralization with the need for accountability and legal certainty.

__Daniel Hayward-Hughes__ is a Partner at Pierson Ferdinand LLP where he leads the blockchain disputes practice in London. He is an English qualified solicitor advocate and has been admitted to the bars of the British Virgin Islands, the Cayman Islands, and Bermuda.

Smart Contracts and Arbitration: Addressing Arbitrability and Enforcement

By Katharina Michl and Maša Samardžić

Abstract

With the rapid development of technology, smart contracts have emerged as a useful mechanism for automating and securing digital transactions. The rise of such technology brings new challenges for dispute resolution. This piece explores the role of arbitration in resolving disputes arising out of smart contracts, analysing both on–chain and off–chain mechanisms, the validity of coded arbitration agreements and procedural issues such as due process and the enforceability of arbitral awards under the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (NYC).

1. Introduction

Smart contracts are programmable, self-executing protocols, i.e. software programs operating on blockchain platforms. They automatically carry out, verify, and enforce the terms of an agreement when triggered by predetermined events. Smart contracts use a conditional logic structure, typically "if this happens, then do that" and aim to facilitate secure and transparent transactions that are recorded immutably on the blockchain. They aim to eliminate the need for intermediaries such as lawyers or brokers.

Smart contracts are powerful tools for automating agreements and operations. They often depend on external information from the real world. This information is provided through trusted data sources known as "oracles". Despite their name, smart contracts are not "contracts" in the traditional legal sense; they are rather software code that can represent ownership, transfer assets, or execute business logic within the blockchain environment.

By removing intermediaries and enabling automated execution, smart contracts aim to increase efficiency, reduce costs, and improve the security and reliability of digital transactions.

In 2021, the United Kingdom Law Commission defined the term "*smart legal contract*" as a "*legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program.*" The Commission further identified three categories of smart legal contracts:

- Natural language contracts with automated performance by code,
- hybrid contracts where some contractual obligations are defined in natural language, while others are defined in the code of a computer program, and
- contracts recorded solely in code.

Smart contracts evolving and becoming more complete and self-executing may lead to a new age in dispute resolution in which the involvement of a neutral third party, such as an arbitrator, will no longer be needed. Some even consider that smart contracts could create an entirely dispute-free environment. By contrast some say that disputes are inevitable. The question is not whether disputes in the context of blockchains and smart contracts will arise, but rather which mechanism is best suited to resolve such disputes.

2. Arbitration Agreements in Smart Contracts

One option to resolve such disputes is arbitration. In relation to arbitrating blockchain matters, two main groups of arbitration proceedings can be identified: on-chain arbitration and off-chain arbitration. On-chain arbitration refers to dispute resolution that occurs entirely within a blockchain environment. The equivalent of a "traditional" arbitral award is enforced by a smart contract. It allows for a complete departure from the traditional system of enforcement of awards in commercial arbitration. Off-chain arbitration, on the other hand, occurs outside of a blockchain environment, despite the dispute potentially arising from a blockchain-based transaction or smart contract. Instead of relying on automated, on-chain mechanisms, parties turn to external arbitrators to resolve their disputes.

As the CEO and Co-Founder of blockchain security boutique firm RAID Square, Sébastien Martin states, "*Smart contracts open up a wide range of potential interactions with arbitration. They represent an entirely new frontier, offering both complex cases to be resolved through arbitration and potential tools to enhance the arbitration process itself.*"

Including an arbitration agreement in a smart contract consisting at least partly of natural language does not pose many difficulties. However, if an arbitration agreement is to be included in coded form, this gives rise to more complex issues.

While the UK Law Commission voiced doubts as to the qualification of choice of law agreements embedded in code as binding contracts, it stayed silent with regards to arbitration agreements. Thus, whether an arbitration agreement embedded in code can be qualified as legally binding continues to be unclear. Further, there is no clarity as to whether such arbitration agreements meet the formality threshold of Article II of the New York Convention.

3. Jurisdictional Challenges

Disputes arising from smart contracts and cryptocurrencies frequently present significant challenges regarding the application of conflict of law rules. Smart contracts operate as self-executing programmes on blockchains and are commonly used to create digital assets, transfer ownership, and facilitate decentralized finance. Both smart contracts and the assets they govern are intangible and exist on decentralized networks that span multiple jurisdictions across the blockchain.

Crypto assets such as Bitcoin and Ethereum are traded on a global market accessible to individuals and entities worldwide, yet they are not subject to any single jurisdiction. These assets are not easily traceable on the blockchain which complicates matters even further. Consequently, when disputes arise from smart contracts used to trade such assets, all parties involved face considerable practical difficulties.

In these situations, there is often tension between parties, as each would prefer the dispute to be heard in the jurisdiction of their own domicile. Claimants may be uncertain about where to bring their claim, while defendants may face the prospect of being sued in jurisdictions with which they have no connection. This undermines the principle of legal certainty, as it becomes unpredictable how the law will be applied, and which jurisdiction will ultimately prevail.

Many of these issues can be mitigated if the parties have already entered into an arbitration agreement specifying the choice of law and forum. Such agreements provide clarity and predictability, helping to avoid jurisdictional disputes and ensuring a more efficient resolution process.

3.1. Arbitration vs Litigation

Once a dispute arises out of a smart contract, should parties opt for arbitration or litigation as a method of dispute resolution?

Litigation is still the more popular option when it comes to methods of smart contract dispute resolution. If smart contracts do not expressly contain an arbitration clause, the default option is most often litigation. Many businesses and legal professionals are still more comfortable going via the route of the traditional court system as they are not familiar with the benefits of arbitration and the blockchain itself. Blockchain-based arbitration is still new, making parties hesitant to choose this option.

Litigating smart contracts gives leeway to forum shopping, particularly when there is no exclusive jurisdiction clause. Multiple jurisdictions can claim authority over a dispute, and parties will aim to choose the most favourable one. Since in such disputes there is often a cross–border element, parties will almost never be situated in the same place and, therefore, will opt for the jurisdiction best suited for them. This gives rise to several problems. Commencing several lawsuits across multiple jurisdictions can be extremely costly and slow. If a judge renders a decision in one jurisdiction, such decision may not be easily enforceable in another. Laws regarding blockchain, smart contracts, and digital assets are not harmonized across the globe, making the enforcement of court decisions in another jurisdiction difficult.

Although less common, arbitration offers an effective solution to the problem of forum shopping in disputes involving smart contracts. Where parties have agreed to include an arbitration clause in the smart contract, they are afforded the flexibility to select a neutral jurisdiction that is acceptable to both sides. By specifying the forum in advance, the risk of forum shopping is significantly reduced.

The existence of a pre-selected forum helps to alleviate tensions between parties, as it removes the incentive for either side to seek a jurisdiction that might be more advantageous to it. This approach also minimises the likelihood of parallel proceedings in multiple jurisdictions, saving both time and costs associated with cross-border litigation. Arbitration provides a clear and efficient mechanism for resolving disputes arising from smart contracts. Smart contracts are often borderless as they involve globally distributed parties. This is compatible with the very nature of arbitration. Arbitration is designed for cross-border disputes and provides parties with a neutral forum. The New York Convention allows arbitration awards to be enforced across the globe, making enforcement easier than with court judgments.

3.2. Validity of Coded Arbitration Agreements

Parties and arbitrators often lack the technical expertise to interpret coded agreements, casting doubt on their enforceability and effectiveness. The validity of arbitration clauses expressed in code remains uncertain.

The New York Convention's recognition and enforcement of arbitral awards is fundamentally dependent on the existence of a valid arbitration agreement that satisfies the formal requirements of Article II. This provision requires that an arbitration agreement be "*in writing*" and either "*signed by the parties*" or "*contained in an exchange of letters or telegrams*". At first glance, coded arbitration agreements seem to fall outside the scope of this traditional formulation. However, both judicial interpretation and evolving practice in international arbitration suggest a more flexible and technology friendly approach.

A broader view of the "*in writing*" requirement is also supported by the UNCITRAL Model Law on International Commercial Arbitration (1958) recommendations on interpretation of Article II (2) of the New York Convention. These recommendations encourage the recognition of modern means of communication and affirm that the illustrative list in the New York Convention (“*letters or telegrams*”) is not exhaustive. Consequently, courts in several jurisdictions have accepted electronic communications, including emails, faxes, and digital records, as satisfying the formal requirement for arbitration agreements.

As stipulated in Option I, Article 7 of the UNCITRAL Model Law, the "*in writing*" requirement is satisfied if the agreement is concluded by "*electronic communication*," which UNCITRAL defines as "*any communication that the parties make by means of data messages*." A "*data message*" is further described as "*information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy*."

On the face of these definitions, computer code could be considered a valid form of arbitration agreement as it constitutes a data message stored by electronic means. However, doubts arise as to the original intent of those who drafted the UNCITRAL Model Law, who likely did not envisage computer code falling within the scope of these provisions.

On 11 July 2024, UNCITRAL set out the Model Law on Automated Contracts which provides much-needed guidance on the interpretation of smart contracts. This assists governments in formulating national legislation on smart contract interpretation and supports legal professionals in understanding the technical terminology and interpretative challenges associated with such contracts. If the parties wish to include an arbitration clause in their smart contract, it is still advisable to opt for natural language contracts in order to avoid issues with the validity of the clause and so that relevant parties have a clear understanding of the contract. Another option would be to draft the arbitration clause on a separate sheet in natural language, while the rest of the contract would stay in code. This way the validity of the arbitration clause and its contents are left undisputed.

The arbitration agreement should also specify the seat of arbitration. The law of the chosen seat governs the validity of the arbitration agreement and the procedural aspects of the arbitration. Given the inherently decentralized nature of smart contracts and the use of Distributed Ledger Technology (DLT), which often operates across multiple jurisdictions, it is useful for the parties to expressly agree upon the seat of arbitration. This clarity ensures certainty regarding which country’s courts will have supervisory jurisdiction over the proceedings.

As previously discussed, designating the seat of arbitration provides legal certainty and predictability for both parties and arbitrators. It also serves to prevent forum shopping, which can be a particular concern in cases involving decentralized technologies.

4. Blockchain Arbitration in Practice: Obstacles and Opportunities

Blockchain technology continues to expand rapidly beyond its use in cryptocurrencies and into decentralized finance (DeFi), supply chains and digital identity. With such growth, the question of dispute resolution in such contexts is becoming increasingly important. Blockchain arbitration – dispute resolution mechanisms which can operate together with blockchain ecosystems present obstacles and opportunities, these being the responsibility of arbitrators to investigate.

One of the most discussed obstacles is the lack of technical expertise among arbitrators. Traditional arbitrators focus on legal doctrines of arbitration but not on blockchain architecture, smart contracts, digital assets and functioning of the decentralized market. The knowledge gap between these two spheres may result in lack of technical terminology and faulty smart contract execution.

Input could be sought from blockchain security firms. According to Sébastien Martin, "*Smart contract disputes sit at the intersection of legal, technical, and economic systems. Collaboration between arbitrators and technical professionals allows for a well-rounded understanding of each case. This ensures that decisions consider all relevant dimensions of the dispute*." Additionally, "*arbitrators often do not have the necessary background to fully understand the nature of exploits, vulnerabilities, or how a breach occurred. Cyber experts can explain the technical details in a way that is accessible and relevant for legal decision-making. Similarly, crypto tracers can analyse blockchain transactions to provide clear evidence of what happened, when, and by whom*".

Arbitration has a centralized nature which clashes with the decentralized ethos of blockchain. Arbitral tribunals or arbitral institutions are centralized bodies, imposing their authority and hierarchy into a market which is designed to minimize this very notion.

Moreover, traditional arbitration relies on the identification of parties, witnesses and arbitrators while blockchain relies on anonymity, this being one of the main reasons its users operate in such a market. Verification of identity in arbitration directly undermines one of the key features of blockchain.

Another arbitration feature which appears to clash with blockchain principles is procedural efficiency. Parties can sometimes experience traditional arbitration as slow and procedurally exhaustive. This contradicts the automated and immediate functioning of smart contracts. Smart contracts trigger payments based on the codes embedded into the agreement, and if the dispute resolution process is delayed, it could render the transaction ineffective or cause financial losses, defeating the purpose of automation.

Despite the previously mentioned obstacles, blockchain arbitration opened new and innovative ways of dispute resolution. There are specific programs for on–chain arbitration mechanisms such as Kleros, Aragon Court and Jur, presenting alternatives. These platforms combine blockchain features such as transparency and distributed decision making, offering dispute resolution that fits well with the decentralized environment. These systems are faster, more cost–efficient and aligned with the expectations of blockchain users, as well as being already embedded into smart contracts, and triggered by pre–defined conditions.

While there is great appeal for use of these new innovations, such as on–chain mechanisms, traditional arbitration still offers significant advantages that blockchain–based systems cannot replicate. Specifically, as explained below, arbitral awards can be enforced under the New York Convention. Such global enforceability is crucial in cross–border disputes, in comparison to on–chain decisions which may not be legally recognized in many jurisdictions. Traditional arbitration has been developed through decades of procedural refinement and expert decision–making. In complex commercial disputes, it is imperative to invoke nuanced interpretation and previous judgments that on–chain legal practitioners may not be able to provide.

To reap the benefits of both systems, parties taking part in blockchain transactions should stay prudent when drafting arbitration agreements. Smart contracts should contain a clearly defined arbitration clause, specifying the mechanism, rules and seat of arbitration. When choosing an arbitration seat, it is highly important to choose a jurisdiction supportive of blockchain technology and arbitration. This promotes a more effective enforcement and resolution of proceedings. If there is uncertainty relating to technical issues in smart contract disputes, there is a possibility of collaborating with blockchain experts and bridging the gap between legal expertise and blockchain–specific matters.

5. Enforcement of Arbitral Awards

The enforcement of arbitral awards issued via blockchain protocols presents significant challenges, particularly in relation to the New York Convention. Central to these concerns are the formal validity of coded arbitration agreements, the observance of due process, and the impartiality of decentralized adjudicators. As a result, it is essential to scrutinise whether blockchain-based arbitral awards can be accommodated within the current international legal framework, or if reforms are necessary to bridge the gap between law and emerging technologies.

5.1. Formal Requirement

A coded arbitration clause embedded in a smart contract and stored immutably on a blockchain may be construed as satisfying the formality requirement of the New York Convention. The code itself acts as a record of the agreement to arbitrate. It is accessible and verifiable by both parties and by third parties such as arbitrators or national courts. The execution of such contracts often involves digital signatures or the use of private keys, which are functionally equivalent to handwritten signatures in confirming mutual consent between the parties.

The doctrine of separability ensures that even if a smart contract as a whole is not deemed legally enforceable, the arbitration agreement within it can be treated independently and validated on its own terms.

While smart contracts and coded agreements represent a departure from traditional written contracts, their functional and evidentiary features align with the underlying rationale of Article II of the New York Convention: to ensure a clear, consensual, and documented agreement of the parties to arbitrate. As such, coded arbitration agreements are increasingly viewed as capable of meeting the formality requirements of the New York Convention, paving the way for the recognition and enforcement of blockchain-based arbitral awards. This evolution in interpretation aligns with the broader pro-enforcement ethos of the New York Convention and reflects a shift toward function-over-form reasoning in international arbitration practice.

5.2. Due Process Concerns

Procedural fairness is a fundamental principle of international arbitration, and without it, an arbitral award may be refused recognition and enforcement under the New York Convention. While blockchain-based dispute resolution offers an alternative in terms of speed and cost, it raises important questions regarding due process safeguards. These concerns are particularly acute in the context of automated, decentralized platforms such as Kleros, Aragon Court and Jur where traditional procedural elements – such as notice, impartial adjudication, and the right to be heard – are either redefined or substantially altered.

To properly assess whether such mechanisms comply with the standards of the New York Convention, it is instructive to analyse how a specific protocol such as Kleros functions in practice. Kleros is a decentralized arbitration platform that operates entirely on-chain using smart contracts and crowdsourced decision-making.

Articles V(1)(b) and V(1)(d) of the New York Convention provide grounds for refusing recognition and enforcement of an award if a party was not given proper notice or was unable to present its case, or if the arbitral procedure was not in accordance with the parties' agreement. These provisions contain the core elements of due process: equal treatment, the right to be heard, and impartial adjudication.

Smart Contracts and Arbitration: Addressing Arbitrability and Enforcement

The Kleros protocol diverges significantly from conventional arbitral models. Disputes are resolved by jurors instead of arbitrators. Jurors are blockchain users who self-select by staking tokens to gain eligibility for selection. Once chosen, jurors review evidence submitted during a designated period and cast their votes cryptographically. Jurors need not have legal training, and there are no oral hearings, opportunities for clarification, or reasoned awards. The system prioritises efficiency and decentralization over procedure.

Although Kleros allows both parties to submit evidence and written arguments, concerns remain regarding notice and participation. The process is automatically triggered when a dispute is submitted, and the opposing party may not receive individualised or verifiable notice of the arbitration or the identity of the decision-makers. This raises concerns under Article V(1)(b) of the New York Convention, which requires that respondents receive proper notice and an opportunity to defend themselves.

Another major issue is the impartiality and independence of decision-makers, as required by Article V(2)(b) of the New York Convention. In Kleros, jurors are incentivised through a Schelling point voting system: those who vote with the majority are financially rewarded, while dissenters lose their staked tokens. This creates a structural financial bias, encouraging jurors to align with the expected majority rather than to impartially assess the evidence.

These due process shortcomings make Kleros-based awards particularly vulnerable to enforcement challenges under the New York Convention. In 2021, a Mexican district court enforced an arbitral award using the Kleros blockchain arbitration protocol. This marked the first instance of enforcement of such an arbitral award. The case assessed by the Mexican district court, however, is an illustration of a more hybrid approach, in which a traditional arbitrator validated the Kleros award. While such an approach may offer a temporary solution, blockchain-based systems alone seem not yet sufficient. Their current design appears to lack the safeguards necessary to ensure fairness, transparency, and enforceability across jurisdictions.

By contrast, traditional "off-chain" arbitration remains a more robust and reliable mechanism for resolving international commercial disputes. Institutional arbitral procedures provide clear rules, enforceable procedural rights, and established standards for selecting arbitrators. These features instil confidence in the process and provide courts with a solid legal basis for recognising and enforcing awards. Despite criticism regarding cost and delay, traditional arbitration maintains its legitimacy by consistently upholding the fundamental due process guarantees embedded in international law.

In summary, while decentralized arbitration platforms such as Kleros represent an innovative technological development, they currently fall short of the procedural safeguards required by the New York Convention. Until such platforms incorporate mechanisms for notice, reasoned decisions, and impartial adjudication or are supplemented by conventional oversight, traditional arbitration remains the preferred option for parties seeking enforceable and procedurally sound outcomes in cross-border disputes.

***Katharina Michl** is an associate at Schoenherr Attorneys at Law, a full-service commercial law firm with offices across Central and Eastern Europe. Based in the Vienna office, her practice focuses on international arbitration, particularly in the field of commercial arbitration. She has also served as a tribunal secretary in commercial arbitration proceedings.*

***Masa Samardzic** is an international associate at Schoenherr Attorneys at Law, a full-service commercial law firm based in Central and Eastern Europe. Based in the firm's Vienna office, her practice focuses on international arbitration, with a particular emphasis on commercial disputes.*
She holds a specialized academic background in European and international business law, and she is set to further her expertise by pursuing a specialization in Investment Funds Law in Luxembourg.

Blockchain Arbitration – Legal Analysis

By Pedro Lacasa & Brenda Copani

Introduction

The impact of technology in the field of International Arbitration (as a mechanism for resolving disputes arising from international trade) has been the subject of an unprecedented increase after the COVID-19 pandemic, whose consequences at times left the borders of several states closed, airports empty or shut down, and trips canceled.

The application of technologies supported by Blockchain in the execution of international contracts is rapidly growing, and the proliferation of smart contracts is undeniable (although many authors argue that these smart contracts are, in essence, merely pieces of software code).

The adjudication of commercial disputes as a private adjudication (especially International jumped onto the DLT (distributed ledger technology) revolution.

Currently, multiple mechanisms of "decentralized justice" are being developed, among them Blockchain Arbitration (or arbitration in blockchain). Digital platforms like Kleros, Jur, and Aragon offer arbitration services.

Lack of clarity and no legal basis in relevant definitions

Even though the term "arbitration" in blockchain could lead to misunderstandings in the future, this dispute resolution mechanism through blockchain, still in its early stages, has an imprecision regarding several fundamental aspects in international arbitration:

1. The seat of arbitration
2. The law applicable to the arbitration process
3. The international circulation of arbitral awards

The legal framework of international arbitration is built on the basis of the territorial sovereignty of States. Legal institutions such as the *lex arbitri* (the law of the place of arbitration), the *situs* of arbitration, and state intervention in all phases of an international arbitration (pre-award and post-award) have a direct impact on the final judgment resulting from the arbitration process.

On this basis, it makes no logical sense to claim that a dispute resolution service provided digitally through blockchain—characterized by decentralization—could fit within a legal framework designed to preserve the territorial sovereignty of States in the international order.

A lot of emphasis is being placed on the theory of "Autonomous Arbitration" as a prelude to what blockchain arbitration proposes. However, to date, there is no solid theory on "Autonomous Arbitration". In fact, it seems to be an embryonic intellectual development based on the theory of delocalization. This latter proposal advocates for the autonomy of arbitration, mainly in the pre-enforcement phase of the award, with its leading exponents being of European origin and its judicial recognition found in the French *Cour de Cassation*.

In other words, the theory of delocalization has existed for many decades and is already established in a national judicial system (the French one). The idea of "Autonomous Arbitration" emerged around 2006, preceding a publication that offered the most comprehensive academic treatment of the theory of arbitration delocalization in 2008 (Gaillard, Emmanuel, *Aspects philosophiques du droit de l'arbitrage international*, Martinus Nijhoff).

This development occurred long before the release of Satoshi Nakamoto's Bitcoin whitepaper and well before the concept of Web3 was even conceived.

The Seat: Schrödinger's Cat of Arbitration - Between the Blockchain World and the "Real World".

It is argued that arbitrations conducted on blockchain lack a fixed seat of arbitration, meaning they cannot have a precise and localized place where the arbitration process is conducted.

Even so, some pioneering regulations on this subject, such as the *Digital Dispute Resolution Rules* of the *United Kingdom Jurisdiction Taskforce*, supported by the CEOs of Kleros, Jur, and Mattereum, prescribe the designation of an arbitral seat. In this case, the seat will be in England and Wales and the law applicable to the arbitration will be English law.

However, it seems that everything described above tends to be just a "cool" variant of international arbitration (still involving state intervention), rather than a truly "*autonomous*" transnational arbitration mechanism completely detached from State-intervention.

Considerable attention has been given to a Mexican court's decision to enforce an arbitral award issued through a blockchain protocol—commonly referred to as a Blockchain Arbitral Award—based on Kleros in a residential lease dispute.

Nevertheless, the arbitration clause in the lease contract, despite referencing Kleros as a provider of decentralized justice services, expressly states that "the arbitration will take place in Guadalajara, Jalisco" [sic].

Not to mention the fact that the sole arbitrator designated by the parties in the contract was a person perfectly identifiable in advance (a law graduate from the Institute of Alternative Justice of the State of Jalisco with a certification number stated in the arbitration clause), in lieu of the *random* selection system of Kleros, by which the "jurors" responsible for dispensing justice are appointed according to the amount of staked (or invested) tokens. This reflects that the parties implicitly favor a certification number granted by a State over a random selection system.

The Recognition and Enforcement of Foreign Arbitral Awards: The Problem of the Law of the Seat

The process of recognition and enforcement of arbitral awards (regardless of whether they are characterized as foreign, international, or transnational) is a court procedure established under the national laws of international arbitration in most countries and also provided for in the 1958 New York Convention.

Many provisions of the New York Convention on the enforcement of foreign arbitral awards prioritize the law of the place where the arbitration was conducted (*lex arbitri*). However, if blockchain arbitration is conducted in cyberspace—through computational codes operated by "jurors" or arbitrators located in different geographical locations—it is evident that it neither has, nor can have, a seat (i.e. a territorial jurisdiction where the arbitration process is conducted) serving as the legal connecting factor between the arbitral process and a specific country. It could not, therefore, have a *lex arbitri* either.

It is noteworthy that the vast majority of national arbitration laws require the existence of a "territorial connecting factor" with the State that enacted such laws. For example, Article 1 of the Argentine Law No. 27,449/2018 on "International Commercial Arbitration" expressly states that:

"*The provisions of this law shall apply only if the seat of the arbitration is located within the territory of the Argentine Republic*."

If an arbitration is conducted on the blockchain and not within Argentine territory, Argentine Law No. 27,449 immediately does not apply, as expressly mandated by its Article 1. Almost all national arbitration laws share this rule, which seeks to uphold the primacy of State sovereignty through the application of domestic law.

In the case of Argentina, if a blockchain arbitration does not have its seat within Argentine territory, Law No. 27,449 does not apply, and consequently, the arbitration process may lack an applicable law. Given this, if an arbitration proceeding that culminated in a final award never had an applicable law governing the process, how can it be expected that such an award would be enforced in another State, which would apply its own national arbitration laws and the provisions of the New York Convention?

Certainly, this question has been addressed previously through the foundational principles of the delocalization theory, whose judicial recognition is well established, as exemplified by the Hilmarton and Putrabali cases decided by the French *Cour de Cassation*, where French law was preferred over the provisions of the New York Convention.

However, the theory of delocalization remains a minority position within the current international arbitration framework, both among scholars and judicial authorities.

Therefore, with localization being the rule, how can the philosophy of "blockchain arbitration" be reconciled with the current international legal framework? Some authors argue from the outset that there is a manifest incompatibility between the new (blockchain arbitration) and the old (the legal framework dating from the second half of the twentieth century that currently governs) .

However, the support of various blockchain arbitration platforms for arbitration regulations and judicial decisions based on the pillars of the old legal framework suggests otherwise.

Final Considerations

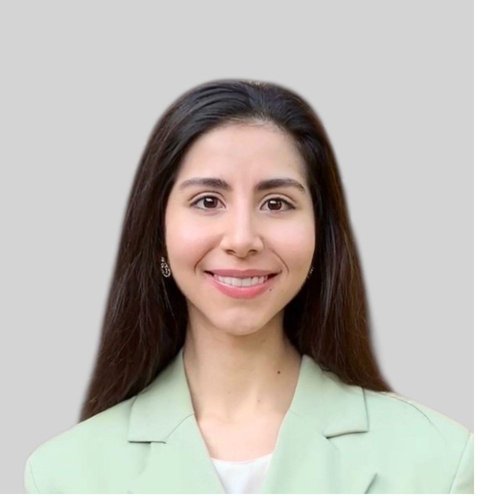
After this legal analysis of blockchain arbitration, the following questions arise, though they remain unanswered. In the realm of international arbitration, it is more important to ask the right questions first:

1. How can an arbitral award be enforced by the courts of another state if that state's law requires a territorial connection to the arbitration?
2. Expanding on the previous question: what criteria should be used to define an "international" dispute, when the proceedings occur entirely in cyberspace?
3. If blockchain arbitration utilize self-executing smart contracts, what then is the rationale for resorting to the international legal framework, such as the New York Convention, to seek judicial enforcement of an arbitral award?
4. In the event that the funds allocated in a blockchain arbitration smart contract are insufficient to satisfy the arbitral award rendered in that arbitration process, to what extent can recourse be made to seek the enforcement of the award in a domestic court? (consider this question along with questions 1 and 2).

As the reader may notice, this world of arbitration in blockchain raises more questions than answers. However, the questions raised by this new dispute resolution mechanism are valid and will arise sooner rather than later in the courts. Their response, despite the silence from academia and judiciaries, remains to be seen.

Pedro Lacasa
Lawyer (Universidad Nacional de Asunción, 2013); Master in Private International Law (Université Paris II Panthéon Assas, 2016); Master in corporate law (Universidad Católica de Asunción, 2020); LLM candidate (Université Paris II Panthéon Assas 2024-2025)

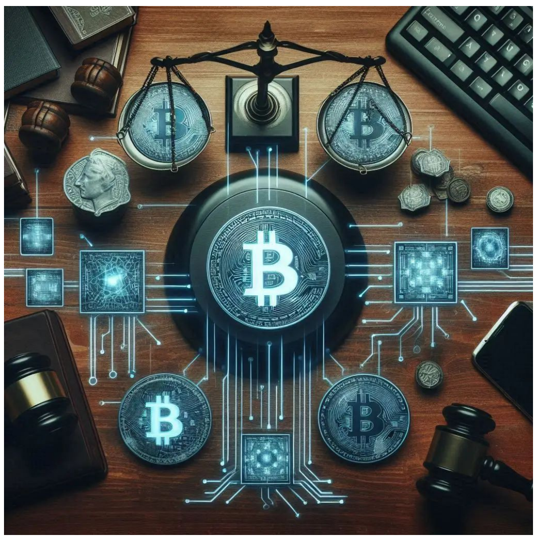
Brenda Copani
Attorney at Law (Universidad Católica Nuestra Señora de la Asunción, 2023), with experience in corporate law, dispute resolution, technology and energy law. BLF Hub Leader for Paraguay (2025).



Which Disputes for Decentralized Justice? A Functional Typology of Cases Fit for Blockchain-Based ADR/ODR Platforms

By Mohammad Hossein Heidarpour (PH.D Researcher, University of Lausanne, BLF Arbitrator List)

Abstract:
This article explores the limits and potential of decentralized dispute resolution platforms by developing a functional typology of disputes that are suitable for resolution in such environments. While these blockchain-based systems promise low-cost, transnational and automated justice, they are not universally applicable to all kinds of legal conflicts. The article classifies disputes across several axes, including their legal nature (commercial vs non-commercial), complexity and value (small vs large), digital context (on-chain vs off-chain), procedural structure (simple vs fact-intensive) and party configuration (bilateral vs multilateral). Each category is evaluated in light of enforceability, procedural fairness and compatibility with smart contract. The analysis reveals that while many disputes, especially those arising from digitally native transactions, may be apt for such platforms, others raise serious concerns regarding due process, public policy, and legal recognition and enforcement of awards or decisions. The article proposes a set of suitability criteria and emphasizes the need for hybrid or adaptive procedural models. This typology contributes to the growing academic and regulatory discourse on decentralized justice and offers guidance for platform designers, policymakers, and legal scholars.



1. Introduction

The emergence of blockchain-based dispute resolution platforms has raised numerous legal questions that continue to be examined with growing attention by scholars at the intersection of technology and dispute resolution. One such critical question concerns the types of disputes that are suitable for submission to these decentralized platforms. While these mechanisms offer innovative procedural advantages, it is clear that not all disputes possess the legal or technical aptitude to be effectively resolved through such novel systems.

This paper adopts a legal and functional analytical approach to clarify this ambiguity by proposing a structured categorization of disputes along five distinct axes. Each category is assessed against a set of suitability, regulatory and technical criteria to determine the extent to which it can be managed by decentralized justice platforms. In cases where a dispute type fails to meet these thresholds, two outcomes are considered: either the matter must be referred to traditional forums of adjudication (on-chain resolution included), or it may be resolved through a hybrid mechanism combining elements of both decentralized and conventional dispute resolution models.

1.1 Context and Problem Statement

Over the past decade, blockchain technology has moved from a niche innovation to a foundational infrastructure in sectors ranging from finance to governance. Within this shift, decentralized dispute resolution platforms, notably Kleros, have emerged as novel tools aimed at addressing disputes in a decentralized, autonomous, and cross-border fashion. These platforms promise low-cost, efficient, and transparent processes, often involving smart contracts, oracles and crowdsourced jurors.

Despite their technological appeal, these mechanisms raise a pressing legal question: Which types of disputes are legally and practically suitable for such platforms? This question has gained relevance as decentralized platforms seek recognition not only within crypto-native communities but also in broader regulatory and judicial systems. However, the boundaries of their legal applicability remain unclear, particularly with regard to arbitrability, procedural fairness and the enforceability of outcomes.

Thus, the central problem this paper seeks to address is the lack of a structured, functional classification of disputes appropriate for resolution by blockchain-based ADR/ODR platforms. Without such a framework, users, developers and regulators face uncertainty about the proper scope and legal viability of decentralized justice systems.

1.2 Structure of the Paper

This paper is organized into six sections, following a logical progression from conceptual foundations to applied legal analysis. After the introduction, which outlines the context and problem statement, the second section provides a technical and legal overview of decentralized dispute resolution platforms. It explains their core procedural features, underlying technologies and how they can be differentiated from traditional ADR/ODR mechanisms, thereby laying the groundwork for the typological analysis that follows.

The third section constitutes the analytical core of the paper. It develops a functional typology of disputes across five axes: legal nature, scale and complexity, digital context, procedural structure and number of disputants. Each category is examined in light of its legal and technical suitability for resolution on decentralized platforms.

The fourth section proposes a set of evaluation criteria, both legal and technical, to assess whether a given dispute type may be appropriately resolved through blockchain-based mechanisms. It also considers the extent to which current regulatory frameworks can accommodate such platforms.

The final section concludes the paper by summarizing the main findings, highlighting the normative and practical relevance of the proposed typology, and identifying areas for further research and regulatory development.

2. Decentralized Justice Platforms: Conceptual and Technical Framework

2.1. Definition and Key Features

As a delimitation of this section, it should be noted that the analysis presented herein is primarily grounded in the structure and operational model of Kleros, the first and most well-known decentralized dispute resolution platform, which remains at the center of attention in legal tech scholarship. The paper focuses on Kleros to outline the key definitions, fundamental mechanisms, juror incentivization processes, and decision-making procedures that characterize decentralized justice. Other emerging models of private digital adjudication, although conceptually related, are excluded to the extent that their design diverges significantly from the Kleros framework and falls outside the scope of the issues addressed in this study. Nonetheless, the general observations and typological analysis proposed in the following sections remain applicable to the broader category of decentralized justice platforms, even when these newer platforms have not yet reached the level of maturity or prominence necessary to warrant their own systemic treatment.

Decentralized dispute resolution platforms are blockchain-enabled, on-chain systems to which parties may refer specific disputes for settlement and final determination. These platforms function through mechanisms such as juror crowdsourcing, whereby randomly selected and anonymous participants adjudicate cases in a binary format (e.g., yes/no, win/lose). The adjudication process is further structured through game-theoretic incentives, particularly the Schelling Point theory, which encourages jurors to vote in alignment with what they believe others will choose. Jurors are typically required to stake platform-specific tokens in advance, and they are rewarded or penalized based on the extent to which their decisions align with the majority, thereby reinforcing consistency and discouraging manipulation.

2.2 Distinction from Traditional ADR/ODR

One might consider, first, the common grounds of both decentralised platforms and the traditional ADR/ODR platforms. The decentralised platforms share some basic elements with classic ADR/ODR mechanisms required for constitution of a simple private adjudication. To name a few, non-judicial nature, party autonomy, efficiency and flexibility goals and the potential for rendering binding decisions or awards can be observed in each method. The establishment of a virtual platform on the headstock of the internet is another existing similarity between decentralised and the more well-known ODR settlement. However, these assimilations come to an end once the decision making process of each category concerns whether a decentralized or centralized approach is adopted.

The traditional ADR/ODR platforms and the decentralized ones are distinguished, however, in several critical aspects; namely, the mode of governance (centralized institutional oversight versus distributed, protocol-based systems), the anonymity and crowdsourcing of adjudicators (where traditional systems rely on appointed and identifiable arbitrators or mediators, while decentralized platforms engage pseudonymous jurors selected algorithmically), and the integration of blockchain infrastructure and crypto-economic incentives. Unlike conventional mechanisms, decentralized platforms utilize smart contracts and game-theoretic models, to guide juror behavior, replacing legal ethics and professional standards with incentive engineering. Moreover, procedural guarantees that are standard in traditional ADR, such as the right to be heard, the ability to present evidence, or to appeal decisions, are often absent or structurally modified in shape and formalities in decentralized systems. This leads to legitimate concerns regarding fairness, due process, and legal defensibility. Additionally, the recognition and enforcement of decisions marks another key difference: while traditional arbitral awards benefit from established frameworks like the New York Convention, the enforceability of blockchain-based outcomes remains uncertain as far as off-chain recognition and enforcement of the awards are concerned, often relying on reputational pressure or voluntary compliance rather than formal legal remedies. These cumulative distinctions shape the legal, practical, and ethical boundaries of decentralized dispute resolution in contrast to its traditional counterparts.

2.3 Legal and Procedural Constraints

This section moves the discussion from functional and structural comparisons to the core legal challenges that decentralized platforms face in real-world application. While the promise of low-cost, efficient, and borderless dispute resolution is compelling, these mechanisms encounter several legal and procedural hurdles that cannot be overlooked.

First, one of the primary issues is the absence of legally binding procedural safeguards. Unlike traditional ADR, decentralized platforms often lack codified rules of procedure governing the conduct of proceedings, admissibility of evidence, timeframes and the right to representation. This can raise concerns about the integrity of the process and the protection of parties' fundamental procedural rights, particularly in disputes that involve asymmetrical power relationships, or multilateral counterparty arrangements with more than two disputants or even third parties.

Second, the anonymized nature of jurors and the absence of identifiable decision-makers make it difficult to guarantee accountability, which is a cornerstone of any legitimate dispute resolution process. There is no mechanism to challenge herd behavior, bias (particularly in cases where certain professions or business are involved), conflict of interest, or procedural irregularities in a meaningful way. While the logic of decentralization aims to reduce central control and improve impartiality, it may paradoxically undermine procedural legitimacy when parties are left without recourse to due process measures indispensable for securing a fair trial.

Finally, there are inconsistencies between these emerging systems and existing legal orders. Courts or state institutions asked to recognize or enforce decisions from such platforms may question whether the process meets minimum standards of due process, including the right to be heard and the impartiality of decision-makers, let alone the evidence taking process and matters of legal jurisdiction and competency. Without a reliable link to jurisdiction, or a clear legal basis for authority and enforcement, these platforms remain in a legal gray area, particularly when the disputes involve parties from different national systems with varying degrees of openness to technological innovation in legal processes.

In summary, while decentralized platforms offer a novel procedural framework, they currently lack many of the legal assurances that make dispute resolution both credible and enforceable.

3. Typology of Disputes: A Functional Approach

This section proposes a functional typology of disputes suitable for resolution through decentralized blockchain-based platforms. Rather than adopting a purely doctrinal or technological lens, the approach here is grounded in practical suitability, evaluating the legal, procedural, and technical characteristics that make certain categories of disputes more apt for such mechanisms. By examining disputes through axes such as legal nature, monetary value, digital context, procedural complexity, and number of parties involved, the aim is to provide a structured framework to assess which types of cases decentralized platforms can realistically and legitimately handle, and under what conditions.

3.1 By Legal Nature: Commercial vs Non-Commercial Disputes

Before delving into the specific merits of commercial versus non-commercial disputes, it is essential to address whether non-commercial disputes are, in principle, referable to decentralized platforms at all. In many jurisdictions, the question of arbitrability serves as a threshold criterion, determining which types of disputes can be validly submitted to alternative forums such as arbitration or ADR. Non-commercial disputes, particularly those involving family law, status-related claims (e.g., citizenship, capacity), or certain public interest matters are often considered non-arbitrable due to their close connection to the state's sovereign interests or the need for judicial oversight. These disputes are typically viewed as falling within the exclusive jurisdiction of national courts.

Article V(2)(a) of the New York Convention allows a court to refuse the recognition and enforcement of an arbitral award if the subject matter of the dispute is not capable of settlement by arbitration under the law of the country where enforcement is sought. This provision reflects a longstanding principle in international arbitration: that certain disputes are non-arbitrable due to their inherent public interest character or because they implicate exclusive state authority. Conventional examples of non-arbitrable matters include categories such as criminal disputes, family law matters (e.g., custody or divorce), bankruptcy proceedings, antitrust and competition law claims, employment grievances, sanctions, and aspects of intellectual property disputes involving validity or registration. These disputes are often seen as involving fundamental rights or regulatory frameworks that demand state supervision and judicial adjudication.

Transposing this logic to decentralized dispute resolution platforms, which may be seen as derivative or “deviated” forms of arbitration, it would follow that the same categories of non-arbitrable disputes would not be appropriately referable to such platforms, especially where enforcement in a national court system is anticipated. However, this conclusion depends on how we legally characterize these mechanisms. If we adhere to the premise that blockchain-based platforms are not arbitration in the classic legal sense, and instead view them as private, self-enforcing systems of dispute resolution, different standards may apply. Provided that party autonomy is respected, and all aspects of the dispute, including enforcement, occur within a purely on-chain environment, there may be no legal barrier to referring even traditionally non-arbitrable matters to these platforms. In such cases, the dispute would be governed by smart contracts, and outcomes would be executed automatically via crypto-economic mechanisms (e.g., token release or digital asset transfer), making court enforcement unnecessary and legal arbitrability rules arguably inapplicable. This interpretation aligns with the emerging doctrine of blockchain self-regulation, which posits that decentralized systems may constitute autonomous normative environments capable of operating outside the traditional constraints of state-based legal frameworks, especially when confined to digitally native contexts.

In contrast, commercial disputes, which involve contractual or transactional relationships between private parties, are widely considered arbitrable and are often undoubtedly suitable for out-of-court resolution, provided that party consent and minimum procedural standards are respected.

With this background, decentralized platforms appear more appropriately tailored to commercial disputes, particularly those that are relatively low in value but high in volume (e.g., freelance work, e-commerce, service provision). The suitability arises from the platforms' speed, cost-efficiency, and ability to handle standardized cases through code-based procedures. However, one should not entirely exclude certain categories of non-commercial disputes, especially where consent, low stakes, and procedural simplicity align with the operational limits of decentralized systems. Still, these should be approached cautiously and likely reserved for pilot projects or hybrid mechanisms where legal enforceability and ethical oversight are ensured. Overall, while commercial disputes form the core use case for decentralized platforms, a limited and well-regulated inclusion of non-commercial disputes may gradually emerge under appropriate safeguards.

3.2 By Value and Complexity: Small Claims vs High-Stakes Disputes

Another important axis for evaluating the suitability of disputes for resolution through decentralized platforms is their monetary value and procedural complexity. Most existing platforms, such as Kleros or Aragon Court, have been primarily designed to accommodate low-value disputes that would otherwise be inefficient or impractical to pursue through traditional courts or even institutional arbitration. This includes, for example, freelance contract breaches, disputes over digital goods, or token listing conflicts, where the value at stake does not justify high legal costs, but the parties nonetheless require a reliable and timely resolution mechanism.

Small claims disputes are especially compatible with blockchain-based dispute resolution due to their standardizable procedures, low evidentiary burden, and relative simplicity. The automated nature of decentralized platforms allows for streamlined case handling and reduced human intervention, resulting in cost-effective justice delivery. Moreover, the crypto-economic design of such systems, including juror incentives and the use of smart contracts for enforcement, functions well in scenarios where efficiency and scalability matter more than full procedural elaboration.

By contrast, high-stakes or complex disputes, those involving significant monetary amounts, multi-jurisdictional issues, nuanced evidentiary assessments, or novel legal questions, pose significant challenges for decentralized systems. These cases often require procedural flexibility, expert adjudication and due process guarantees that current platforms are not yet equipped to provide. Furthermore, where reputational enforcement is insufficient or there is no on-chain remedial solution at hand, and formal recognition or enforcement by state courts is necessary, the absence of a clear legal framework and the anonymized nature of adjudication in decentralized systems can frustrate due and fair process principles, accountability and enforceability in cases where off-chain recognition is to be sought.

That said, a hybrid model could eventually emerge wherein decentralized platforms act as the first-instance mechanism for high-value disputes, followed by optional review or confirmation by more formal arbitral or judicial bodies. For now, however, the most fitting domain of decentralized justice remains small claims resolution, particularly in digitally native contexts where transactions and enforcement are self-contained within the blockchain ecosystem.

Despite the practical limitations of decentralized platforms in handling high-stakes and complex disputes, the emergence of blockchain oracles, which serve as trusted data feeds or bridges between off-chain information and on-chain smart contracts, offers new potential for expanding the scope of such systems. In complex cases involving dynamic facts, technical evidence, or real-world contractual performance, oracles can be employed to automatically verify and input external data, allowing the platform to process information that would otherwise be inaccessible or unverifiable within the blockchain environment. This capability makes it technologically feasible to adjudicate even high-value disputes, particularly where factual determinations depend on measurable and objectively verifiable data. However, the reliance on oracles introduces its own challenges, notably regarding security, data protection, manipulation risks (e.g., oracle attacks), and added costs related to oracle integration and maintenance.

Moreover, as the reliance on oracles increases in complexity, so too does the infrastructure needed to ensure reliability, accuracy, and auditability. This raises the question: if resolving a high-value dispute on a decentralized platform ultimately requires elaborate oracle inputs, multi-step verification, and protocol-level governance, what is the advantage over using conventional ADR/ODR mechanisms? The cost and time benefits typically associated with decentralized justice may erode in proportion to the complexity of the dispute, particularly where procedural safeguards, expert input, or legal certainty are necessary. Therefore, while oracles offer an important functional extension that can help accommodate complex disputes, their application must be balanced against the cost-efficiency rationale that underpins the very appeal of decentralized platforms. As such, referral of high-stakes disputes to these systems may only be justified in fully digitized ecosystems where both the dispute and its enforcement are intrinsically on-chain, and the parties prioritize automation, transparency, or ideological commitment to decentralization over traditional adjudicatory assurance.

3.3 By Digital Context: On-Chain vs Off-Chain Disputes

As elaborated earlier in this paper, one of the most fundamental criteria in assessing the suitability of disputes for resolution through decentralized platforms lies in their digital context, namely, whether the dispute is fully on-chain or involves significant off-chain elements. In the case of on-chain disputes, where all parties, transactions, obligations and evidence are embedded within a blockchain environment (such as smart contract execution failures or token-based DAO governance decisions), decentralized platforms function with optimal efficiency. This is because crypto-economy, the underlying mechanism driving blockchain systems, relies on economic incentives and automated enforcement through smart contracts, thereby reducing the need for human discretion and external verification. The determinism and transparency inherent in blockchain environments support secure, tamper-proof and rule-based adjudication that can execute outcomes directly on-chain.

By contrast, off-chain disputes, which originate in the real world, such as those involving service contracts, physical goods, or legal identities, pose challenges due to the need for off-chain fact-finding, party identification and enforceability. Nevertheless, these disputes can still be accommodated within decentralized platforms under certain conditions. One approach is through the transposition of contractual obligations into smart contracts, either at the outset or after the dispute arises. This requires that the terms be sufficiently clear, objectively verifiable and capable of being executed programmatically. Moreover, parties must voluntarily agree to submit their disputes to such platforms and recognize the binding nature of the outcome, typically enforced through reputational incentives or escrow mechanisms rather than state coercion. As such, while fully on-chain disputes remain the most natural candidates for decentralized resolution, a carefully designed procedural bridge can extend these platforms' reach into off-chain domains, provided appropriate consent, clarity, and enforcement architecture are in place, with a particular attention to the applicable law upon the contractual obligations envisaged in the underlying agreement.

3.4 By Procedural Requirements: Simple vs Fact-Intensive Disputes

When assessing the suitability of disputes for resolution via decentralized platforms, another key dimension is the procedural complexity, in particular, the distinction between simple and fact-intensive disputes. Simple disputes, such as non-payment for services rendered or minor contract performance issues, are generally well-suited to blockchain-based platforms. They involve straightforward factual scenarios, often self-contained within the blockchain environment, requiring limited evidence and procedural steps. In contrast, fact-intensive disputes often involve multiple layers of complexity and external variables that decentralized platforms are not yet equipped to manage reliably.

Such disputes may require third-party evidence, including witness statements, documentary records or data housed off-chain. They frequently necessitate expert opinions, site inspections or technical verifications that cannot be easily automated or validated through smart contracts or oracles. Additionally, certain disputes are contextually bound to ongoing or prior real-world litigation or arbitration, raising legal and evidentiary interdependencies that decentralized systems cannot effectively address in isolation. While blockchain oracles provide a potential gateway for feeding off-chain information into on-chain systems, their accuracy, cost-efficiency and reliability remain uncertain, particularly in situations demanding nuanced human judgment, case-specific analysis or interpretation of complex legal standards.

Until technological advances allow for more refined integration of off-chain information in a trustworthy, scalable and cost-effective manner, fact-intensive disputes remain largely unsuitable for resolution via decentralized platforms. This limitation, however, is not necessarily inherent to blockchain technology itself but rather reflects the current state of development. Future progress in areas like AI-integrated oracles may gradually close this gap, provided that such enhancements do not compromise the foundational principles of decentralization and autonomy.

3.5 By Number of Disputants: Bilateral vs Multilateral Disputes

The distinction between bilateral and multilateral disputes presents a significant functional boundary for decentralized dispute resolution platforms. Most existing systems, Kleros being the most prominent example, are structurally designed around binary adjudication mechanisms, where jurors must choose between clearly defined options presented by two opposing parties. This Schelling-point-based model, which leverages incentive-aligned majority voting among anonymous jurors, performs efficiently in two-party disputes where resolution hinges on factual verification or contractual clarity. However, in multilateral disputes, involving three or more parties with competing claims or overlapping interests, this model quickly encounters practical and conceptual limitations. However, it appears that effort have been made to enable the resolution of multiparty disputes.

In Kleros’s current architecture, the binary nature of juror decision-making cannot accommodate triangular or pluralistic claims, where outcomes may involve apportioning fault, determining priority or assessing cumulative liability. Such complexity undermines the feasibility of rendering a decision that reflects the diverse factual and legal positions of multiple parties, especially in non-mutually exclusive outcomes. Furthermore, multilateral disputes often require nuanced procedural coordination, such as multi-party notice, reply and rejoinder rounds, and evidence triangulation, all of which are absent or highly constrained in current decentralized platforms. These technical limitations are exacerbated by the lack of centralized case management and rigid procedural scripting via smart contracts, which do not lend themselves to adaptive adjudication.

To overcome these challenges, future iterations of decentralized justice systems could experiment with multi-option voting mechanisms or layered decision phases that permits a wider array of verdicts. Another pathway could be the development of modular dispute layers, where individual bilateral components of a multilateral dispute are adjudicated separately, followed by an integrated consensus mechanism. However, these innovations must not erode the fundamental tenets of decentralization, namely transparency, immutability and juror independence. Until such solutions are technically and economically viable, multilateral disputes remain relatively incompatible with the current design and logic of decentralized platforms.

4. Suitability Criteria and Regulatory Alignment

This section aims to articulate the fundamental criteria against which the suitability of various categories of disputes for resolution by decentralized platforms can be evaluated. Drawing from both legal doctrine and procedural logic, the analysis proceeds on the premise that not all disputes, by their nature, complexity, or regulatory context, lend themselves equally to adjudication via blockchain-based systems. Accordingly, this chapter introduces a framework composed of three interdependent dimensions: the challenges surrounding enforcement and recognition, the clarity and robustness of applicable legal frameworks and procedural design, and the technological architecture and constraints embedded in the platforms themselves. The objective is not merely to offer a taxonomical classification of referable disputes, but rather to investigate how regulatory coherence, enforceability conditions, and design limitations interact in determining whether a given dispute type can be resolved effectively and legitimately in a decentralized, on-chain environment. Of particular interest is the role of international and domestic standards, such as the New York Convention and national arbitration laws, in shaping the enforceability of decisions issued by these platforms, especially when questions of arbitrability and party consent are implicated. As such, this chapter lays the groundwork for a nuanced, criteria-based suitability analysis that complements the typological categorization developed earlier in the paper.

4.1 Enforcement and Recognition Challenges

While decentralized dispute resolution (DDR) platforms such as Kleros have introduced novel mechanisms for adjudication through blockchain-based processes, their legal status and the enforceability of their decisions remain deeply uncertain. One of the principal benchmarks for evaluating the potential recognition and enforcement of decisions rendered by such platforms is the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. Although originally intended for conventional arbitration, the Convention offers a useful analytical framework through which the legal viability of decentralized justice systems can be appraised, particularly if jurisdictions begin treating these decisions as analogous to arbitral awards.

Article V(1) of the New York Convention establishes the conditions under which recognition may be refused. These include the absence of a valid arbitration agreement in writing, lack of due notice, excess of jurisdiction and irregularities in the composition of the arbitral tribunal. Crucially, under Article V(2)(a), enforcement may be refused if the subject matter of the dispute is not "capable of settlement by arbitration under the law of that country", i.e., the arbitrability requirement. Additionally, Article V(2)(b) allows a state to refuse enforcement where it would violate the public policy of the enforcing country. These provisions pose significant challenges for DDR platforms that lack a centralized seat as the most essential element of any arbitral proceeding, institutional backing or a clearly defined legal procedure.

The requirement of a written arbitration agreement (Article II of the Convention) is particularly problematic in decentralized environments. Smart contracts embedded in blockchain protocols may reflect mutual assent, but they typically lack the formal clarity and intent-based negotiation processes expected in traditional arbitration. Furthermore, it is questionable whether the appointment of anonymous jurors by an algorithmic mechanism can fulfill the Convention's demand for a "duly constituted arbitral tribunal."

Despite these formal gaps, certain jurisdictions have started to display legal flexibility. For instance, the Mexican courts have recognized and enforced a decision rendered by Kleros in a landlord–tenant dispute, signaling an openness to treating platform-based adjudications as enforceable outcomes when they meet minimum standards of procedural fairness and party consent. This case sets a potentially influential precedent and demonstrates that national courts may, over time, expand their interpretation of enforceable decisions to include technologically derived rulings, particularly when aligned with domestic ADR principles.

In practice, even where full arbitral recognition is not attainable, DDR decisions can serve as pre-arbitral or pre-litigation procedural requirements. Parties may agree contractually that such decisions act as a condition precedent to initiating state proceedings or arbitration, akin to multi-tiered dispute resolution clauses (e.g., negotiation, then mediation, and then arbitration). Alternatively, these decisions may be framed as contractual determinations, obliging the losing party to perform a specific act (e.g., repay funds, release tokens, or deliver goods). In such cases, failure to comply with the DDR decision may give rise to a new cause of action, allowing the prevailing party to request specific performance or damages before a national court.

Nonetheless, the public policy exception remains a considerable hurdle. Decisions rendered without respect to adversarial principles, due process, or transparency, such as lack of opportunity to present a defense, unknown adjudicator identities, or opacity in procedural rules, may be struck down by state courts. Moreover, the anonymity of parties, difficulty verifying identity, and lack of formal procedural safeguards further undermine enforceability in many jurisdictions. Unless DDR platforms can demonstrate procedural integrity, transparency, and compliance with minimal standards of justice, they will continue to face challenges in achieving recognition as legitimate dispute resolution mechanisms under both domestic and international law.

4.2 Clarity of Legal Frameworks and Procedural Design

A key determinant of whether decentralized dispute resolution (DDR) mechanisms can be considered suitable substitutes or complements to traditional adjudicative systems lies in the clarity, coherence, and legal validity of their procedural frameworks. In traditional arbitration or court-based mechanisms, procedural design is anchored in codified norms, whether national civil procedure rules or institutional arbitration rules, which ensure predictability, legal certainty, and compliance with fundamental procedural guarantees. In contrast, many blockchain-based platforms operate within technologically programmed and self-executing procedures, often governed by protocols developed unilaterally or through decentralized communities, without clear links to national legal orders. This raises profound concerns about their legal intelligibility, the enforceability of their outcomes, and their conformity with internationally accepted standards of justice.

One of the primary shortcomings in current DDR procedural design is the absence of universally recognized rules of procedure. While platforms like Kleros provide documentation outlining their process, including evidence submission, juror selection and voting mechanics, these protocols do not correspond to established procedural norms recognized under domestic arbitration laws or international frameworks such as the UNCITRAL Model Law. Moreover, the static and code-dependent nature of smart contract-based adjudication restricts flexibility in procedural management, there is typically no provision for motions, hearings or procedural discretion. This rigidity may severely affect the ability to deal with complex fact patterns or procedural incidents such as joinder, interim measures or bifurcation.

In addition, the legal qualification of such procedures remains unsettled. Are they arbitration, contractual adjudication or sui generis mechanisms of private ordering? The uncertainty surrounding their classification makes it difficult for parties, counsel, and courts to determine the consequences of participating in such processes or challenging their results. This ambiguity may discourage parties from engaging DDR platforms, particularly in cross-border disputes where procedural clarity is essential to secure recognition.

For DDR systems to gain legal credibility, they must evolve towards transparent, well-documented and legally interoperable procedural schemes. This might include aligning core steps with those recognized in arbitration (such as notice, opportunity to respond, impartial decision-making), integrating adaptable procedural layers through governance modules or developing "legal wrappers" around the protocol that allow courts to identify the procedural legality of decisions rendered. Without such alignment, DDR platforms risk being perceived as opaque or arbitrary, limiting their acceptance in both private contracts and public enforcement regimes.

4.3 Technological Constraints and Platform Design Considerations

Beyond legal frameworks, the architecture and operational logic of blockchain technology itself present fundamental constraints on the full delivery of justice through decentralized dispute resolution (DDR) platforms. While blockchain enables core features such as transparency, automation and tamper-resistance, it simultaneously introduces structural limitations that complicate compliance with traditional principles of fairness, accountability and procedural integrity.

One significant challenge is the immutability of the blockchain ledger. Once decisions are recorded and executed via smart contracts, they are practically irreversible, regardless of procedural errors, new evidence or changes in legal interpretation. Moreover, the anonymity or pseudonymity of participants, both disputants and jurors, creates obstacles for ensuring impartiality, verifying identity and detecting conflicts of interest. Jurors in platforms such as Kleros operate under pseudonyms and are incentivized to vote with the perceived majority through token-based reward systems, a model that is vulnerable to herd behavior and informational cascades. These dynamics may undermine truth-seeking and instead promote conformism, particularly in fact-sensitive or morally complex cases.

The gamification of adjudication via staking tokens and probabilistic selection raises additional concerns about the seriousness with which jurors treat their role. In systems where jurors are rewarded or penalized depending on their alignment with majority outcomes, incentives may prioritize economic gain over legal reasoning. This creates the risk of a system that optimizes for consensus rather than correctness, especially when cases lack objectively verifiable outcomes.

Further, blockchain platforms lack procedural flexibility. The code-based nature of smart contracts inhibits discretionary adaptation, making it difficult to accommodate exceptions, nuanced argumentation or evolving legal interpretations. This rigidity limits their ability to adjudicate multifaceted or precedent-sensitive disputes. Also, the absence of clear mechanisms for joinder of parties, interim relief, document authentication or evidentiary standards restricts their applicability to more complex scenarios.

Finally, the business models of most platforms are designed to favor volume and low-cost resolution rather than jurisprudential robustness. In pursuing scalability, platforms may forgo procedural sophistication or robust checks and balances, making them poorly suited for disputes that demand legal precision or substantive justice. Without addressing these foundational constraints, blockchain-based DDR platforms risk remaining peripheral to mainstream legal practice, confined to narrow use-cases where procedural and substantive stakes are relatively low.

5. Conclusion

5.1 Summary of Findings

This article has offered a functional and critical analysis of the types of disputes that may be appropriately referred to decentralized dispute resolution (DDR) platforms, such as Kleros. Through a typology-based approach, it has become evident that the suitability of disputes for decentralized resolution depends not solely on the subject matter or value of the claims, but on a multifaceted combination of legal, procedural and technological criteria.

First, the legal nature of disputes significantly impacts their referability. While most commercial disputes, particularly those governed by smart contracts and involving digitally native transactions, are well aligned with blockchain-based systems, non-commercial disputes, especially those touching on public order or requiring state intervention, remain outside the practical and legal scope of DDR platforms. This distinction stems not only from arbitrability constraints embedded in national laws and international instruments such as the New York Convention, but also from the inherent limitations of party consent and enforceability frameworks.

Second, disputes characterized by low monetary value and low complexity, such as microtransactions or binary content moderation claims, are demonstrably better suited to decentralized platforms. In contrast, high-stakes or fact-intensive disputes raise concerns about procedural sufficiency, evidentiary reliability, and adjudicative depth, especially in the absence of mechanisms expert determination, or cross-examination.

Third, the dichotomy between on-chain and off-chain disputes has emerged as crucial. Fully on-chain disputes, embedded in crypto-native ecosystems, benefit from cryptoeconomic incentives and self-enforcing smart contracts. However, off-chain disputes involving real-world contractual interpretation, identity verification or asset recovery still struggle to meet the technical and procedural demands of blockchain-based resolution.

Finally, the article has underscored the legal and technological constraints that shape the limits of these platforms. Issues such as the rigidity of procedural design, the anonymity of jurors, gamified voting mechanisms, and the absence of institutional safeguards illustrate the current gap between decentralized justice and the standards of due process and legal certainty recognized in national and international legal orders.

Collectively, these findings suggest that DDR platforms can serve as effective complements to existing systems, particularly in digital-native, low-value or high-volume environments, but are not yet positioned to serve as full substitutes for traditional adjudication in complex or sensitive legal contexts. Further legal harmonization, procedural development and technological refinement are necessary before they can become integral to mainstream dispute resolution.

5.2 Implications for Research and Platform Development

The analysis presented in this paper suggests several avenues through which decentralized dispute resolution platforms can evolve to meet recognized due process standards and thereby enhance their prospects for recognition by state judicial authorities. One key development would be the integration of multi-layered adjudication mechanisms, such as peer review stages, to allow for corrective procedures and mitigate risks of erroneous or biased decisions. This could be accompanied by preparatory phases wherein disputes are clarified, evidence is organized, and procedural steps are standardized before the final deliberation, fostering both transparency and procedural rigor.

Moreover, platforms should invest in developing interoperable legal-technical tools to overcome blockchain's inherent limitations, such as pseudonymity, immutability, and lack of evidentiary discretion. These tools might include identity-verification layers, secure evidence-upload protocols, and real-time communication frameworks. Lastly, embedding programs that transcribe smart contracts into legally coherent plain-language texts (and vice versa) can enable clearer understanding for users while enhancing legal reliability, ensuring greater legal certainty and enforceability across jurisdictions.

5.3 Areas for Further Exploration

Future research should further investigate the intersection between decentralized adjudication models and national enforcement systems, particularly in mixed legal traditions. A deeper empirical assessment of user trust, procedural transparency and effectiveness of outcomes is also essential. Additionally, technical aspects such as AI-supported reasoning in dispute resolution, and the integration of legal ontologies into smart contract design, merit closer examination. As decentralized platforms evolve, cross-disciplinary studies involving law, computer science, and behavioral economics will be crucial to understanding how digital justice can be both scalable and legally robust without compromising fundamental rights and procedural integrity, while maintaining the core characteristics of blockchain to preserve its advantages over traditional ADR/ODR systems and thereby justify its superiority from the disputants' perspective.

Mohammad Hossein Heidarpour is a *PH.D. researcher at University of Lausanne, Head of the Department of Legal Technology at SMB International Law Firm, Geneva, Attorney at law, Iran Central Bar, BLF Arbitrators List, Startups Legal Advisor.*

Navigating Crypto Asset Disputes in Singapore: Legal Trends and Enforcement Challenges

By Lin Shumin & Arushee Bhatnagar

Executive summary

As use of cryptocurrency becomes more commonplace, courts in Singapore are actively developing legal principles around cryptocurrencies. The general trend in recent cases shows that the Courts are streamlining an approach to issues such as ownership**,** custody, and tracing of digital tokens. These also bring with them complex enforcement challenges.

Cryptocurrencies are property

Singapore courts treat cryptocurrencies as a recognisable form of property. In the case of *CLM v CLN and others* [2022] 5 SLR 273 ("***CLM v CLN***"), the High Court dealt directly with the issue of whether stolen cryptocurrency could be subject to a proprietary injunction.
In that case, the plaintiff discovered that his BTC and ETH holdings had been wrongfully transferred to wallets controlled by unknown individuals. He sought to freeze and recover 109.83 BTC and 1,497.54 ETH. The Court granted both a proprietary injunction and a worldwide Mareva injunction, confirming that:

a) Cryptocurrency constitutes property under Singapore law.
b) Owners of misappropriated crypto can assert proprietary rights over the assets.
c) Courts will protect these rights using existing legal tools such as injunctions.

The Court held that cryptocurrencies were deemed "property" in the legal sense under the *Ainsworth* framework from *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 at 1248. The *Ainsworth* framework establishes that for something to be considered property, it must be:

a) Definable;
b) Identifiable by third parties;
c) Capable in its nature of assumption by third parties; and
d) Have some degree of permanence or stability."

In *CLM v CLN*, the Court found that cryptocurrencies satisfied all the above requirements. This case marks a significant step in how Singapore courts view custody and legal ownership of digital tokens.

Practical hurdles of enforcing judgments overseas

Even with legal recognition of crypto ownership, however, practical enforcement remains difficult. Cryptocurrency assets are easily moved, often held by entities in foreign jurisdictions, and transacted across multiple platforms. All these issues make tracing the flow of funds much more difficult.

Cryptocurrency service providers are often based overseas. Determining whether a wrongful act occurred in or outside Singapore affects which laws apply to the dispute. (*Rickshaw Investments Ltd v Nicolai Baron von Uexkull* [2007] 1 SLR(R) 377). A single legal claim may span multiple jurisdictions.

Reaching out to crypto exchanges

The Singapore law enforcement authorities typically make direct requests to crypto exchanges, to freeze the funds and for the disclosure of information. The Singapore Police Force ("***SPF***") works with the various cryptocurrency exchanges based locally and abroad to investigate cryptocurrency crimes.

However, not all crypto exchanges may comply, and in any case, the SPF is not obliged to provide the information obtained to the victims. Hence, victims may need to obtain a court order to compel disclosure of information or for other actions to be taken.

Navigating Crypto Asset Disputes in Singapore: Legal Trends and Enforcement Challenges

Enforcing Judgments Across Borders

Obtaining a judgment in Singapore is only the first step. Enforcement in a foreign country depends on the laws of that jurisdiction. Conversely, if a judgment is secured overseas, enforcement in Singapore is only possible under common law if it is a foreign money judgment, i.e. a judgment for a definite sum of money. (*Poh Soon Kiat v Desert Palace Inc* [2010] 1 SLR 1129).

If a judgment has been obtained, the client can directly enforce judgment in the foreign jurisdiction where the crypto exchanges are located. It would then be necessary to hire local counsel to enforce the judgment in that particular jurisdiction. The High Court in *Bybit Fintech Ltd v Ho Kai Xin* [2023] 5 SLR 1748 observed that the procedures for serving a notice of seizure on persons are logically extendable to cryptocurrency or other digital currency.

However, the client would need to be aware that the crypto exchange might not cooperate, and that they may have to adopt other strategies to secure compliance with such court orders.

Enforcement applicants must also be careful in determining which entity the court papers are served on. The entity which operates the platform and holds the platform's assets may not be the holding company which is more commonly known.

Enforcement applicants should also be aware that certain jurisdictions will only enforce a judgment on the merits, and not judgments obtained in default. For example, India does not recognize a foreign judgment as being conclusive, if it has not been given on the merits of a claim (*UCO Bank, Singapore Branch v Green Mint Pte Ltd* [2023] 5 SLR 709 at [2]).

Freezing Assets and Tracing Stolen Crypto

Even with a court order, freezing and tracing crypto assets is challenging:

a) Crypto is pseudonymous, making it hard to link wallets to real identities.
b) Funds can be split, mixed, or laundered across multiple wallets or platforms.
c) Exchanges involved may be uncooperative or based in jurisdictions with limited legal assistance frameworks.

In *CLM v CLN*, the plaintiff was able to use blockchain records to trace transfers and identify wallets held by two crypto exchanges. However, not all victims will have access to such clear data. Where suspicions of wrongdoing arise, victims may need to engage forensic experts to trace funds and produce evidence of fraud or misappropriation.

Conclusion

Singapore courts recognize cryptocurrencies as property, allowing owners to protect their rights through legal action. However, recovering stolen cryptocurrencies and digital assets remains difficult due to its global, anonymous, and complex nature. Successful enforcement often requires cross-border cooperation, expert tracing, and navigating different legal systems.

Lin Shumin (Director) *has an active disputes practice and is experienced in complex contractual disputes, shareholder's disputes, company law issues, and tortious actions. Shumin has acted for a wide range of clients from various industries before the Singapore Courts and in international arbitrations. This includes acting for companies in the web3, retail, hospitality, and shipping industries as well as venture capitalists and high net-worth individuals.*

Arushee Bhatnagar *is a senior associate, who has assisted in several high-value international arbitrations and litigations. She also regularly assists in advising web3 companies on a variety of issues including employment disputes, breach of duty claims by users, fraudulent misappropriation of assets and contractual disputes.*

Blockchain Disputes: The Need for Legal Preparedness in the Era of Economic Tokenization

By Sherzod Abdulkasimov

The rapid development of blockchain technologies and active implementation of various types of tokens in economic processes are creating a fundamentally new legal reality. What seemed like futuristic concepts just a few years ago has now become an integral part of business relationships. Digital assets are used for settlements, investments, representing property rights, and implementing complex financial instruments. Many states have already announced or launched their own central bank digital currencies, including China with the digital yuan, the Bahamas with Sand Dollar, Nigeria with eNaira, as well as pilot projects in the European Union, USA, and other developed jurisdictions.

However, along with new opportunities come new risks. Disputes related to blockchain technologies and tokens possess unique characteristics that require a specialized approach to their resolution. Traditional legal mechanisms are not always capable of effectively working with decentralized systems, smart contracts, and cryptographic assets. Moreover, the global nature of blockchain technologies means that disputes may arise between parties located in different jurisdictions, while the assets themselves may be accessible from any point in the world where there is an internet connection.

Global Nature of Blockchain Technologies and the Need for International Approach.

A fundamental characteristic of blockchain technologies is their cross-border nature. Unlike traditional financial instruments, which are usually tied to a specific jurisdiction through bank accounts, company registration, or physical location of assets, crypto assets exist in a global digital space. A private key providing access to tokens can be used from anywhere in the world with internet access. This means that the owner of crypto assets may be in one country, tokens may be placed in a blockchain whose nodes are distributed worldwide, and a smart contract may execute on infrastructure located in a third jurisdiction.

Such global accessibility creates unprecedented challenges for traditional legal systems. When a dispute arises between a token holder from Uzbekistan and an issuer from Singapore regarding a smart contract deployed on the Ethereum blockchain, whose nodes operate worldwide, determining jurisdiction becomes an extremely complex task. Each of the potentially applicable jurisdictions may have different approaches to regulating crypto assets, different evidence procedures, and various enforcement mechanisms.

The situation becomes even more complicated with the development of government digital currencies. When central banks of various countries issue their own digital currencies, complex questions arise about the status of such assets in international law. For example, if a dispute arises regarding a cross-border transaction between digital yuan and digital euro, what law should apply and which court has jurisdiction to consider such a dispute?

Advantages of Arbitral Resolution of Blockchain Disputes.

In the context of the global nature of blockchain technologies, international commercial arbitration provides significant advantages compared to national judicial systems. International recognition and enforcement of arbitral awards through the New York Convention of 1958 represents the main and decisive advantage of arbitration over national courts in the context of blockchain disputes. This advantage lies in the fact that an arbitral award can be enforced in any of the more than 160 member countries of the convention, where the respondent's assets are discovered. Given the global nature of crypto assets, this means virtually universal enforceability worldwide.

Unlike arbitral awards, enforcement of national court decisions is limited by existing bilateral or multilateral agreements on mutual recognition and enforcement of judicial decisions between specific states. Many countries do not have such agreements with each other, creating significant obstacles to cross-border enforcement. Moreover, even when agreements exist, procedures for recognizing judicial decisions are often more complex and lengthy compared to arbitral awards.

For crypto assets, which can be moved across borders in minutes, the ability to quickly obtain an enforcement document in any jurisdiction where debtor assets are discovered is critically important. The New York Convention provides a presumption of enforceability for arbitral awards, meaning that local courts are obligated to enforce the decision, except for a very limited list of grounds for refusal.

For example, a decision of an Uzbekistan court may be difficult to enforce in countries with which there are no corresponding international agreements, even if the respondent's crypto assets are located there. At the same time, an arbitral award rendered in accordance with the rules of a recognized arbitral institution can be enforced in virtually any country in the world thanks to the New York Convention.

This difference is particularly critical in the crypto industry, where assets may be placed on exchanges or in wallets controlled by service providers in various jurisdictions. A crypto asset holder may use exchanges in Singapore, wallets in Switzerland, and DeFi protocols deployed in jurisdictions with favorable regulation. An arbitral award ensures the possibility of enforcement in all these jurisdictions, while a national court decision may face serious obstacles.

Arbitral institutions also possess greater flexibility in adapting procedures to the specifics of blockchain disputes. While national courts are bound by rigid procedural frameworks, arbitral tribunals can develop specialized procedures for working with digital evidence, appoint technical experts with necessary qualifications, and adapt consideration timeframes to the complexity of technical issues.

Confidentiality of arbitral proceedings presents particular value for crypto industry participants, where disclosure of technical details of smart contracts or trading strategies can cause substantial business damage. Unlike public court proceedings, arbitral proceedings allow preserving commercial secrets and avoiding unwanted publicity.

Speed of dispute resolution is also critically important in the rapidly developing crypto industry. Arbitral procedures usually take significantly less time than judicial proceedings, especially when dealing with technically complex issues requiring specialized expertise. This is particularly important for disputes involving volatile crypto assets, where delay in dispute resolution can lead to significant financial losses.

Finally, arbitrators can be selected from among experts possessing both legal and technical qualifications in blockchain technologies. This ensures higher quality consideration of technically complex issues compared to national courts, where judges may not possess the necessary technical knowledge.

Specifics of Blockchain Disputes.

Blockchain disputes are characterized by high technological complexity. Judges, arbitrators, and lawyers face the need to understand complex technical concepts, including consensus mechanisms, cryptographic algorithms, principles of smart contract operation, and various types of tokens. An error in interpreting technical aspects can lead to incorrect legal decisions, which is particularly critical in a field where technical details often determine legal consequences.

The cross-border nature of blockchain technologies creates additional complexities. Transaction participants may be located in different jurisdictions, the blockchain itself may be decentralized worldwide, and smart contracts may execute on servers in third countries. This creates complex questions of determining applicable law and jurisdiction, especially when various jurisdictions have radically different approaches to regulating crypto assets.

The problem of evidence in blockchain disputes also requires a special approach. In traditional disputes, evidence is usually presented in physical or easily verifiable electronic form. In blockchain disputes, evidence may include cryptographic signatures, transaction hashes, smart contract data, and other technical elements requiring special expertise for their correct interpretation. Moreover, the immutability of blockchain records, while ensuring a high degree of reliability, creates new questions about how to interpret data that cannot be changed after the fact.

Main Categories of Blockchain Disputes.

Smart contract disputes represent one of the most complex categories of blockchain disputes. Smart contracts automatically execute when predetermined conditions are met, however disputes may arise regarding correct programming of contract conditions, correspondence of code to parties' intentions, actions during technical failures or bugs, as well as interpretation of ambiguous conditions. Particularly complex are cases where smart contract code contains errors that lead to results contradicting the parties' intentions.

Disputes over token rights are becoming increasingly common with the growing popularity of asset tokenization. Such disputes may concern the nature of rights represented by tokens, legitimacy of token issuance, violation of tokenholder rights, as well as fraud in conducting initial token offerings. Particularly complex are disputes over tokens that represent rights to real assets, where it is necessary to establish a connection between the digital token and physical or intangible asset.

Decentralized financial protocols create new types of disputes, including loss of funds due to protocol bugs, disputes over yield farming income distribution, conflicts in decentralized governance, and disputes over position liquidations. The peculiarity of DeFi disputes lies in the fact that they are often related to automated protocols where human intervention is minimal, creating new questions about liability and possibility of damage compensation.

Non-fungible tokens generate disputes over intellectual property rights, authenticity and origin of NFTs, copyright infringement, and fraud on NFT marketplaces. Particularly complex are disputes about what exact rights are transferred with an NFT, since the token may not include all rights to the associated content.

Government Digital Currencies and New Legal Challenges.

The development of central bank digital currencies creates a fundamentally new category of disputes. When a central bank issues a digital version of national currency, this raises complex questions about the legal status of such assets. On one hand, central bank digital currencies should have the status of legal tender on par with physical money. On the other hand, their technical implementation through blockchain or other distributed ledger technologies creates new legal nuances.

Cross-border operations with government digital currencies are particularly complex from a legal standpoint. When digital yuan interacts with digital euro through international platforms like mBridge, questions arise about what law applies to such operations, how disputes between holders of various government digital currencies are resolved, and which courts or arbitral institutions have jurisdiction to consider such disputes.

Additionally, government digital currencies may create new types of disputes related to programmable money. If a central bank implements certain usage restrictions or automatic execution mechanisms for certain functions in digital currency, this may lead to disputes about the legitimacy of such restrictions and their compliance with human rights and fundamental freedoms.

Preparation for Blockchain Disputes: Strategic Approaches.

Lawyers and law firms must invest in technical education for effective client representation in blockchain disputes. This includes studying the basics of blockchain technologies, understanding differences between types of tokens, including utility tokens, security tokens, and governance tokens, mastering principles of smart contract operation, and studying features of various blockchain platforms. Without such understanding, lawyers will not be able to effectively analyze evidence or formulate legal arguments in technically complex disputes.

Creating an expert network is critically important for successful conduct of blockchain disputes. This includes establishing connections with technical experts capable of conducting smart contract and blockchain data analysis, finding reliable blockchain auditors for technical expertise, as well as forming a network of international partners for effective conduct of cross-border disputes. The quality of expert support often determines the outcome of blockchain disputes.

Procedural preparation includes developing standard procedures for collecting digital evidence, creating checklists for smart contract analysis, and preparing templates for various types of blockchain disputes. Effective procedural preparation allows quick response to emerging disputes and avoids procedural errors that may negatively affect case outcomes.

Business structures should take preventive measures to minimize blockchain dispute risks. This includes incorporating clear arbitration clauses in smart contracts, specifying applicable law and jurisdiction, conducting preliminary smart contract audits, and carefully documenting all intentions and agreements. A preventive approach is significantly more effective than reactive response to already emerged disputes.

Risk insurance is becoming an increasingly important element of risk management in blockchain projects. Companies should consider the possibility of insurance against smart contract bugs, study insurance products for DeFi protocols, and create reserve funds to cover technical risks. Insurance helps minimize financial losses and provides additional protection for blockchain ecosystem participants.

Internal company procedures should include staff training in blockchain technology basics, creating incident response procedures, and installing blockchain asset monitoring systems. A well-prepared team can quickly identify problems and take measures to resolve them before they escalate into serious disputes.

International Practice and Arbitral Institution Adaptation.

Singapore became one of the leaders in developing legal mechanisms for blockchain disputes. The Singapore International Arbitration Centre developed special rules for disputes related to digital assets, including expedited procedures for technical disputes, arbitrator qualification requirements, and special evidence rules. The Singapore approach demonstrates how arbitral institutions can adapt to the needs of the new digital economy.

Switzerland created a favorable legal environment for blockchain business, which includes clear token classification, specialized courts, and international arbitral procedures. Swiss experience shows the importance of a comprehensive approach that combines favorable regulation with effective dispute resolution mechanisms.

British courts actively develop case law on blockchain disputes, especially in areas of recognizing crypto assets as property, enforcement of smart contracts, and cross-border recovery of digital assets. British practice demonstrates how traditional legal systems can adapt to new technological realities.

The International Chamber of Commerce also adapts its rules for blockchain disputes, including developing special procedures for technical expertise and modifying evidence rules. These changes reflect growing recognition of the need for specialized approaches to blockchain disputes.

Future Trends and Technological Solutions.

As a practicing crypto investigator spending significant time analyzing and searching for stolen crypto assets, I have come to an important conclusion about the future of arbitration in blockchain disputes. Daily work with blockchain analytics tools, tracking fund movements through multiple addresses and wallets, analyzing transaction patterns, and establishing connections between various crypto assets shows that technologies have reached a level where conducting investigations and asset analysis in real time becomes possible.

Based on this practical experience, I can assert that in the near future, arbitrators considering blockchain disputes will also work directly on the blockchain, analyzing asset transactions and establishing their location in real time. Modern blockchain analytics tools already allow tracking fund movements through dozens of intermediate addresses, identifying obfuscation attempts through mixers and decentralized exchanges, as well as establishing connections between various wallets of one owner.

This technological capability will radically change evidence procedures in arbitration. Instead of relying on static snapshots of blockchain data at specific moments in time, arbitrators will be able to observe disputed asset movements dynamically, ensuring more accurate establishment of factual circumstances and more effective enforcement of decisions.

Particularly important this becomes in the context of interim measures and preliminary orders. The ability to track crypto assets in real time will allow arbitrators to quickly identify attempts to hide or withdraw assets and take appropriate measures for their blocking or seizure. This solves one of the main problems of traditional arbitration - the difficulty of ensuring preservation of disputed assets until a final decision is rendered.

Practical experience shows that modern tools already allow tracking funds even after passing through complex obfuscation schemes. Machine learning algorithms can identify behavior patterns characteristic of asset concealment attempts, giving arbitrators a powerful tool for combating bad faith party behavior.

In one recent investigation, it was possible to trace the path of stolen crypto assets through more than 50 intermediate addresses, including passage through several mixers and decentralized exchanges. Modern analysis tools allowed establishing final withdrawal points and identifying centralized exchanges where assets were ultimately cashed out. Such a level of detail and ability to work in real time give arbitrators unprecedented opportunities for effective dispute consideration and decision enforcement.

This means that future arbitral procedures may include not only traditional consideration of documents and witness testimony, but also active monitoring of blockchain assets during the proceedings themselves. Arbitrators will be able to observe attempts to move disputed assets and take appropriate interim measures in real time.

Artificial intelligence development may revolutionize blockchain dispute resolution through automated smart contract analysis, use of AI arbitrators for simple technical disputes, and predictive analytics for risk assessment. AI can help in rapid analysis of large volumes of blockchain data and identifying patterns that may be important for dispute resolution.

New models of dispute resolution directly on blockchain are emerging, including decentralized arbitration platforms, community voting mechanisms, and automatic enforcement of arbitral decisions. Such on-chain solutions may provide faster and more efficient resolution of certain types of disputes, especially those related to technical protocol parameters.

Cross-chain technology development creates new types of disputes, including disputes over bridges between blockchains, conflicts in multi-chain protocols, and jurisdictional questions in interoperable systems. These new technologies require further development of legal mechanisms and arbitral procedures.

Recommendations for Legal Infrastructure Development.

Educational programs should become a priority for preparing the legal community for blockchain disputes. This includes organizing specialized courses for judges and lawyers, creating comprehensive educational materials, and conducting regular conferences for experience exchange. Education quality directly affects dispute resolution quality.

Procedural improvements include developing specialized evidence rules for digital assets, creating a registry of qualified technical experts, and simplifying international cooperation procedures in blockchain disputes. Effective procedures ensure fair and fast dispute resolution.

Institutional development requires creating specialized judicial panels, developing arbitral institutions with blockchain technology expertise, and international standardization of procedures. Specialized institutions can ensure higher quality consideration of technically complex disputes.

Blockchain Disputes: The Need for Legal Preparedness in the Era of Economic Tokenization

Technological integration includes implementing electronic document workflow, creating databases of blockchain dispute precedents, and developing remote participation systems in proceedings. Technologies can significantly increase legal process efficiency.

International law harmonization through developing international standards, creating multilateral agreements, and unifying legal approaches is critically important for effective resolution of cross-border blockchain disputes. Unified standards facilitate recognition and enforcement of decisions in various jurisdictions.

Conclusion.

Economic tokenization and blockchain technology development, including government digital currencies, irreversibly change the legal landscape. Disputes related to digital assets already today require a specialized approach and deep understanding of technological features. The global nature of blockchain technologies, where access to assets is possible from anywhere in the world, makes international arbitration a preferred dispute resolution mechanism compared to national judicial systems.

Arbitral institutions possess flexibility, speed, and most importantly, global enforceability of decisions necessary for effective resolution of cross-border blockchain disputes. The ability to enforce arbitral awards in any country worldwide where respondent assets are discovered through the New York Convention mechanism represents a decisive advantage over national courts limited by bilateral agreements. Additional advantages include the possibility of selecting qualified arbitrators, adapting procedures to technological dispute specifics, and ensuring confidentiality of proceedings.

Blockchain analytics technology development and practical crypto investigation experience show that the future of arbitration will be closely connected with real-time asset analysis and tracking capabilities. Arbitrators will receive tools allowing not only dispute consideration based on static evidence, but also active monitoring of disputed asset movements during proceedings, which will radically increase the effectiveness of interim measures and decision enforcement.

Successful adaptation of the legal system to new realities requires significant investments in education and personnel training, development of specialized institutions, international cooperation and standardization, as well as flexibility in adapting to constantly changing technological conditions. Those jurisdictions that first create effective blockchain dispute resolution mechanisms will gain significant competitive advantages in attracting innovative business and developing the digital economy.

The time for preparing for blockchain disputes has already arrived today. Each day the number of government and private digital assets grows, cross-border transaction volumes increase, and technological solution complexity rises. The quality of legal system preparation for these challenges will determine the effectiveness of legal protection in the digital age and the ability of various jurisdictions to participate in the global digital economy on equal terms.

Sherzod Abdulkasimov, *International Arbitrator, Crypto Investigator and Managing Director of Praelegal Uzbekistan law firm*

Bitcoin: The birth of digital law in Internet Jurisdiction

By Ignacio Ferrer-Bonsoms

The rise of Bitcoin has transformed much more than financial systems: it has started a new legal revolution. Bitcoin is not just a currency or a technological protocol; it is the first globally accepted example of digital law.

This form of "digital" law has not been emanated by states, nor parliaments, nor courts: it is born directly from code, consensus and the unstoppable logic of the blockchain.

Bitcoin as digital law, not just as money

Traditional law is backed by governments, enforced through courts and written in laws. Bitcoin and crypto assets represent something radically different. Their rules are embedded in their protocol, executed automatically by their decentralized network and respected globally by millions of participants without the need for a central authority.

In this sense, Bitcoin is a self-executing law: a set of immutable, transparent and universally accessible rules that organize economic and social behaviour in the digital space.

Bitcoin not only proposes a new payment system; it is a new way of regulating human interactions without borders or intermediaries. Its consensus rules - such as the limit of 21 million coins, the block creation time or the irreversibility of transactions - function as constitutional norms, yet they require neither police nor traditional enforcement.

The emergence of internet jurisdiction

The most revolutionary aspect of Bitcoin is that it contributes to the creation of an internet jurisdiction of its own: a legal space that exists outside national borders. In this new environment, legal authority is no longer the monopoly of states.

Decentralized communities can establish their own rules, governance systems and dispute resolution mechanisms.

This concept challenges the traditional legal order. Can there be law without a state? Bitcoin's answer is yes. Internet jurisdiction means that communities on the blockchain can self-organize, self-regulate and self-enforce their agreements through smart contracts and decentralized protocols. Code is no longer just law, it is digital law of the internet jurisdiction.

There is no division of powers in the Internet jurisdiction

The division of powers, formulated by Montesquieu in the 18th century, has been the fundamental pillar on which the modern State has been built. The separation of legislative, executive and judicial powers has served as a guarantee of individual freedoms and as a brake on the concentration of power in a single authority. This model has structured Western democracies and has been exported to multiple legal systems around the world.

However, the birth of internet jurisdiction and the expansion of blockchain technology are radically challenging this classic principle. In decentralized digital communities, functions that were once separate are now integrated and automated in a single space: the internet.

In the blockchain, anyone can set the rules (legislative function), automatically execute transactions and contracts (executive function), and submit disputes to a legal oracle (judicial function). Thus, the three traditional functions of state power converge and are exercised simultaneously within the technological system.

This means, in practical terms, the end of the division of powers in digital environments. The new model is not based on separation to prevent abuse, but on code transparency, resistance to censorship and mathematical security. Trust is not placed in the institutions, but in the technical architecture that ensures that the rules are equal and enforceable for all.

Overcoming "code is law" with digital laws in the internet jurisdiction

The famous phrase "code is law", popularized by Lawrence Lessig, pointed out that behavior on the internet could be regulated directly by computer code. What the code permitted or prohibited was, in practice, the effective law in cyberspace.

However, with the advent of blockchain technology, this concept has evolved. Today, we are not just talking about a code that regulates access or functionalities. We are talking about the creation of true autonomous, complete and self-executing digital laws.

Code is now the core of new decentralized legal systems, where entire communities create, implement and enforce their own digital laws through consensus and blockchain technology.

Each era has developed its own law

Each era has developed a law adapted to its economic and social needs. In the Middle Ages, for example, commercial law emerged as an essentially private law. It was driven by merchants who needed clear rules for their international operations, and did not depend on the power of the monarch, but on the force of private contracts and arbitration courts. This financial and commercial renaissance coincided, as it will in our time, with the birth of a strong currency, the "florin". This is why the Medieval renaissance took place first in Florence and then in Venice, spreading throughout Europe.

Today we are witnessing a similar phenomenon. Digital laws are emerging around a strong and decentralized currency: Bitcoin. Like medieval mercantile law, digital laws are built from practice, consensus and the need to resolve conflicts in a transnational environment, without relying necessarily on states.

Bitcoin is not just an asset; it is the reference around which a new digital law is being formed, reminiscent of the autonomy and solidity of the old mercantile law, but now with a much more advanced technological architecture: the blockchain.

The challenge: building from the jurisdiction of the internet

Bitcoin and Ethereum are not just currencies, they are building the jurisdiction of the internet. The decentralized nature of these systems means that law can now emerge directly from code and consensus, not just from governments.

Bitcoin: The birth of digital law in Internet Jurisdiction

The advancement of blockchain technologies has opened the door to a disruptive phenomenon: the real possibility of organizing as a society from the jurisdiction of the internet, outside of traditional states.

This new space, based on decentralized networks and governed by community consensus, allows the creation of rules, governance structures and legal transactions without the need for state intermediation.

The blockchain can offer an autonomous legal environment where rules are self-executing and where relationships can be established and enforced exclusively within the network.

The development of smart contracts has allowed the direct execution of digital legal business: sales, loans, collaboration agreements, all of them formalized and fulfilled within the digital jurisdiction.

But it is also necessary to start incorporating justice mechanisms directly into the “Digital Law code” to resolve disputes. This is precisely what Blockchain Arbitration & Commerce Society (BACS) proposes. Through its own regulatory framework, the blockchain enables a third party — a legal oracle — to resolve disputes directly on-chain, making arbitral awards automatically enforceable. This represents a true before-and-after moment in the history of dispute resolution, legal systems, and international arbitration.

BACS, for example, integrates attachable tokens, i.e. tokens that can be legally seized in case of litigation, and bridges that allow tokens from other blockchains to enter a jurisdiction where those assets can be subject to legal enforcement.

This fusion of blockchain design and legal functionality opens the door to secure and legally valid merchant contracts in the decentralized economy.

A must read: "Bitcoin Digital Law: why cryptocurrencies are digital laws of the internet and why states must adapt”

This book explores essential questions like: if Bitcoin is regulated outside of the States, how is it regulated? What kind of law is it? Can we speak of a new source of law operating in the jurisdiction of the internet? Does the jurisdiction of the internet exist? Can we as a society begin to regulate ourselves based on the jurisdiction of the internet? And curiously can a digital law that is ultimately more robust and secure than any country's constitution?

By studying the past we can intuit the future. By delving into the agricultural and industrial and cognitive revolution we can understand what the future will look like with the new internet. It’s no coincidence that the modern state is losing strength and that new forms of government are needed. It is also no coincidence that the elites do not want us to understand new technologies.

Since the emergence of the blockchain, it is possible to regulate ourselves in a decentralized, private way, with a law that is digital, self-regulating and self-executing. Those born under the figure of the Modern State, accustomed to moral rules forged in the Industrial and French Revolution, find it difficult to understand this change.

Likewise, states, elites and official organizations repeat over and over again the same message from various platforms: Bitcoin is unregulated, it is only good for dirty business, it is merely speculative, etc. While we listen to these slogans, the price of Bitcoin continues to rise, unstoppable.

Internet technology allows us to be sovereign, to issue digital laws in a decentralized way, and to organize ourselves through new institutions. It is our responsibility to seek social and legal solutions in line with the internet revolution. This is the message that Bitcoin gives us: let's not leave in the hands of distrustful third parties what we can solve from the community itself. Money and law, in the end, belong to society - to the community - and not to states.

__Ignacio Ferrer-Bonsoms__, is a lawyer and legal advisor. He is president of the Blockchain Arbitration & Commerce Society, an association that has the first Arbitration Court specialized in blockchain, cryptocurrencies and artificial intelligence.

Electronic Voting using Blockchain

By Andrés Acosta

E-voting projects have been a reality for several years, especially with the emergence of blockchain technology. This groundbreaking innovation has also extended its influence to the field of electronic voting, offering potential solutions to long-standing challenges such as security, transparency, and high operational costs. The adoption of blockchain in voting systems has primarily involved using the technology as an immutable ledger that guarantees the integrity of the electoral process.

Electronic voting addresses various problems present in traditional systems, such as difficulties for citizens living abroad to exercise their voting rights, limited accessibility for individuals with illnesses or mobility impairments, and low voter turnout due to long lines at polling stations.

In this context, blockchain technology has recently gained popularity across multiple sectors and can significantly contribute to improving e-voting processes. Its features—such as data immutability—ensure that once a vote is recorded, it cannot be altered or deleted. Moreover, it enables full transparency and traceability, allowing real-time and post-election audits without compromising voter confidentiality.

Currently, several Latin American countries are implementing electronic voting. Ecuador recently introduced telematic voting, while El Salvador implemented electronic voting in its 2024 elections, allowing over 700,000 Salvadorans abroad to vote over a 30-day period.

Blockchain functions as a decentralized chain of blocks, storing encrypted information in a database accessible to all authorized participants in the system. It acts like a large, unalterable ledger, where information is validated and stored through a shared protocol.

In Peru, Law No. 32270 was recently passed, amending Law No. 26859, to allow the incorporation of virtual electronic voting supported by blockchain technology for Peruvians living abroad. This aims to reduce absenteeism among foreign voters. In the last general election (2021), voter turnout abroad did not exceed 25% of the electoral roll—only 23% of the 997,033 eligible voters participated, resulting in a 77% abstention rate.

The electronic voting process will include a digital polling station composed of nine regular members and nine alternates, who will serve as the Polling Station President, Secretary, and Third Member. These individuals will be selected by lottery from a pool of seventy-five citizens with higher education. Serving as a polling station member is mandatory and cannot be declined.

Citizens will be able to vote voluntarily through the portal https://votodigital.onpe.gob.pe. They will authenticate themselves on the platform using their electronic identification document, view the digital ballot, cast their vote, and receive a digital receipt. Eligible participants include police officers, members of the armed forces deployed outside their home districts, and citizens residing abroad who choose to vote electronically.

The adoption of digital voting in Latin America is progressing gradually, driven by the need to modernize electoral systems and increase civic participation. Recent examples such as Ecuador and El Salvador demonstrate varying degrees of technological and regulatory advancement.

With secure electronic identification and technologies like blockchain, the next logical step in the evolution of e-voting is the implementation of **liquid democracy**. This model represents an innovative blend of direct and representative democracy, enabling more flexible, dynamic, and personalized participation. Instead of voting only every few years for fixed representatives, citizens can decide how, when, and on what issues they want to participate directly.

In this system, a citizen can vote directly on a specific topic, delegate their vote to a trusted or specialized representative, or revoke that delegation at any time. This flexibility allows citizens to engage actively while retaining control over their representation. The ability to shift between direct voting and delegation makes the democratic process more adaptable and inclusive.

Liquid democracy is **flexible**, as it allows vote delegation by topic (e.g., health, education, environment); **dynamic**, since delegations can be modified at any time; and **scalable**, because it can be implemented in small communities or on a national or global scale, promoting broad citizen involvement in decision-making.

For example, imagine a country's Congress linked to a digital citizen platform. Individuals could review the legislative topics, access educational content, and choose to vote directly or delegate their vote to a subject-matter expert or representative. If the delegate no longer meets their expectations, the citizen could rescind the delegation and cast their vote directly before the voting period closes.

This model not only empowers individual voters but also fosters the emergence of a new kind of leadership—rooted in knowledge, ethics, and trust. It breaks down the traditional divide between representatives and the represented, enhancing the legitimacy of collective decisions and cultivating a more informed, collaborative, and accountable political culture. In this sense, liquid democracy is not merely a technological evolution but a qualitative leap forward in the exercise of civic sovereignty.

In conclusion, liquid democracy presents a real opportunity to modernize our democratic systems by integrating technology that fosters more open, intelligent, and decentralized participation. If implemented responsibly, it could form the basis of a new, more inclusive and transparent social contract—better aligned with the needs and expectations of a digitally connected society.

However, it is important to emphasize that the integration of blockchain into electoral processes also presents **technological, social, and regulatory challenges**. Ensuring digital literacy, legal adaptation, cybersecurity, and equitable connectivity are all crucial factors. These must be addressed holistically to ensure that these emerging solutions truly strengthen democracy rather than create new forms of exclusion.

The use of blockchain in elections should not be seen merely as a modernization effort, but as a shift toward building **more inclusive, secure, and transparent electoral systems** that reflect the realities of a digitally empowered world.

***Andrés Acosta**, is the CEO of Aura Systems, Member of the Harvard Business Review Board, Founding Partner of the Peruvian Blockchain Association and Vice President of the Technology Commission for the Peru-Brazil Chamber of Commerce.*

Ripple's Labyrinth:
From Howey to Crypto Clarity

By *Yuriy Brisov*

The SEC's 2020 lawsuit against Ripple Labs Inc. over XRP sales crystallised a decades-long struggle to apply 20th-century securities law to blockchain innovation. This article traces the jurisprudential lineage from *SEC v. Howey's* citrus groves to Judge Torres's analysis of a cryptographic ledger; the path of legal precedents has evolved. In 1946, the U.S. Supreme Court ruled that selling plots of Florida orange groves with service contracts constituted an "investment contract" under federal law. Seventy-seven years later, that same precedent – *SEC v. W.J. Howey Co.* would be invoked to determine the fate of a digital asset powering a $26 billion cross-border payments network.

The Birth of Decentralised Ambition

In April 2016, Christoph Jentzsch, a Berlin-based programmer, introduced "The DAO" (Decentralised Autonomous Organisation), a groundbreaking Ethereum-based venture fund designed to operate without a central management structure. The DAO allowed investors worldwide to acquire DAO tokens, granting voting rights on proposed projects and a share in potential profits. Within a 28-day funding window, The DAO raised over $150 million worth of Ether from more than 11,000 investors – one of the largest crowdfunding campaigns in history. However, the enthusiasm was short-lived. On June 17, 2016, an anonymous hacker exploited a vulnerability (a recursive call bug) in The DAO's smart contract code, siphoning approximately 3.6 million Ether (around $50 million at the time) into a "child DAO" account. The attack caused Ether's price to plummet from over $20 to under $13. This incident exposed flaws in the "code is law" philosophy underpinning decentralised governance and highlighted the absence of legal safeguards for investors. The Ethereum community debated remedies and ultimately executed a hard fork to reverse the hack, splitting the blockchain into Ethereum (the fork) and Ethereum Classic (the original chain).

Regulators took notice. Despite the DAO's origins in Germany, its global investor base included U.S. participants. The U.S. Securities and Exchange Commission (SEC), tasked with protecting U.S. investors and maintaining fair markets, asserted jurisdiction to investigate potential securities law violations. Before 2017, the SEC had primarily regarded cryptocurrencies like Bitcoin as commodities and refrained from extensive oversight of token sales. However, the DAO's collapse prompted a reassessment. In a 21-page investigative report dated 25 July 2017, the SEC concluded DAO tokens were securities under the *Howey* test, stating: "Investors in The DAO reasonably expected to earn profits from the managerial efforts of others." The SEC's 2017 DAO Report marked a pivotal moment: it clarified that federal securities laws can apply to digital asset offerings. This served as a warning to U.S. crypto issuers and investors, emphasising the importance of compliance with existing laws, even in novel situations.

Notably, the SEC did not ban Initial Coin Offerings (ICOs) outright, but rather underscored the legal requirements to protect investors and maintain market integrity. The report's impact was profound. In 2018, ICO activity declined by roughly 90% as many projects moved offshore to evade U.S. jurisdiction. A paradox emerged: the SEC had asserted authority over token sales but provided little formal guidance for compliant offerings, leaving issuers uncertain how to proceed within the bounds of U.S. law.

Tezos: The $232 Million Cautionary Tale

Just weeks after the DAO Report, another massive ICO tested the regulatory waters. In July 2017, Tezos – pitched as a self-amending "governance blockchain" – raised $232 million in Bitcoin and Ether. Global excitement for Tezos quickly gave way to legal and internal turmoil. A rift between the founders and the Swiss-based Tezos Foundation led to several class-action lawsuits alleging the ICO was an unregistered securities offering and that promoters made misrepresentations (see *In re Tezos Sec. Litig.*, No. 17-cv-06779 (N.D. Cal. filed Oct. 25, 2017). Early in 2018, plaintiffs' attorney David Silver filed a Freedom of Information Act (FOIA) request with the SEC regarding Tezos. The SEC denied the request, citing FOIA Exemption 7(A), which permits withholding records compiled for law enforcement if disclosure "could reasonably be expected to interfere with enforcement proceedings.

This cryptic response, not confirming whether Tezos was under investigation, fueled speculation that the SEC was closely monitoring Tezos. Ultimately, however, the SEC never brought public enforcement against Tezos or its founders. The private litigation was settled in 2020 for $25 million, resolving investors’ claims without any admission of liability.

The DAO Report and the Tezos saga together set the stage for a more aggressive SEC posture on crypto. By late 2020, the Commission, led by outgoing Chairman Jay Clayton, was ready to target a much bigger fish in the crypto pond.

The DAO Report’s Ripple Effect

The SEC’s 2017 DAO Report resonated well beyond the blockchain community, unsettling Silicon Valley boardrooms, prestigious law firms, and crypto startups alike. Although the report lacked the formal authority of a rulemaking, its message was clear: many digital tokens could be classified as investment contracts, and the SEC was closely monitoring the situation. In subsequent years, the Commission took enforcement actions against several high-profile token issuers – Munchee, Paragon, AirFox, Kik, and Telegram, to name a few – each time citing *Howey*. Most of these cases resulted in settlements, enabling the SEC to influence industry conduct without risking costly court decisions. However, one firm chose to contest the charges, laying the groundwork for a courtroom battle that would challenge *Howey*’s applicability in the crypto era: Ripple Labs.

Ripple’s Ascent and the SEC Showdown

When the SEC sued Ripple Labs in December 2020, it marked a pivotal escalation in the agency’s campaign to assert jurisdiction over digital assets. While previous SEC targets were relatively small startups, Ripple was a $10 billion fintech with an established global user base, and XRP was among the top five cryptocurrencies. The case thus became a litmus test for *Howey*’s viability in governing blockchain-based token sales. The SEC’s complaint – filed on December 22, 2020 – alleged that XRP is a security and that Ripple’s $1.3 billion in sales of XRP since 2013 violated Section 5 of the Securities Act by failing to register the offers. The SEC argued XRP met all three prongs of *Howey*: investors paid money (or other value) to Ripple in a common enterprise, with a reasonable expectation of profits derived from Ripple’s entrepreneurial efforts (building out XRP’s utility in cross-border payments). Fresh off its win in *SEC v. Telegram* (2020), the SEC seemed poised to cement authority over a major crypto asset.

However, unlike Telegram (which halted its token issuance) or Kik (which settled), Ripple chose to fight – an approach that would force a judicial reckoning with applying *Howey* to a freely-trading digital token.

Ripple and its executives, Brad Garlinghouse (CEO) and Christian Larsen (co-founder), mounted an aggressive defense. They argued, inter alia, that: (1) XRP, as a token, is a **currency** or medium of exchange (like Bitcoin) outside the SEC’s remit; (2) the SEC never formally warned that XRP was a security during the token’s first seven years of circulation; and (3) XRP’s market value has not been tightly tethered to Ripple’s actions, given that XRP was traded globally and largely by third parties, not Ripple itself.

The battle lines were drawn between a “literalist” view of *Howey* – focusing on the contractual scheme surrounding a token’s sale – and Ripple’s more **substance-over-form** view – that a token with a bona fide utilitarian function (here, facilitating fast transactions) cannot be a security in itself.

SEC v. Ripple Labs: A Five-Year Legal Chronicle

Litigation Begins: The SEC filed suit in the Southern District of New York on December 22, 2020, coinciding with the final weeks of the Trump administration. Ripple promptly indicated it would not capitulate. In early 2021, the SEC amended its complaint, and the case plunged into extensive discovery. Fact discovery lasted through August 2021, and expert discovery through February 2022. The pretrial phase saw fierce skirmishes. In March 2022, Judge Analisa Torres (the presiding U.S. District Judge) denied the individual defendants’ motions to dismiss and also refused to strike Ripple’s “fair notice” defense – signalling that thorny due process issues would remain in play. Both sides exchanged voluminous evidence on XRP’s use and marketing. By September 2022, each had moved for summary judgment, setting the stage for a much-anticipated ruling.

Industry and Political Undercurrents: The drawn-out timeline (2020–2023) reflected not just the case’s complexity but also external pressure. Under Chairman Clayton (who authorized the case) and his successor Gary Gensler, the SEC showed unwavering resolve to press the lawsuit despite an evolving crypto landscape. Ripple, for its part, garnered an unusually broad coalition of allies. Over a dozen amicus briefs were filed on Ripple’s behalf, from crypto exchanges, industry associations, and XRP holders, all arguing the SEC’s theory would harm innovation.

This public support and the case’s stakes perhaps encouraged the court’s careful, time-consuming deliberation. Any hint of settlement remained elusive – likely because the SEC, especially under Gensler, wanted a definitive court precedent to guide the industry (and perhaps because Ripple sought vindication). Indeed, the case became a crucible for the SEC’s “regulation-by-enforcement” strategy in the cryptocurrency sector.

The Split Decision (July 2023): On July 13, 2023, Judge Torres issued her landmark summary judgment opinion. In a nuanced holding, she ruled that Ripple’s XRP token was sold in violation of securities law when offered directly to institutional investors, but not when sold via programmatic exchange transactions or distributed to employees as compensation. Crucially, Judge Torres applied *Howey*’s investment-contract test to each distinct category of XRP sales. For the institutional sales (generally, negotiated sales to hedge funds and sophisticated buyers, totalling approximately $728 million), the court found that all *Howey* elements were satisfied. These buyers paid money to Ripple, entered a common enterprise, and had a reasonable expectation of profit from Ripple’s efforts to develop the XRP ecosystem.

In contrast, programmatic sales (blind trading on public exchanges, which account for less than 1% of global XRP volume) did not meet *Howey*’s third prong. Retail buyers on an exchange, the court reasoned, had no privity with Ripple and no concrete promises or representations from Ripple at the point of sale – their expectation of profit, if any, was based on speculation or market forces, not on Ripple’s managerial efforts. Likewise, XRP distributions to executives and developers (as compensation or rewards) lacked an investment opportunity for anyone. By parsing the sales contexts, Judge Torres essentially found XRP itself “not a security,” except as packaged in specific transactions.

This Solomonic outcome gave something to both sides. The SEC could claim victory that Ripple’s direct institutional sales were unlawful unregistered securities offerings – a point reinforcing the application of Howey to outright token sales. Ripple, on the other hand, could reference a court ruling stating that XRP tokens traded on secondary markets are not securities – a first-of-its-kind judicial determination challenging the SEC’s view that virtually any token sale can implicate securities laws. The decision immediately sent shockwaves through the crypto industry and was celebrated as a significant victory for crypto advocates seeking clearer limits on the SEC’s reach.

Post-Ruling Developments: The divided nature of the ruling initiated further battles. The SEC promptly signalled its intention to seek an interlocutory (mid-case) appeal regarding the adverse portion (the programmatic sales holding), contending that Judge Torres’s distinction between institutional and retail sales was legally flawed. However, Judge Torres denied the SEC’s motion on 3 October 2023, stating there was no “controlling question of law” and no substantial ground for difference of opinion – the issue pertained to the fact-specific application of Howey to Ripple’s sales, not a pure legal question suitable for immediate appeal. Around the same time, the SEC, perhaps recognising the futility of prolonging the dispute, voluntarily dismissed its remaining claims against Garlinghouse and Larsen (the individual defendants) on 19 October 2023. This averted an imminent jury trial and moved the case closer to a final resolution.

With liability largely determined, Judge Torres proceeded to the remedy phase. In August 2024, she entered a final judgment ordering Ripple to pay a civil penalty of $125 million for the institutional sales violation. She also imposed injunctions to ensure Ripple’s compliance going forward. Ripple reluctantly agreed to the penalties but also filed a notice of appeal – as did the SEC, still hoping to overturn the ruling that XRP’s secondary-market sales were lawful. The legal battle appeared destined for the Second Circuit.

Regulatory Whiplash and Settlement (2025): The courtroom conflict took a sharp turn when the U.S. presidential administration changed in January 2025. A new SEC leadership team, under a more crypto-friendly chair, reassessed the agency’s stance. In March 2025, before appellate briefing had advanced much, the SEC withdrew its appeal, effectively accepting Judge Torres’s rulings on XRP’s non-security status in secondary sales. Ripple’s CEO, Brad Garlinghouse, described the SEC’s retreat as a “long overdue surrender,” and Ripple said it would also drop its cross-appeal on the institutional sales ruling. The parties reached a settlement to close the case: Ripple agreed to pay $50 million (a reduced fine) with no admission of wrongdoing, and the SEC agreed to remove some harsh injunction terms, subject to court approval. Over four years after the lawsuit started, SEC v. Ripple Labs finally concluded – not with a clear appellate precedent, but with a practical truce that preserved Judge Torres’s opinion and its influence. The SEC’s retreat, following other crypto enforcement rollbacks in 2025, indicated a possible shift in U.S. regulatory strategy towards a more conciliatory or nuanced approach.

Notwithstanding the case’s mixed outcome, Judge Torres’s July 2023 opinion has been widely regarded as a well-reasoned and doctrinally significant contribution to crypto jurisprudence. Observers praise the ruling’s clarity: it meticulously applied each prong of *Howey* to distinct facts, showing how careful factual analysis can separate compliant transactions from unlawful ones. The opinion is grounded in orthodox securities-law principles yet sensitive to the realities of decentralised digital assets. For instance, Judge Torres reaffirmed that the subject of an investment scheme (here, the XRP token) is not itself a security – a point often misunderstood in the crypto debate – rather, it is the “contract, transaction, or scheme” involving the asset that must be examined. As she put it, an investment contract requires an ongoing legal relationship or promises to investors, “not merely an asset” circulating in the market.

Applying the third *Howey* prong (expectation of profits derived from others’ efforts), the judge drew a principled line. She found that sophisticated institutional buyers purchased XRP with clear promotional inducements from Ripple – they were explicitly told of Ripple’s efforts to grow XRP’s value, satisfying the “efforts of others” element. In contrast, retail XRP buyers on exchanges were generally anonymous and had no reason to know whether Ripple (or anyone connected to Ripple) was on the other side of a trade; they received no promises at the time of purchase. Any profit expectation by these public buyers was based on general market forces or speculation, not on Ripple’s managerial actions, which broke the causal link required by *Howey*. Importantly, evidence showed that since 2017, Ripple’s exchange program accounted for less than 1% of global XRP volume, so **“the vast majority”** of XRP purchasers in the market did not invest in Ripple at all. This empirical backdrop bolstered Judge Torres’s legal conclusion that programmatic sales were not investment contracts.

The measured tone and rigour of Judge Torres’s analysis have made her opinion a persuasive reference point beyond her courtroom. It offers a potential template for how other courts might approach token sales with nuance. It signalled to regulators and industry alike that long-standing securities doctrines can, when applied judiciously, accommodate new technology. To be sure, as a trial court ruling, *SEC v. Ripple* is not binding precedent elsewhere. Yet it quickly became a cornerstone of the legal debate – cited in other crypto cases as persuasive authority (indeed, defense counsel in *SEC v. Coinbase* and other ongoing cases have invoked the Ripple ruling to argue that at least secondary-market trading of tokens falls outside securities laws).

Beyond the Courtroom: Ripple’s Impact on Regulation

Perhaps the most immediate ripple effect of *Ripple* (pun intended) was within the SEC itself. Judge Torres’s reasoning implicitly acknowledged that how a token is distributed and used matters greatly for securities law. For example, her analysis highlighted that genuinely decentralised, mining-based cryptocurrencies – such as Bitcoin or Litecoin, which emerge from *proof-of-work* mining rather than any ICO or centralised sale – lack the sort of “contract, scheme, or transaction” between an issuer and investors that *Howey* requires. In other words, if no one is selling an asset to the public as an investment, it may fail the *Howey* test even if people buy it hoping its price will rise. Following the ruling, the SEC took steps in 2025 to clarify its stance on such tokens. On 20 March 2025, the SEC’s Division of Corporation Finance issued a public Staff Statement confirming that ordinary proof-of-work (PoW) mining activities do not constitute securities transactions.

The SEC emphasised that miners who validate blockchain transactions and receive block rewards are not investing in a common enterprise led by others, but rather contributing their computational work, thus failing *Howey*’s core requirement that profits be derived from the efforts of a separate promoter. The staff guidance concluded that participants in PoW mining, whether solo or in pools, “do not need to register” their activities under the Securities Act, as those mining rewards are more akin to a commodity-like payment for services than an investment of money for profit from an issuer’s efforts. This clarification aligned with what many in the industry long argued: Bitcoin, Ethereum (in its mining era), and similar PoW tokens are fundamentally outside the securities realm, absent some additional scheme.

The influence on stablecoins is subtler but equally important. Stablecoins are cryptocurrency tokens designed to maintain a stable value (often pegged 1:1 to a fiat currency, such as the US dollar). Buyers of genuine stablecoins generally do not expect to make a profit from holding them; their main purpose is transactional (using them as money or storing value). This lack of a profit motive indicates that most stablecoins also do not satisfy Howey’s third prong. In April 2025, the SEC issued formal guidance on certain stablecoins for the first time. On 4 April 2025, the Division of Corporation Finance released a “Statement on Stablecoins,” which addresses USD-pegged, fully reserved stablecoins (referred to as “Covered Stablecoins”). We will not delve further into stablecoins, as this issue has already been extensively studied. It is also worth noting that the US is close to passing stablecoin legislation under the name GENIUS. This law, which is now a bill approved by the Senate, explicitly distinguishes stablecoins from securities.

The staff concluded that offers and sales of fully collateralised payment tokens do not constitute the offering of securities under the 1933 or 1934 Acts. In the SEC’s view, these stablecoins are used as a means of payment or transfer of value, rather than as investments—they lack the speculative or profit-driven qualities typical of an investment contract. The guidance noted that as long as a stablecoin is fully collateralised by low-risk assets and redeemable one-for-one for fiat currency, it functions essentially like a digital dollar rather than a security. However, the SEC warned that other crypto assets mislabelled as “stablecoins,” but offering yield or relying on algorithms (rather than reserves), could still be scrutinised as securities or other regulated instruments. Essentially, by early 2025, the SEC had begun to define a more nuanced regulatory boundary: explicitly exempting certain PoW tokens and plain-vanilla stablecoins from the securities category, even while continuing to pursue cases of fraud and unregistered offerings in other crypto sectors.

Global Aftermath of *SEC v. Ripple*

While Judge Torres’s decision is not legally binding outside the United States, regulators worldwide closely observed the Ripple saga, often using it as a benchmark for their own regulatory approaches. In the United Kingdom, the crypto regulatory framework has developed significantly differently from the U.S. securities-focused model. The U.K. Financial Conduct Authority (FCA) and HM Treasury have long classified tokens like XRP as “exchange tokens,” a category of unregulated crypto-asset mainly used for payments or utility. In a January 2021 report, HM Treasury formally grouped XRP with Bitcoin and Ether as exchange tokens – neither e-money nor security tokens under U.K. law. In essence, British authorities indicated early on that XRP did not display the characteristics of a security or investment product. (This stance was reiterated in the U.K.’s financial promotions guidance and taxonomy of crypto-assets from 2019–2021.) Instead of trying to fit cryptocurrency into outdated definitions, the U.K. has been devising specialised rules.

In April 2025, HM Treasury published draft legislation to create a comprehensive regulatory regime for crypto assets, including new licensing requirements for exchanges, custodians, and stablecoin issuers, thereby bringing consumer protection and market integrity rules to the crypto market without labelling the tokens themselves as “securities”. The proposed rules would expand oversight beyond the prior focus on anti-money-laundering and advertising compliance, moving the U.K. toward a tailored framework that treats crypto-assets as a distinct class. The U.K.’s approach, therefore, stands in stark contrast to the U.S.: rather than litigating the status of tokens in court, U.K. regulators have largely assumed tokens like XRP are not securities and have worked to craft new law for the risks they do present (fraud, consumer harm, systemic concerns, etc.).

Across the Channel, **European Union** regulators noted the Ripple outcome as part of a broader transatlantic dialogue on crypto. The EU’s response, however, has been driven less by court cases and more by legislation. In 2023, the EU enacted the Markets in Crypto-Assets Regulation (**MiCA**), a sweeping law establishing a uniform framework for crypto-asset issuance and services across member states. MiCA deliberately avoids the U.S. path of shoehorning crypto into the traditional securities regime. Instead, it regulates crypto assets that are not already covered by existing financial laws (e.g. it exempts tokenised stocks or bonds, which remain under traditional securities rules).

Under MiCA, tokens like XRP (which confer no share, bond, or ownership rights) would generally be classified as “crypto-assets” subject to specific disclosure and compliance requirements. H**owev**er, they are not considered transferable securities or investment products. European policymakers have welcomed the EU's decision to create a new legislative framework rather than rely on lengthy litigation to define basic terms in the Ripple case. MiCA’s approach—defining categories such as “asset-referenced tokens” and “e-money tokens”—avoids the binary U.S. question of whether a token is a security, focusing instead on the registration of token issuers and exchanges, consumer disclosures, and reserve requirements for stablecoins. While *SEC v. Ripple* highlighted the uncertainties in the U.S., the EU has moved forward with a comprehensive regime that makes the security/non-security distinction less central. The industry response in Europe has been pragmatic: firms are preparing to comply with MiCA’s licensing and white paper rules by 2024–2025, rather than waiting for court battles.

Other jurisdictions also examined the Ripple decision through their own legal frameworks. In Singapore, for instance, regulators have never considered XRP under U.S. securities law. The Monetary Authority of Singapore (MAS) has explicitly stated that “the treatment of a token under the Howey Test is not a consideration” when determining if it is regulated under Singapore’s Securities and Futures Act. Singapore’s legislation does not even include the U.S.-style “investment contract” category. Instead, it categorises tokens based on their features: those functioning like securities (e.g., tokenised stocks or collective investment schemes) are regulated as such, while pure payment tokens, such as XRP, are governed under payment and anti-money-laundering laws, rather than securities laws. [34]

In fact, Ripple’s subsidiary in Singapore obtained a Major Payments Institution licence in 2023 to offer digital payment token services – a regulatory acknowledgement that XRP is regarded as a digital payment token within Singapore’s framework, rather than a capital markets product. Singaporean officials observed the U.S. Ripple case with interest, but it did not alter their approach; if anything, Judge Torres’s reasoning reinforced MAS’s functional approach that focuses on a token’s use case rather than applying a uniform label.

In the **United Arab Emirates (UAE)** – home to several crypto hubs – the Ripple outcome was also more validation than disruption. The UAE has proactively built a tailored regulatory environment for virtual assets. The Abu Dhabi Global Market’s Financial Services Regulatory Authority (ADGM FSRA), since 2018, has maintained a framework that differentiates between categories like “virtual assets,” “digital securities,” and “utility tokens.” Under the ADGM rules, cryptocurrencies such as Bitcoin or XRP, used as a medium of exchange or utility, are classified as commodities or payment assets rather than regulated securities; however, intermediaries dealing with them must be licensed.

The Dubai Virtual Assets Regulatory Authority (VARA) similarly licences crypto exchanges and issuers under a special regime outside traditional securities laws. In 2024, for example, Ripple gained approval under this regime to offer blockchain-based payment services in Dubai – an expansion based on UAE law recognising XRP as a regulated virtual asset, not an unregistered security. UAE regulators observed the Ripple case in the U.S., but it did not change their approach; the UAE’s priority remains on strong licensing of crypto activities (with consumer protection rules and compliance standards), rather than on classifying tokens as securities or not. In fact, a leading UAE regulator remarked that the prolonged U.S. legal battle only highlighted the benefits of the UAE’s clear licensing approach for virtual asset service providers.

In Australia, the Ripple decision arrived amid the country’s ongoing efforts to reform its crypto regulation. Australia’s legal system, like Singapore’s, does not rely on a *Howey*-style test; instead, a crypto token may be regulated as a financial product (such as a security, derivative, or managed investment scheme) if it falls within one of those definitions, otherwise it remains unregulated. To date, Australian authorities have not deemed XRP to be a financial product, and no enforcement action similar to that taken against Ripple has occurred. Australian regulators and lawmakers have taken a deliberate approach: in early 2023 the Treasury launched a “token mapping” initiative to categorize different types of crypto assets and assess how existing laws apply. The goal is to craft a tailored legislative framework rather than to stretch the definitions of “security” or “financial product” to cover every token. Australian officials observing Ripple have echoed the view that relying on 80-year-old legal concepts for crypto is problematic, which is why the government is working on new regulations (including potential licensing for crypto asset service providers) informed by the token mapping exercise. In short, Australia, like the U.K. and EU, is moving toward explicit crypto-specific regulation – a route that may avoid the kind of uncertainty exemplified by the Ripple litigation.

Conclusion: A New Chapter for Crypto Jurisprudence

The legacy of *SEC v. Ripple Labs* is still unfolding, but its influence is undeniable. In the United States, the case led to the first judicial delineation of how federal securities laws apply to different modes of token sales. It demonstrated the possibility of a middle ground between labelling an entire blockchain ecosystem as a securities offering and categorically declaring the token outside regulation. The SEC’s enforcement strategy is already adjusting in light of the ruling – future complaints against crypto issuers are likely to plead their facts more carefully to satisfy *Howey* under the circumstances of both primary and secondary sales. Crypto firms, for their part, have been rethinking how they raise funds and distribute tokens. In the aftermath of Ripple, many projects are steering away from public ICOs to avoid “Ripple-like” scenarios – for example, by airdropping tokens to users, selling only to accredited investors via private SAFT (Simple Agreement for Future Tokens) deals, or emphasising tokens earned through network participation rather than purchased as investments. The distinction drawn in Ripple – between an issuer actively soliciting investment versus a token simply trading on the open market – provides a roadmap for these projects to structure themselves on the “non-security” side of the line.

Ultimately, the lengthy dispute and fragmented outcomes in *SEC v. Ripple* have intensified calls for legislative clarity. Even Judge Torres’s considered opinion is just one trial court’s perspective, and contrasting decisions (such as Judge Rakoff’s in *SEC v. Terraform Labs*, which disagreed with parts of Ripple’s reasoning) demonstrate that judicial views can differ. The uncertainty and costly litigation surrounding crypto tokens highlight that relying on 1930s-era concepts, such as “investment contract,” to regulate 21st-century digital assets is a recipe for confusion. As one U.S. lawmaker remarked, expecting courts to equate oranges with XRP is neither efficient nor sustainable. Following Ripple, there is a rising bipartisan call in Congress for a new statutory framework that clearly differentiates when a digital asset falls under securities law versus commodity or banking regulation. Whether such legislation will materialise remains uncertain. In the meantime, Ripple represents a crucial moment in crypto law – a case that has simultaneously challenged the SEC’s broadest theories, affirmed its core authority in direct cases of capital-raising, and ignited a global debate about the best way to integrate cryptocurrencies into the regulatory framework. The maze of crypto regulation is far from fully mapped, but thanks to the Ripple case, we now have a clearer guide than ever before.

Yuriy Brisov *is a London-based lawyer with over 20 years of legal experience, including more than a decade specializing in blockchain, cryptocurrency, and digital regulation. He is a partner at D&A Partners and co-founder of CryptoMap, a platform designed to help businesses navigate the complexities of global cryptocurrency jurisdictions. He holds advanced law degrees from institutions in both the United States and Russia. Throughout his career, Yuriy has advised a wide range of international blockchain projects—including Entangle, NOBELDAO, IOGINALITY, GoMining, MIDAS, TravelGo, EVEDEX, Binance, and Waves—on operational structuring, regulatory compliance, and strategic engagement with regulators. He has also worked closely with governments and regulatory bodies in the UK, US, UAE, Estonia, Serbia, Kazakhstan, Bahrain, and Australia, contributing to the development of forward-looking frameworks for digital assets, cryptocurrency taxation, and smart contract regulation.*

Are Stablecoins Bank Deposits?

By Olu Omoyele

Introduction

As stablecoins continue to gain ground rapidly in global finance, a fundamental legal and regulatory question has emerged: Are stablecoins bank deposits? This isn't just a matter of classification or semantics – it affects how stablecoin issuers are regulated, how users are protected, and who is allowed to operate in this fast-evolving sector.

Yet, the question of what constitutes a deposit is not a new one and predates crypto innovation. In the UK and EU, the legal distinction between deposits and electronic money (e-money), for instance, has led to a proliferation of bank-like financial technology (FinTech) firms that hold customer money without being treated as bank deposits, despite being repayable at par e.g. firms like Wise, Revolut, and Tide. So, why is there a contentious debate about the treatment of stablecoins?

But first…

What is a Stablecoin?

A stablecoin is a cryptocurrency or digital asset designed to maintain a stable value, typically pegged to the value of a fiat currency or a basket of assets. They come in various forms, including fiat-backed stablecoins like USDC and USDT (backed by reserves held in bank accounts or government securities), crypto-collateralized stablecoins like DAI (backed by overcollateralized crypto assets), and algorithmic stablecoins (which use supply-demand mechanisms to maintain their peg, though often with instability, as seen with the collapse of TerraUSD).

The question of whether stablecoins are deposits relates only to fiat-backed stablecoins, as these most closely resemble traditional money instruments. They are typically backed by reserves held in bank accounts or short-term (i.e. liquid) government securities.

Stablecoins aim to combine the speed, programmability, and borderlessness of crypto with the stability of fiat currencies. They're often used for payments, trading, lending, and remittances, or as a store of value. But this hybrid nature has raised regulatory questions, particularly around how to classify and supervise them.

What is a Bank Deposit?

In general, a bank deposit is defined as money placed with a bank, with an obligation to repay, at par, either on demand or at an agreed time in future. The precise legal definition can vary by jurisdiction, but deposits are repayable claims against a bank that uses the funds for its own account, often in lending or investments.

The activity of accepting deposits is a tightly regulated activity usually reserved for licensed banks.

Stablecoins vs Deposits

At first glance, fiat-backed stablecoins resemble deposits: holders exchange fiat for digital token which is redeemable at par. However, key differences exist, for example, most stablecoin issuers do not engage in lending activity; instead, they hold the fiat they receive in custodial accounts or short-term government bonds.

Like bank deposits, which represent a claim on the issuing bank, stablecoins represent a claim on its issuer. However, since most stablecoin issuers are not banks (although this may be set to change as traditional banks enter the space), this raises concerns about the enforceability of those claims in the event of an issuer's insolvency, especially as stablecoins are not covered by deposit insurance schemes – such as the FDIC in the US, the NDIC in Nigeria, or the FSCS in the UK – leaving holders exposed to potential losses.

Are Stablecoins Bank Deposits?

Due to these structural differences, regulators have been hesitant to treat stablecoins as deposits. Still, classification depends on design and marketing. If an issuer receives fiat, promises repayment, and offers the service to the public, it risks being seen as accepting deposits without a license.

Stablecoins vs Electronic Money

In the EU and UK, electronic money (e-money) provides a more appropriate regulatory analogy than deposits. Under the EU's E-Money Directive and the UK's Electronic Money Regulations 2011, e-money is a monetary value stored electronically and represents a claim on the issuer. Like fiat-backed stablecoins, e-money is issued in exchange for fiat, and is redeemable at par value at any time.

Critically, e-money issuers must safeguard user funds, usually through segregation in a trust account or an insurance guarantee, and they cannot lend those funds, unlike deposit-taking banks.

Does Classification Matter?

Treating stablecoins as bank deposits would have major implications. Only licensed banks would be able to issue them, shutting out most FinTechs and crypto-native firms like Tether and Circle.

This would bring far stricter capital, liquidity, and compliance requirements, while in return offering deposit insurance cover. But in this instance, the business model of stablecoin issuers would be radically different as they would be able to trade with the funds on their own account, thus exposing them to significantly greater risks.

Classifying stablecoins as e-money, by contrast, imposes lighter regulation but still ensures full reserve backing, asset safeguarding, and redemption rights.

So, Are Stablecoins Bank Deposits?

The short answer is No, stablecoins are not deposits. Just because your money is safeguarded by a third party and is repayable does not make it a deposit. After all, e-money is precisely such an example that is not considered a deposit. There are others too, such as money market funds, commercial paper, and so on, where repayable/redeemable funds are kept with others without becoming deposits.

If you take the analogy further, there are many other types of entities that safeguard money but are not considered deposit-takers (i.e. banks), such as payment platforms (e.g. PayPal), stockbrokers (e.g. IG), and even coffee shops (e.g. Starbucks).

What makes something a deposit is not whether it is repayable, but what can be done with the funds. Where the entity holding the funds (i.e. the issuer) can trade with them on their own account, these are deposits. It follows, therefore, that where the issuer is forbidden from trading with the funds and must instead safeguard them in segregated accounts, these are not deposits.

As such, stablecoins that are fully backed and redeemable functionally resemble e-money far more than bank deposits and, logically so, their legal and regulatory treatment should be akin to e-money, not deposits.

Thankfully, this is the approach taken by the EU's Markets in Crypto-Assets Regulation (MiCA), which treats stablecoins that are pegged to a single fiat currency as a new category of e-money, the E-Money Token (EMT), with similar obligations to e-money for safeguarding and redemption. The UK is following suit, bringing fiat-backed stablecoins under the oversight of the Bank of England and the Financial Conduct Authority (FCA). In Singapore, under the Payment Services Act, stablecoins may qualify as e-money if they are backed by fiat currencies and redeemable. Issuers are required to safeguard user funds, but are not considered deposit-taking institutions.

MiCA also introduces a separate category for stablecoins backed by a basket of assets, including commodities, multiple fiat currencies, or other crypto assets – these are called Asset-Referenced Tokens (ARTs). While MiCA treats ARTs as a distinct class of asset, it treats EMTs merely as an extension of the existing e-money concept.

Looking ahead

Stablecoins represent a new frontier in the evolution of money, sitting at the intersection of traditional finance and digital innovation. By combining the stability of fiat currencies with the efficiency of blockchain technology, they offer a compelling alternative for payments, remittances, and on-chain financial services.

Whether stablecoins are classified as deposits is ultimately a legal and policy choice – not just a technical question. Regulating them as e-money strikes the right balance, allowing innovation and competition while protecting users through reserve, redemption, and transparency requirements.

As stablecoins become increasingly embedded in the global financial infrastructure, clear legal frameworks are essential. These decisions will shape not just how stablecoins are regulated, but the broader architecture of digital money for years to come.

Olu Omoyele *is the founder and CEO of DeFi Planet, a leading Web3 media publication. He has over 20 years of experience spanning both the public and private sectors, with deep expertise in financial regulatory policy and banking risk management. His career includes roles as a regulator at the Bank of England and as a Director at Bank of America Merrill Lynch.*

Olu is an independent regulatory consultant, and he holds a postgraduate degree in Financial Law from King’s College London and a certificate in Blockchain Technologies: Business Innovation and Application from MIT Sloan. He currently serves as a senior advisor to Gora, a decentralized blockchain oracle, and as a governor on the Algorand blockchain.

Passionate about the transformative potential of Web3, Olu is driven by its promise to enable decentralized governance, enhance operational efficiency, and usher in a new era of trustless systems. He believes that broad adoption of Web3 depends on access to clear, accurate, and timely information—and he’s committed to making that a reality.

Liquid Staking under MiFID II

By Emanuele Gambula

1. Introduction

Liquid staking has emerged as a popular innovation in the realm of decentralized finance ("**DeFi**"), raising complex questions about its legal classification under European financial and banking laws. The scope of this article is to examine whether liquid staking falls within the scope of Directive 2014/65/EU ("**MiFID II**") *i.e.* whether liquid staking tokens should be treated as a financial instrument (such as transferable securities, derivatives, or structured deposits). On the other hand, it shall be assumed that further legal considerations could arise when similar DeFi applications (*e.g.* yield farming) are viewed under the lenses of a structure that resembles a collective investment undertaking. This matter is not merely academic: liquid staking protocols like Lido (which issues stETH tokens on Ethereum) manage tens of billions in assets, and Rocket Pool (issuer of rETH) provides an alternative decentralized staking solution. The regulatory characterization of these liquid staking tokens (sometimes colloquially called "*staking derivatives*") will determine which legal regime applies, with significant implications for investor protection, licensing, and oversight.

For the purpose of this article, some further considerations shall be made: (i) we draw on recent European Securities and Markets Authority ("**ESMA**") guidelines on the conditions and criteria for the qualification of crypto assets as financial instruments issued March 19, 2025 and academic commentaries to provide a comprehensive legal analysis, before concluding with a clear answer on MiFID II applicability; and (ii) in this article we will not consider the implication of staking under the Regulation (EU) 2023/1114 ("**MiCAR**"), which does not contain specific provisions regarding staking; thus, to the extent of the limitations set therein, MiCAR "*It does not therefore prohibit staking, and staking as such is not subject to specific requirements or licensing*".

2. Staking vs. Liquid Staking: A Technical Overview

Staking in a proof-of-stake blockchain refers to locking up a cryptocurrency (*e.g.* ETH on Ethereum) to support network consensus and security, in return for periodic rewards (newly minted tokens or fees). Traditionally, staked tokens are illiquid during the staking period, they cannot be transferred or traded until they are unstaked. In this regard, one should also consider the definition provided by ESMA on one of its Q&A (June 20, 2024); specifically, ESMA defines staking as "*the process of immobilizing crypto assets to support the operations of proof-of-stake and proof-of-stake-like blockchain consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards*".

By contrast, liquid staking allows holders to stake their assets via a third-party protocol and receive in exchange a liquid token that represents their staked position. This liquid staking token can be freely transferred, traded, or used especially in DeFi applications while the original asset remains locked in the staking contract. In essence, liquid staking "unlocks" the liquidity of staked assets by issuing a wrapped or derivative token (in technical terms) that functions as a certificate of ownership over the staked asset. For example, when a user stakes ETH through Lido, they receive stETH, a token representing their claim on the pooled ETH and any accrued rewards. Similarly, Rocket Pool's protocol issues rETH to depositors, representing staked ETH plus yields. These tokens are fungible and tradeable, namely: stETH is interchangeable with any other stETH and can be sold on secondary markets or used as collateral in loans. Critically, holding the liquid staking token confers the right to redeem or swap it later for the underlying staked asset (plus accumulated rewards, once unstaking is possible). However, unlike traditional financial instruments, liquid staking tokens typically do not carry governance or profit-sharing rights in a business enterprise. They do not give the holder equity-style rights such as voting in a company or dividends, nor debt-style rights to fixed interest payments. Instead, the only "return" is the crypto staking yield automatically accruing to the token (through protocol mechanics), and any increase in the token's market value. In short, a liquid staking token is a receipt for a share of a pooled asset and its yield, without additional entitlements one would expect from traditional securities or debt instruments.

3. Transferable Security Analysis under MiFID II

MiFID II defines "transferable securities" as "*those classes of securities which are negotiable on the capital market, with the exception of instruments of payment*". This definition encompasses typical shares, bonds, and comparable securities, including any other securities giving rights to acquire/sell or yielding cash-settled returns by reference to underlying assets. To determine if a crypto asset is a transferable security (and thus a financial instrument under MiFID II), ESMA's new guidelines emphasize three cumulative criteria: (i) the asset is not a means of payment, (ii) it is issued as part of a class of securities (*i.e.* fungible and interchangeable tokens conferring identical rights within that class), and (iii) it is negotiable on the capital market. Liquid staking tokens arguably meet some of these formal criteria but not others. They are certainly fungible tokens issued in large numbers on a blockchain (for example, all stETH tokens confer the same rights pro rata to their holder) and are negotiable, being freely transferable and traded on crypto markets. Moreover, they are not used as general-purpose payment instruments (their primary role is as investment representations, not as currency for buying goods), satisfying criterion (i).

However, the more nuanced question is whether liquid staking tokens belong to a “class of securities” in the substantive sense intended by MiFID II. ESMA advises that one must look to whether the rights granted by the token are equivalent to those of traditional securities like shares or debt instruments. In this regard, liquid staking tokens diverge significantly from classic securities. They do not confer ownership in a corporate entity or any governance rights over an issuer’s management in the manner of shares. Any “voting” rights attached to such tokens are typically limited to protocol parameters or technical updates, not shareholder votes on corporate matters, a distinction the ESMA guidance highlights as crucial (tokens only allowing votes on protocol or platform updates are not to be treated as shares). Likewise, a liquid staking token does not represent a debt obligation of an issuer who promises repayment of principal with interest; there is no issuer credit risk or scheduled coupon.

As noted, no promise of dividends or interest payments exists, the holder’s gain is simply their proportionate share of blockchain-generated rewards. ESMA’s guidelines explicitly point out that if a token lacks the typical financial returns of securities (*e.g.* dividends or interest) and the usual membership rights of a class of securities, it should not be classified as a security even if investors purchase it hoping for profit from its price appreciation.

This is directly applicable to liquid staking tokens: an investor might buy stETH anticipating that its value in ETH will increase as staking yields accrue, but that expectation alone does not transform stETH into a share or bond. Accordingly, liquid staking tokens likely fail to qualify as transferable securities under MiFID II, because they do not embody the essential rights of shares, bonds, or similar instruments. They are better understood as novel crypto assets that fall outside the traditional categories of equity or debt.

4. Transferable Security Analysis under MiFID II

Another angle is to ask whether a liquid staking token could be considered a derivative under MiFID II. Derivatives (such as options, futures, swaps, forwards, and contracts for differences) are financial instruments whose value references an underlying asset or metric and often involve a contractual obligation for future performance or cash settlement. At first glance, a liquid staking token’s value does depend on an underlying asset, for example, the price of ETH and the amount of ETH staking rewards. Industry parlance even labels these tokens “staking derivatives.”

Legally, however, it might be argued that liquid staking tokens do not fit well into the derivative category. They are not structured as contracts obligating two parties to exchange cash or assets at a future date based on some underlying reference price. Instead, a liquid staking token (“**LST**”) functions more like evidence of current ownership in a pool of assets. There is no separate bilateral contract whose value fluctuates with an external reference; the token embodies a direct *pro-rata* claim on the underlying staked asset. In other words, the token’s value is established algorithmically by the amount of reserve asset backing it, rather than *“synthetically” referencing* an external asset or index.

The ESMA guidelines make precisely this distinction: when a token’s value is determined by reserved assets (assets set aside to back the token), then according to ESMA, the token should be considered an asset-referenced crypto asset under MiCAR, rather than a derivative. Liquid staking tokens fall in this category each stETH, for example, is fully backed by a certain fraction of ETH actually held (staked) in the protocol’s smart contracts. There is no discretionary management or complex formula determining stETH’s value; it is essentially a bookkeeping ratio reflecting the real assets in reserve (the pool of staked ETH and accumulated rewards) and the total token supply. This stands in contrast to a true derivative, like a cash-settled futures contract, whose value is defined by reference to an external price index, and which involves an agreement to exchange payments at a future date.

Furthermore, liquid staking arrangements do not exhibit the hallmark of derivatives whereby rights and obligations are contingent on a future event or date. With a typical derivative (say a forward or swap), there is a time-lag between entering the contract and its performance (settlement) during which the payoff is contingent on future market movements. By contrast, when one acquires a liquid staking token, one’s rights (the claim on underlying ETH plus any ongoing rewards) arise immediately and continuously, not upon a future contractual settlement date. In this sense, an LST is more akin to holding the underlying asset itself than to entering a derivative contract about the asset. ESMA’s guidance highlight that if a crypto asset “exists as a standalone asset” and does not derive its value from specified underlying assets in the MiFID sense (like securities, commodities, etc. referenced in a contract), it should be distinguished from derivative contracts. Liquid staking tokens exist as standalone tokenized claims and do not require cash settlement or involve leverage and speculation in the manner of derivatives. They also are not covered by the specific classes of derivatives listed in Section C (points (4) to (10)) of Annex I of MiFID II (which enumerate options, futures, swaps, forward rate agreements, etc., including commodity, interest rate, currency and other derivatives). An stETH or rETH is plainly not an option or swap, nor is it a contract for differences: it grants no right to receive a payment based on the difference between two prices. It is simply redeemable (or exchangeable) for the underlying ETH (subject to the protocol’s unstaking mechanics). In sum, liquid staking tokens are not derivatives under MiFID II’s definitions. As ESMA in its guidelines noted, if a token’s “value or performance” is determined by *synthetically referencing* another asset or right, one should analyze it as a potential financial instrument (derivative). But if, as here, the token’s value is anchored by real, reserved assets and grows primarily through the algorithmic accumulation of those assets (rather than an external index or the efforts of a counterparty), it should *not* be considered a derivative contract. The prevailing view is that calling these tokens “derivatives” is a misnomer; they are better characterized as asset-backed tokens or even “receipt tokens” representing a bailment-like relationship in crypto terms, rather than contracts for speculative gain.

5. Deposit and Structured Deposit Consideration

MiFID II's list of financial instruments also includes structured deposits, and one might analogize a liquid staking token to a deposit receipt or a form of structured product. After all, when using liquid staking, the participant is effectively depositing an asset (ETH) into a protocol and receiving a token in return; this resembles how a bank customer deposits money and receives a bank account balance (or a certificate of deposit in some cases). Could an LST be regarded as a deposit or structured deposit under EU financial law? Upon examination, the answer should be negative. Deposits in EU law are stringently defined and are fundamentally tied to fiat money and banking institutions. The Directive 2014/49/EU ("**Deposit Guarantee Schemes Directive"** or "**DGSD**") defines "deposit" as a credit balance resulting from funds left in an account with a credit institution, which the institution is obliged to repay under legal and contractual conditions. Importantly, the notion of deposit in the DGSD (and consistently in the Regulation (EU) No 575/2013 (CRR)'s definition of the regulated activity of taking deposits) assumes fiat or scriptural currency and a banking relationship. Crypto-assets like ETH are not legal currency, and protocols like Lido are not credit institutions. Moreover, the DGSD explicitly excludes certain balances from being considered deposits, including those where the principal is not repayable at par (*i.e*. not guaranteed to be returned in full nominal amount). A liquid staking token fails this criterion: if you stake 1 ETH and receive 1 stETH, the "exchange rate" between stETH and ETH is not fixed one-to-one over time. As staking rewards accrue, 1 stETH entitles you to an increasing amount of ETH (or conversely, protocols like Rocket Pool issue rETH in such a way that each rETH grows in ETH value). The result is that the holder will not be repaid a fixed sum equal to their original contribution; the value of their token in terms of the underlying can fluctuate (generally upward, aside from slashing risks). This means the token is not repayable at face value on demand or at any specific maturity date thus missing a key attribute of deposits (indeed, DGSD excludes balances whose principal is not repayable at parfitd.it). Additionally, the currency element would be ETH, which is not official currency; and more pertinently, the amount of ETH returned is not fixed. Thus, treating liquid staking as a deposit-taking activity would be inconsistent with the letter and spirit of deposit insurance and banking. Not surprisingly, liquid staking providers do not come with deposit guarantee protection: users bear the risk of loss (*e.g.* from slashing or smart contract failure), unlike bank depositors protected by DGSD schemes. As per structured deposit, MiFID II Article 4(1)(43) defines "structured deposit" as a deposit fully repayable at maturity where interest or a premium is payable according to a formula that is linked to an index, financial instrument, commodity price, or other benchmark. This essentially covers bank products where your return (beyond guaranteed principal repayment) is tied to some market indicator, for example, a 5-year note that guarantees your principal back, plus an interest amount equal to, say, 50% of any upside in a stock index. A liquid staking token again does not meet this definition. Firstly, as noted, there is no fixed maturity or term for an LST and the holder can typically redeem whenever the underlying network allows unstaking (and in protocols like Lido, there is no set end date at which your stETH is "due" *i.e*. it exists indefinitely until you choose to redeem or sell it). It is therefore not a time-bound instrument with a maturity date at which full repayment is promised. Secondly, it is not "fully repayable at maturity" in the sense of guaranteeing the return of a fixed principal amount; the value of the token at any future point depends on variable factors (stake rewards and ETH price) and could be higher or lower in underlying terms. Thirdly, the "yield" on an LST is not a pre-defined interest or premium determined by a formula referencing an external index or rate. Instead, the "interest" the holder earns is the ongoing protocol reward (new ETH issuance for staking) which is algorithmically added to the pool. This reward rate is determined by the blockchain protocol's rules (and network conditions like total stake and inflation rate), not by a formula set out *ex ante* by the "product manufacturer" referencing financial indices. For instance, a structured deposit might say "*pays 5% if EURIBOR is above X%,*" whereas stETH simply grows at whatever rate Ethereum's consensus mechanism delivers, which is not a contractual formula but an emergent network outcome. To conclude, liquid staking tokens are not structured deposits: they lack a set maturity, are not repaid at par, and have no predefined formulaic interest tied to financial benchmarks.

6. Conclusion

It has been found that liquid staking tokens (*e.g.*, stETH, rETH) typically might not fall within MiFID II taxonomy of any financial instrument. ESMA has reinforced a "substance-over-form" view, stating that only tokens mirroring the characteristics of shares, bonds or derivatives should be treated as financial instruments. LST could potentially fall instead under MiCAR assuming that the issuer would be sufficiently centralized so that a clearly identifiable natural or legal person can be legally deemed as the "issuer" and/or as a "Crypto Asset Service Provider" whereas, pursuant to Recital 22 MiCAR, a fully decentralised protocol without an "identifiable issuer" should be exempted from MiCAR's scope, provided that in any case Crypto Asset Service Providers providing services with respect to LST should be in scope of MiCAR.

__Emanuele Gambula__ is admitted to practice law in Italy. He graduated cum laude and completed a research thesis on the application of blockchain technology within civil enforcement laws, as well as obtained the certification on Computer Science for Lawyers course (CS50L). He did his internship in one of the top tier international law firm in Milan, where he specialized in data protection, legal tech and consumer law. During his internship he completed a specialization course in blockchain, with a final project on the tokenization of derivative instruments. After that, he started working in one of the biggest Italian law firm, where he developed his main expertise in banking law, financial regulations, fund formation (UCITS, FIA and ELTIF funds) and FinTech.

Biography:

- X. Xiong, Z. Wang, X. Chen, W. Knottenbelt, M. Huth, *Leverage Staking with Liquid Staking Derivatives (LSDs): Opportunities and Risks*, January 4,2025.
- Artt. 40 and 50 of MiCAR.
- ESMA, *Questions and Answers*, ESMA_QA_2067, June 20,2025.
- EBA, *Report on the eligibility of deposits, coverage level, and cooperation between deposit guarantee schemes*, August 8, 2019.

The European Blockchain Sandbox

By Michael Jünemann and Marjolein Geus

I. Introduction

The European blockchain regulatory sandbox for Distributed Ledger Technologies ("**European Blockchain Sandbox**") is a European Commission ("**EC**") initiative that creates a pan-European framework for a cross-border regulatory dialogue between Distributed Ledger Technology ("**DLT**")/blockchain innovators in the private and the public sector and regulators and regulatory authorities on national and European Union ("**EU**") level (1). It aims to enhance legal certainty for innovative DLT/blockchain applications and facilitate the development of best practices in this area.

The term "sandbox" is used for different testing environments that often involve testing and/or derogation from existing legislation or regulatory approval. The characteristics of the European Blockchain Sandbox are different compared to other sandboxes. The European Blockchain Sandbox provides a framework for a confidential and informal cross-border regulatory dialogue between regulators/authorities and innovators covering a range of different regulatory areas. Use cases that are participating in the European Blockchain Sandbox are selected on the basis of transparent and non-discriminatory application terms and selection criteria. The European Blockchain Sandbox does not provide a framework for derogation of certain laws or regulations and the participating use cases are not "approved" by the participating regulators/authorities. Also, the dialogues that are taking place as part of the European Blockchain Sandbox are normally less time-consuming than participation in a sandbox that includes regulatory and operational testing. Best practices, lessons learned and areas for clarification that are identified during the regulatory dialogues are made available for the wider community through the publication of best practices reports and public webinars.

The sandbox is open for a broad range of DLT/blockchain use cases in the public and the private sector, also in combination with other technologies such as Artificial Intelligence ("**AI**") and Internet of Things ("**IoT**"), with an emphasis on topics that are of relevance across sectors and regions. Particular focus is on areas of application where novel legal and regulatory questions arise in the financial sector and other key sectors such as sustainability, health, supply chain and logistics/trade, mobility and energy. Important regulatory areas include financial sector regulation, data protection and regulation of non-personal data, Environmental, Social, and Governance ("**ESG**") regulation, electronic Identification, Authentication and Trust Services ("**eIDAS**"), cyber security regulation, consumer protection, smart contracts for automated data processing, liability issues and Anti-Money Laundering ("**AML**")/Know Your Costumers ("**KYC**") rules.

II. The classic "Regulatory Sandbox"

Compliance with the regulatory requirements in the financial sector is not only associated with a certain organisational effort, but also with greater financial expenditure. In particular, the licence requirement in financial sector (2) regulation will make it more difficult for young companies, in particular to enter the market (3) and, under these circumstances, there is also a certain amount of risk: they will have to invest time and money in order to be able to launch their business on the market at all. However, they often have no opportunity to evaluate their business model in advance and have increased difficulties in assessing its market opportunities on the basis of test series. This can create a high barrier to market entry for young entrepreneurs particularly, but also for more mature entrepreneurs, and consequently lead to innovations being prevented. The so-called classic "regulatory sandbox" in the financial sector is a concept that offers financial institutions and companies a controlled space to test innovative fintech solutions with the support of an authority for a limited period of time so that they can validate and test their business model in a secure environment and thus preventing the above-mentioned supervisory regulations problems (4).

III. Overview of the project "European Blockchain Sandbox"

The European Blockchain Sandbox was launched in 2023. However, as mentioned above this is not a classic regulatory sandbox for testing a business model, but a framework to enhance a cross-border regulatory dialogue between authorities/regulators and innovators in a safe and confidential environment. Over three years, starting in 2023, 20 innovative DLT/blockchain use cases are selected covering different industry sectors and European Economic Area ("**EEA**") regions to engage in the confidential and informal cross-border regulatory dialogues with relevant national and EU regulators and authorities. To the extent that best practices/recommendations are identified during the confidential and informal dialogue meetings that can be shared with the wider community, these are published in the form of best practices report, but only with the consent of the participants and never with a link to individual use cases.

1. The First Cohort

Therefore, the selected use cases in the first cohort have been successfully matched with well over 50 national and EU regulators/authorities from across the EU/EEA and covering a broad range of regulatory areas. The results of the regulatory dialogues for the first cohort have been shared with the wider community as a best practice report in June 2024 without disclosing confidential information in order to facilitate a secure and confidential dialogue on relevant regulatory issues allowing innovators to understand better relevant laws and regulations and allowing authorities and regulators to understand better innovative DLT technologies from a regulatory and legal perspective.

As mentioned, the reports with best practices and lessons learned as a result of the combined experiences will always respect confidentiality from the part of the use cases and the regulators/authorities. The approach during the dialogues of the first cohort depended on the use case and the area(s) of regulation:

☐ Several dialogues focused on regulatory compliance by DLT/blockchain use cases. Examples are the dialogues with a focus on the Regulation (EU) 2016/679 (General Data Protection Regulation – "**GDPR**"), cyber security, AML, Regulation (EU) 2023/1114 (Markets in Crypto-Assets Regulation – "**MiCAR**") and financial sector regulation. During these dialogues, valuable guidance was provided by the participating regulators/authorities to the use cases which resulted in best practices and lessons learned which are presented in the best practices report.

☐ Other dialogues focused on how the use of DLT/blockchain applications can support efficient and effective compliance and oversight. Examples of the use of DLT/blockchain as an extra tool, making compliance and oversight more efficient, were discussed in the customs area, battery passports/Digital Product Passports ("**DPPs**"), cultural asset passports and carbon dioxide ("**CO2**") reporting (EU Emissions Trading System ("**ETS**")/Monitoring, Reporting and Verification ("MRV").

☐ Finally, the dialogues for some use cases focussed on EU regulation as a facilitator such as (i) the use of the European Union Digital Identity ("**EUDI**") wallet and new categories of qualified trust services in scope of the Regulation (EU) 2024/1183 ("**eIDAS 2**") , (ii) the possibility to qualify as a recognized Data Altruism Organisation ("**DAO**") in the sense of the Regulation (EU) 2022/868 ("**Data Governance Act**"), as a possibility to enhance credibility of a DLT/blockchain use case and (iii) the possibility to qualify as a recognized DAO in the sense of the Data Governance Act.

2. The Second Cohort

The use cases selected for the second cohort have again been successfully matched with a broad group of national and EU regulators and authorities from across the EU/EEA, covering diverse regulatory fields. The dialogues built on the experience from the first cohort and further deepened the confidential and constructive exchange on regulatory challenges and innovation opportunities. The best practices and key insights from the second cohort have been shared with the broader public in the second cohort best practice report in April 2025, in line with the principle of preserving confidentiality and without referencing individual use cases.

The dialogues for the second cohort could benefit from the lessons learned and best practices from the first cohort allowing for deeper dives into specific areas and taking into account new regulatory developments.

As with the first cohort, the dialogues in the second round followed different regulatory themes depending on the specific use case:

➢ A number of dialogues again focused on regulatory compliance issues. Particular attention was paid to the GDPR, the Regulation (EU) 2024/1689 ("**AI Act**"), data regulation, sanctions lists, AML, MiCAR and financial sector regulation. During these dialogues valuable guidance was provided by the participating regulators/authorities to the use cases which resulted in best practices and lessons learned presented in the best practices report. These best practices and lessons learned are presented on a generic level and are not specifically linked to individual use cases or dialogues. In view of the ongoing regulatory developments in each of these areas, these will likely again become relevant topics in the third round of dialogues.

➢ Other dialogues emphasized the supportive function of DLT/blockchain for regulatory oversight and enforcement. Examples of the use of DLT/blockchain applications as an extra tool, making compliance and oversight more efficient, were discussed in connection with the AI Act, battery passports/DPPs, the Regulation (EU) 2023/1115 (EU Deforestation Regulation – "**EUDR**") and the Directive (EU) 2022/2464 (Corporate Sustainability Reporting Directive – "**CSRD**"). The use of DLT/blockchain as part of mandatory monitoring, reporting and oversight will likely again become a relevant area for the dialogues in the third cohort.

➢ Finally the use of new areas of regulation and existing or new regulatory tools and qualifications with a focus on regulation as a facilitator were discussed in some of the dialogues, such as (i) the use of legal wrappers for DAOs, (ii) the use of the EUDI Wallet and new categories of qualified trust services in scope of the eIDAS 2 Regulation, (iii) the introduction of the EU corporate certificate and the digital EU power of attorney in the latest amendment of the Directive (EU) 2017/1132 ("**Company Directive**"), (iv) the possibility to qualify as a recognized data intermediation service in the sense of the Data Governance Act and the use of EU harmonized regulatory instruments such a MiCAR and the Regulation (EU) 2022/858 ("**DLT Pilot Regime**").

The European Blockchain Sandbox is organised by a consortium led by Bird & Bird with its consultancy arm OXYGY and blockchain experts from Warren Brandeis while the website development is undertaken by Spindox. A panel of independent academic experts from European universities is overseeing the application and selection process for the annual selection of use cases and is in the lead for the annual most innovative regulator award.

IV. Objectives of the European Blockchain Sandbox

DLT/blockchain innovators are to be given a better understanding of the regulatory framework for compliance reasons and also to make use of EU regulatory instruments. In addition, the project aims to raise awareness among authorities, public bodies and DLT/blockchain innovators for a better understanding of innovative technologies and potential regulatory challenges as well as possible solutions. Furthermore, the project aims to identify best practices and lessons learned which are shared in the form of annual best practice reports.

V. Course of the selection procedure

For each cohort, the programme set-up and the application and selection process are important. Applications for the first cohort could be submitted using a form that was made available via the project website (link) and could be submitted until 14 April 2023. Uploading and completing the forms involved time and effort for the participants, as information about the use case and the selection criteria was requested in detail. By the end of the application term almost 90 applications had been received from across all EU/EEA regions. The selection by independent blockchain experts and a panel of independent academic experts was completed by the end of June 2023.

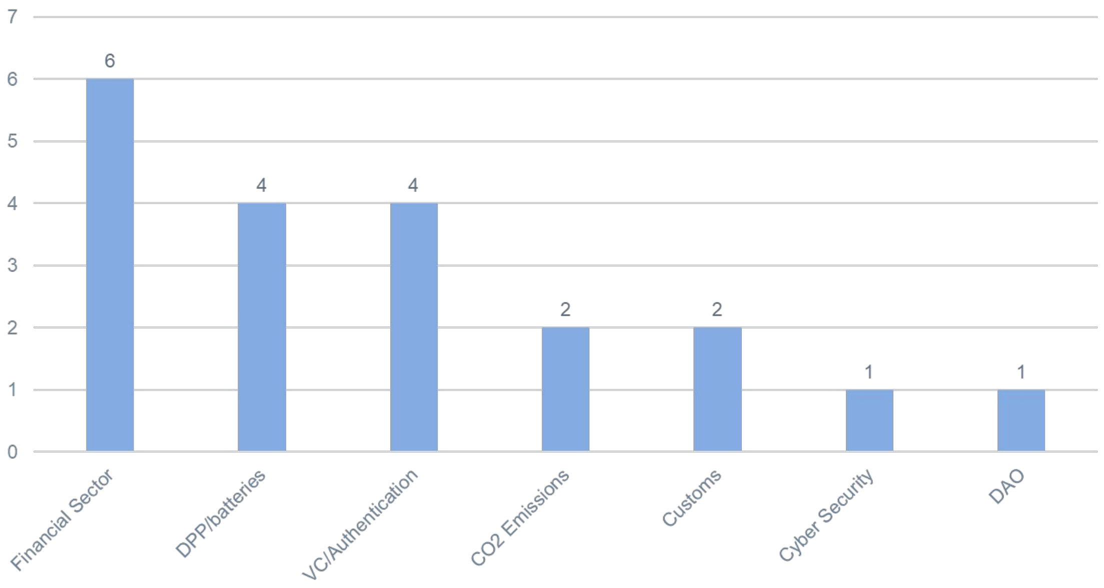
At the beginning of 2024, the same process for the second cohort was accomplished. Projects of this cohort were announced in June 2024 and can be found online here.

In the meantime, the third cohort has also been confirmed. The list of selected projects available on the programme website here, following a similar application and review process.

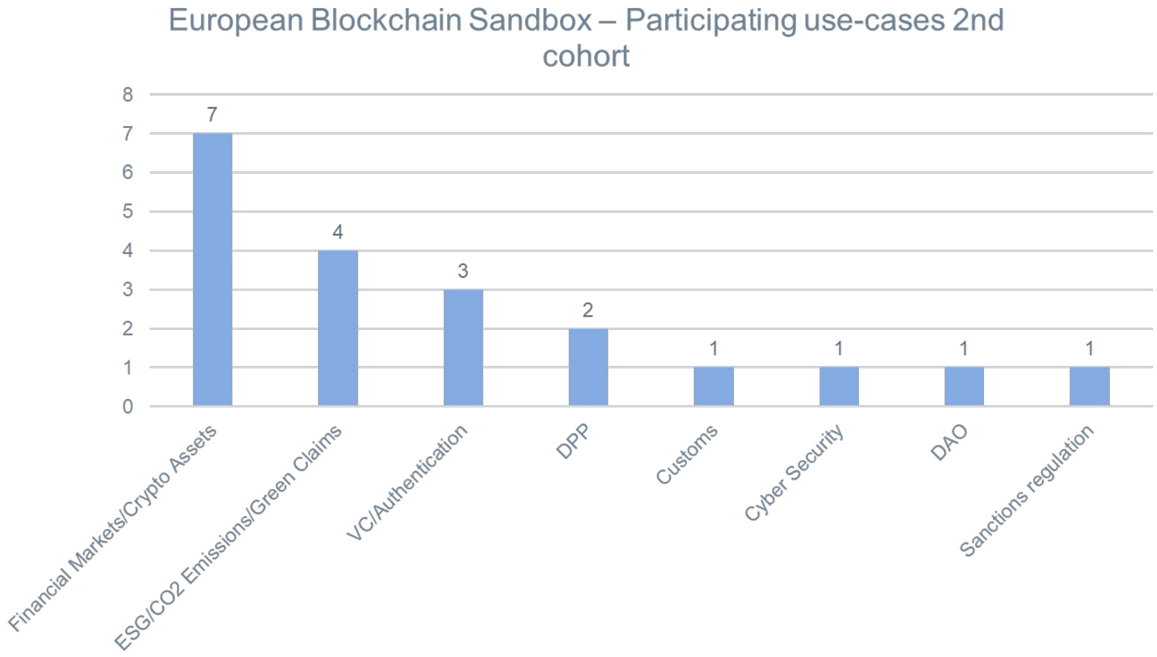
The selection is based on the selection criteria published on the project website. Firstly, the basic eligibility criteria must be met. These are mandatory conditions that determine the applicants' eligibility to participate in the blockchain sandbox. Eligible applications are scored against three different award criteria: i) maturity of the business case, ii) legal/regulatory relevance and iii) contribution to the wider EU policy priorities. In addition, there is a categorisation into four different lots: "micro", "small", "other" and "public institutions".

There are different tiebreaker rules: One is the presence of regulator/authority support if the use cases in the final shortlist of candidates have similar scores that qualify them for selection. In addition, an eligible use case is favoured over other candidates if an EEA region would otherwise not be represented in the final shortlist of candidates. Finally, technical novelty of the use case is applied as a tiebreaker if candidates have similar scores in the final shortlist that are not resolved by the other tiebreakers.

Following the selection, the regulatory focus areas for the dialogues for each of the use-cases are determined. The relevant national and EU regulators and authorities are contacted to provide them with information about the sandbox and the rules and to invite them to participate. More than 50 authorities and regulators from different regulatory areas participated in the dialogues for the first group of 20 use cases, which between them represented all EU/EEA regions and a range of industry sectors (including one EBSI use case proposed by the European Blockchain Partnership). The financial/crypto asset applications were well represented but not dominating, and a broad variety of other use cases was represented in the first cohort, covering areas such as verifiable credentials/authentication, CO2 emissions, digital product passports, cultural asset passports, customs, cyber security, data sharing and DAOs.


European Blockchain Sandbox – Participating use-cases 1st cohort

In the second cohort, the selection of 20 use cases once again ensured a wide geographical and sectoral representation across the EU/EEA. As in the first cohort, the financial and crypto-asset applications played a notable but not prevailing role. Beyond that, the second cohort introduced an extended set of thematic fields, including — among others — AI, verifiable credentials/authentication, ESG reporting, digital product passports, e-voting, customs, cyber security, data sharing, and DAOs. Many of the projects also integrated DLT/blockchain with other advanced technologies such as AI and IoT.



VI. Advantages of the European Blockchain Sandbox

The European Blockchain Sandbox offers many advantages both for the operators of the DLT/blockchain use cases and for the regulators/authorities involved:

1. Advantages for participants

Participating DLT/blockchain providers in the project receive specialised legal and regulatory advice to enhance effective and efficient compliance and the use of applicable EU regulatory instruments.

Furthermore, the European Blockchain Sandbox offers use case owners the opportunity to engage in a constructive dialogue with various national and EU regulators and supervisory authorities, where they can communicate and clarify the need for guidance and legal certainty in a secure and confidential environment.

In addition, use case owners have the opportunity to expand their network by participating in this pan-European project, while no fees are charged for applying and participating in the European Blockchain Sandbox.

2. Advantages for regulatory authorities

The European Blockchain Sandbox also offers many opportunities and benefits to European regulators and authorities.

They are given the opportunity to discuss regulatory issues that have arisen at national level in a cross-border environment in connection with concrete innovative DLT/blockchain use cases and the chance to share experiences and ideas with innovators and other regulators and authorities. They will be able to enhance their knowledge of cutting-edge technologies and have the chance to be recognised as the "most innovative regulator".

In addition, by participating in the project, they will have the opportunity to include relevant regulatory topics for discussion and to contribute to the development of best practices and lessons learned, which are published in the aforementioned best practices reports.

VII. Prospects

DLT and blockchain are relatively new technologies and have become indispensable in today's world. DLT and blockchain technologies are becoming more and more relevant for virtually all national and EU regulators and supervisory authorities.

Feedback from both the first and second cohort of selected use cases and participating regulators/authorities was consistently very positive. The use cases appreciated the legal/regulatory guidance and the possibility to have open dialogues with regulators/authorities.

The regulators/authorities appreciate to learn more about DLT use cases and to have a cross-border dialogue with other national and EU regulators/authorities.

Based on the experience from the first round of dialogues, several improvements were made to the dialogue format – and were well received. These adjustments included, in particular, a change of the set-up of the blockchain expert meeting in the preparation of the dialogues (no longer on a per use case basis) and the introduction of a regulator-only meeting between the first and second dialogue meeting for the financial sector dialogues, with many participating national competent authorities for each dialogue.

In its second year of operation, the project has further matured. More regulatory areas and competent authorities were involved in the dialogues with even more engagement by participating national and EU regulators than in the first cohort.

Building on this experience, the third cohort is expected to allow even more focused and advanced regulatory dialogues. Important elements for the third cohort will be, on the one hand an increased focus on a combination of innovative technologies such as DLT/blockchain in combination with AI, IoT, cloud computing, and on the other hand deeper dives on the basis of ongoing experiences in the EU member states and new regulatory developments on EU level such as the blockchain guidelines by the European Data Protection Board (“**EDPB**”) which were published for consultation on 14 April 2025, the implementing regulations for electronic ledgers on the basis of eIDAS 2 and expected further developments in the areas of auditing/certification of smart contracts, the development of standards including for the development and deployment of smart contracts and the implementation of the AI Act. In addition, the third round of dialogues will provide the opportunity to discuss DLT/blockchain solutions in additional industry sectors such as energy and health care.

In conclusion, the establishment of the European Blockchain Sandbox is an important step towards promoting innovation in this area within the EU/EEA and thus making Europe an attractive location for innovative companies. The European Blockchain Sandbox creates the opportunity to support innovation within a legally secure framework. Here, the EU can seize the opportunity to be a positive example in the "patchwork" of different regulations for DLT and blockchain technologies worldwide. The cooperation and dialogues in the context of the European Blockchain Sandbox will lead to a better mutual understanding and a more effective and efficient application of relevant laws and regulations. Regulation is important for the market and also serves to protect consumers in particular and does not have to hinder future innovations and the EU's economic area. The European Blockchain Sandbox makes an important contribution here.

***Dr. Michael Jünemann** is a partner at Bird & Bird and leading the financial regulatory expert team for the European Blockchain Sandbox. He is head of the international Finance and Financial Regulation Group of the firm and understands the intricacies of the legal frameworks around FinTech and is one of the few to integrate knowledge of technology with capital markets law.*

***Marjolein Geus** is the project leader for the European Blockchain Sandbox and a Bird & Bird partner specialising in European and international regulatory and multi-jurisdictional projects in the communication and technology sectors and leading the Global Tech & Comms Group as well as being the head of the international Sector Regulation and Consulting practice of Bird & Bird.*

[1] Regulatory authorities could range from competent authorities entrusted with supervision and enforcement of regulation or regulators with a role in the development and implementation of regulations.

[2] In principle, the provision of banking business within the meaning of Section 1 Paragraph 1 of the German Banking Act (*Kreditwesensgesetz – KWG*) or the provision of financial services within the meaning of Section 1 Paragraph 1a KWG is subject to a licence requirement in accordance with Section 32 KWG and the provision of financial services within the meaning of Section 2 Paragraph 2 of the German Investment Firm Act (*Gesetz zur Beaufsichtigung von Wertpapierinstituten – WpIG*) is subject to a licence requirement in accordance with Section 15 WpIG. This means that in these cases, a licence must be applied for from the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin*) before business is commenced.

[3] *Roth*, ZBB 2022, 364, 365.

[4] EBA/DP, 2017/02, p. 7.

The regulation of DeFi: what are we seeing offshore?

By Sara Hall

Introduction

Each of Cayman, the British Virgin Islands and Bermuda has development legislative frameworks which provide the virtual assets industry with regulatory certainty. These frameworks are based in part on the FATF standards and guidance for virtual assets, and in part on existing securities legislation. Each has a well-established process for obtaining a regulatory licence (or registration) and each issues guidance to assist with understanding the application process. None has sought to issue express guidance on DeFi and none has an express supervisory regime for DeFi. Change may, however, be on the horizon as Bermuda has recently consulted on establishing a supervisory framework for DeFi platforms. This article considers the recent consultation paper available which is here.

Bermuda's consultation paper

The Bermuda financial services regulator, the Bermuda Monetary Authority (BMA) launched a consultation in February 2025 calling for proposals for a collaborative pilot project focused on testing "embedded supervision" practices for DeFi platforms. "Embedded supervision" refers to the automated monitoring of compliance with a regulatory framework, through tools (such as automated reporting) embedded in the smart contracts.

To assist it with developing this regime, the BMA invited responses from digital asset businesses, DeFi operators, FinTech companies, technology developers, and academic institutions.

Objectives of the Pilot

The pilot project is designed around three core objectives:

1. **Collaborative Understanding & Risk-Based Regulation**
   The BMA would like to better understand the complexities of DeFi and inform the development of adaptive, risk-based regulatory frameworks. The project will examine how Embedded Supervision can be applied to DeFi projects with varying degrees of decentralization and governance models.

2. **Technical Feasibility & Operational Efficacy**
   Participants will assess which components of DeFi require Embedded Supervision and how relevant data should be communicated to regulators. The pilot will evaluate the effectiveness of automated compliance checks and reporting, while identifying technological, operational, and security challenges, by assessing outcomes achieved.

3. **Risk Monitoring & Best Practices**
   The initiative aims to monitor changes in DeFi risk parameters, evaluate the stability and disclosure practices of platforms, and quantify efficiency gains from real-time compliance monitoring. The findings will contribute to the establishment of best practices for implementing and maintaining Embedded Supervision in DeFi.

Key Challenges Addressed

The BMA recognises several challenges inherent to DeFi that the pilot seeks to understand and explore.

- **The lack of a central authority** which complicates traditional oversight and accountability measures.
- **AML/KYC Compliance:** DeFi’s pseudonymous nature requires innovative approaches to anti-money laundering and know-your-customer processes if illicit activity is to be identified and prevented.
- **Technological Complexity:** Rapid technological evolution demands regulatory agility and enhanced technical expertise.
- **Cross-Border Operations:** DeFi’s global reach complicates jurisdictional authority and regulatory applicability as no one set of laws or regulations is applicable.
- **Pace of Innovation:** The fast-moving DeFi landscape necessitates proactive and adaptive regulatory responses.
- **Degrees of Decentralisation:** Understanding the true level of decentralisation in DeFi projects is critical for effective oversight. Some projects may not in fact be decentralised as a small group of stakeholders such as developers or miners exert significant influence.

Potential Pilot Project Examples

The BMA encourages creative and innovative proposals, suggesting several illustrative pilot concepts:

- Implementation of a Regulatory Decentralised Autonomous Organisation (DAO) with BMA participation (for example, as a non-voting member).
- Embedded Supervision in DeFi lending platforms, focusing on risk parameters and disclosure.
- Integration of regulatory requirements into DeFi smart contracts.
- Development of real-time compliance reporting systems (for example to detect and report in real time regulatory breaches).
- Automated collateral management for stablecoins with automated alerts if collateral fell below regulatory thresholds.
- Establishment of regulatory nodes on public blockchain networks for direct and real time oversight.

Proposal Submission Guidelines

The BMA set out key deliverables for submissions, to include:

- Executive summary and project objectives
- Detailed methodology and work plan
- Technological overview and regulatory considerations
- High-level risk analysis and management strategies
- Team composition and relevant expertise

Evaluation of the Proposals

The BMA has committed to evaluate proposals based on innovation, feasibility, alignment with pilot objectives, and potential impact on regulatory practices.

Implications for the Digital Finance Sector

This initiative represents a significant step towards understanding whether it is possible to have meaningful regulatory oversight in the DeFi space and if so, how this can be achieved. By piloting Embedded Supervision, the BMA is looking at developing effective, real-time supervisory mechanisms that can keep pace with the rapid evolution of digital finance while recognising that, unlike centralised finance, there may be no controlling person or entity to supervise. The BMA anticipates the inputs from this pilot will assist in the development of future regulatory frameworks for DeFi, which will enhance compliance, and foster innovation in the sector, while preventing financial crime and illicit activity. If successful, we can expect both onshore and other offshore jurisdictions will need to consider whether to adopt a similarly innovative approach and invest resources in this field.

Sara Hall *has over 30 years' experience in global senior in-house roles and private practice. She now practises Cayman Islands, British Virgin Islands and Bermuda law in our Global Regulatory & Risk Advisory Practice Group. She specialises in financial services and international regulation, as well as digital assets, decentralised autonomous organisations, cryptocurrencies and non-fungible tokens.* ***https://www.walkersglobal.com/en/People/h/Hall-Sara***

Framework for the legal classification of DeFi and related activities under Swiss financial market law

By Christian Meisser, Florian Prantl, Fabio Andreotti, and Rolf H. Weber.

Initiative of the Digital Assets Working Group (DeFi sub-group) of the Swiss Blockchain Federation

Version: FINAL 1.0, 4 March 2025

This document has been translated for convenience. Reference is made to the original version published in German.

1. Introduction

1.1. Concept and objectives

Decentralized Finance ('DeFi') involves the provision of financial services and infrastructures through software - primarily public blockchains and smart contracts – without a central operator or intermediary. DeFi aims to establish an open, efficient and secure addition and alternative to the traditional finance industry. It has seen significant growth in recent years, expanding across all financial sectors, including payments, trading, lending and asset management. However, to date DeFi varies in form and lacks a uniform understanding of what 'decentralization' means.

This circular is structured as follows:

1. In a first section, we provide an overview of the current legal discourse on DeFi with reference to more detailed literature (section 1.2).
2. In the following sections, we explore the criteria necessary to legally distinguish '*genuine DeFi*' from de facto centralised, blockchain-based financial market infrastructures and services (hereinafter referred to as '*on-chain CeFi*'*):*
   a. *Step 1*: As a prerequisite, we summarize an existing framework by Schuler/Cloots/Schär for the assessment of technical decentralization (section 2).
   b. *Step 2*: We distinguish between legal and technical decentralization (section 3.1) and reexamine the regulatory concept of financial groups (*aufsichtsrechtlicher Gruppenbegriff*) (section 3.2).
   c. *Step 3*: We develop an actionable legal framework to classify DeFi within the personal scope (*persönlicher Anwendungsbereich)* of Swiss financial market law (section 4).
   d. *Step 4*:We differentiate between the 'operation' a DeFi application or protocol and conducting DeFi-related activities (section 5)
3. Finally, we provide a summary of our findings (section 6).

It is important to note that numerous legal issues surrounding DeFi are not addressed in this circular. For instance, the regulatory requirements for both regulated and unregulated market participants wishing to provide clients with access to DeFi applications remain largely vague and unclear. Also, given the increasing adoption of DeFi, establishing a more comprehensive regulatory framework that balances its unique risks and potential benefits will become crucial for any jurisdiction intending to foster innovation in this sector.

1.2. Overview of the legal discourse on DeFi

In Switzerland, the Swiss legislator and Federal Council, the Swiss regulator FINMA, as well as legal scholars have previously recognised and specifically addressed decentralization in the financial industry. Likewise, DeFi has been the topic of various discussions and reports in other jurisdictions as well as by international organizations and standard-setting bodies in recent years.

1.2.1. Swiss legislator and Swiss Federal Council

In its efforts towards the Swiss DLT legislation, the Swiss Federal Council initially noted in the 2018 Swiss DLT Report that the applicability of anti-money laundering legislation to decentralized platforms depends whether *"platforms have the option of influencing clients' transactions"*. This practice was intended to be incorporated as such in the Swiss DLT legislation (at ordinance level). While subsequently the revision of the Swiss Anti-Money Laundering Ordinance introduced the criterion of an '*ongoing business relationship*', the corresponding explanatory report to AML ordinance re-confirmed, with specific respect to decentralized trading platforms, that smart contracts which process transaction without "*access possibility for the trading platform*" are not subject to the AMLA.

The Swiss DLT legislation also explicitly clarified that "*fully decentralised «financial market infrastructures», i.e., financial market infrastructures without a direct operator*" remain excluded from the scope of application of financial market infrastructure legislation. This regulatory position is being maintained in the ongoing revision of the FMIA.

1.2.2. International organizations and the European Union

At the international level, several supranational organizations, policy makers and certain regulators and legislators have taken initial positions on DeFi, including the Financial Action Task Force (FATF), the European legislator in Recital 22 on MiCAR ("*Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation*"), the International Organisation of Securities Commissions (IOSCO) , the Financial Stability Board (FSB), the Bank for International Settlements (BIS), or the Organisation for Economic Co-operation and Development (OECD).

1.2.3. FINMA

The Swiss regulator FINMA has repeatedly addressed DeFi in its annual reports for 2021, 2022, and 2023, as well as in industry roundtables and similar events. FINMA emphasises a case-by-case analysis against the backdrop of the principles of technology neutrality and an economic (*substance over form*) and risk-based approach (*same risks, same rules*). According to the 2021 annual report, the aim is to distinguish projects "*without identifiable operators*" from those that "*describe themselves as DeFi but are actually organised and controlled centrally and therefore similar to traditional financial market intermediaries. Such projects fall within the scope of financial market law.*" Possible regulatory anchors mentioned by FINMA's 2023 annual report include, without further explanation, (i) the management of application development via admin keys or via the majority of governance tokens (see section 4.2.2), (ii) the dependency of the application on data entered by a specific person via e.g., a blockchain oracle (see section 5 point 4), (iii) the business relationships with end users (insofar as this refers to the licensing of the DeFi application, see section 5 point 5), and (iv) the income flows from the application to a specific person (see section 5 point 6).

1.2.4 Legal doctrine

Finally, Swiss legal scholars have increasingly published on the topic of DeFi in recent years and have highlighted the importance of distinguishing between centralized and decentralized financial services and infrastructures. For additional details, please refer to the literature cited in the footnote.

1.2.5 Summary

While the discussion on DeFi covers a broad range of topics, two main findings emerge:

1. The term 'DeFi' is repeatedly misused for de facto centralised structures or on-chain CeFi.
2. 'Truly decentralised' DeFi is not covered by existing financial market laws and to capture its unique risks and challenges, it requires a regulatory approach distinct from existing financial market infrastructures and services regulations.

2. Technical framework

In '*On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralised Finance*', Schuler/Cloots/Schär propose to make the distinction between 'DeFi' and 'on-chain CeFi' based on centralization vectors (**Figure 1**).

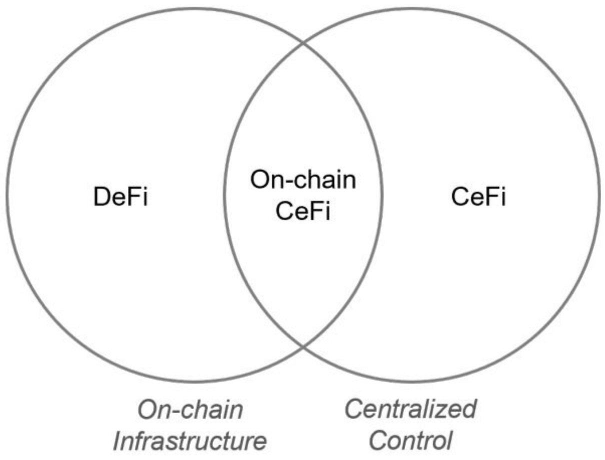


Figure 1: On-chain CeFi denotes blockchain-based financial protocols with material centralization vectors.

This distinction stems from the initial observation that DeFi protocols are constructed across multiple technological layers. Adopting the layer-model as proposed by Schär, the authors suggest evaluating the level of decentralization of DeFi protocols using centralizations vectors within the specified levels or layers detailed below (**Figure 2**):

1. Blockchain level (*settlement layer*): The settlement layer serves as the foundational base for all DeFi protocols built upon it.
2. Smart contract level (*asset and protocol layer*): DeFi protocols utilize smart contracts to represent tokens (*assets*) and to embody the protocol's working logic (*protocol*).
3. User interface level (*application and aggregation layer*): Web-based user interfaces or frontends enable simplified user interaction with the blockchain and the smart contract layer of one or more DeFi protocols (in the latter case referred to as '*aggregators*'). In principle, user interfaces are an off-chain element, i.e. merely (i) a graphical user interface, (ii) which visualises information from the blockchain, and (iii) suggests transaction commands based on the user's input. User interfaces are thus typically optional for the user, non-exclusive and have no influence on the lower (blockchain and smart contract) levels. However, centralization vectors on the user interface can nonetheless occur in exceptional circumstances, particularly when the operator gains access to user assets in specific instances (*custodial setup*).

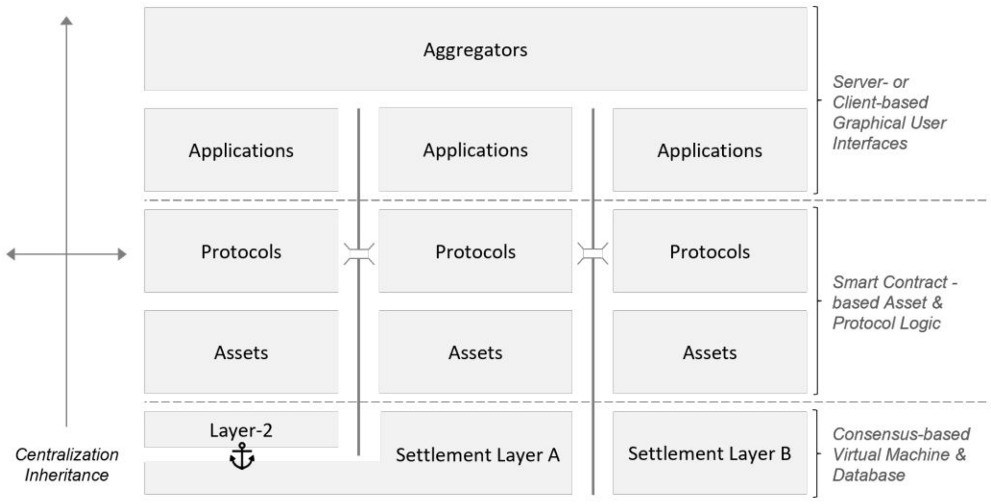

Aggregators
Applications
Applications
Applications
Server- or Client-based Graphical User Interfaces
Protocols
Protocols
Protocols
Assets
Assets
Assets
Smart Contract - based Asset & Protocol Logic
Layer-2
Settlement Layer A
Settlement Layer B
Consensus-based Virtual Machine & Database
Centralization Inheritance

Figure 2: Multichain DeFi Stack (adapted from Schär[58])

.

From this, the authors propose a framework to assess decentralization of blockchain-based financial infrastructure from a technical perspective and to distinguish genuine DeFi protocols from on-chain CeFi. The assessment logic can be summarized as follows:

1. Blockchain level: Is the underlying blockchain sufficiently decentralized? If not, it is classified as on-chain CeFi according to the authors' framework.
2. Smart contract level: Do the smart contracts contain functions that (i) are limited in accessibility, (ii) are 'critical' in nature, and (iii) do not have sufficiently decentralized access? If these three conditions are met, the DeFi protocols qualifies as on-chain CeFi. An example would be (i) a function accessible solely with a majority of governance tokens, (ii) which allows control over users' tokens and is thus critical, where (iii) an individual holds the majority of these tokens and exercises effective control.
3. External or 'exogenous' factors: The framework then assesses factors external to the DeFi protocol itself, particularly any 'off-chain promises' (e.g., a commitment by an individual to maintain the value of a decentralized stablecoin through secondary market intervention) and dependencies on 'third-party assets or protocols' (e.g., reliance on price data supplied by a blockchain oracle). Significant 'off-chain promises' or dependencies on centralized 'third-party assets or protocols' can also qualify the overall arrangement as on-chain CeFi.

3. Decentralisation and the regulatory concept of groups

3.1. Legally relevant 'operation' vs. technical risks

Before applying the framework of Schuler/Cloots/Schär for the purpose of establishing a legal framework for the classification of DeFi and related activities, we need to highlight that the discussion on decentralisation from a *technical* perspective addresses different issues than the discussion from a *legal* perspective:

1. Legal decentralisation focuses on the question of whether, from the perspective of the personal scope of application of financial market law, there is an operator who controls the DeFi protocol and to whom the activities of the DeFi protocol can be attributed. This constitutes a 'positive' examination: Is there an individual or a group of connected persons who effectively 'operate' the DeFi protocol, meaning they can control or influence it in a significant way?
2. The technical decentralization focuses more broadly on the question of whether there are any centralization vectors present that pose technical or operational risks to users. This involves a 'negative' examination: Is there *no* individual upon whom the DeFi protocol is directly or indirectly dependent, or by whom it could be compromised?

To illustrate this with an example: If a DeFi protocol is built on a public blockchain that, due to very high hardware requirements for node operators, has only a limited number of nodes, such centralization on the blockchain level can be considered a technical decentralization risk. However, the initiators of the DeFi protocol, who launch a project on this public blockchain, typically do not gain any sort of control over the DeFi protocol due to such centralization vector. Accordingly, from a legal perspective, such centralization on the blockchain level alone does not render the initiators the legally relevant 'operators' of the DeFi protocol.

From the above, we can conclude that legal decentralization can exist even if the ideal state of full technical decentralization is not (yet) achieved. However, this should not detract from the fact that, according to the views expressed in this circular, legal decentralization will regularly require a high level of technical decentralization.

3.2. Regulatory concept of groups (*aufsichtsrechtlicher Gruppenbegriff)*

Financial market law has always grappled with the challenge of market participants deliberately organizing their activities in a way that individually, they do not meet the relevant criteria or thresholds for regulation, but if viewed collectively as a group, they would. To combat circumvention of the laws through such strategic and artificial structuring, Swiss case law has developed the regulatory concept of a groups (*aufsichtsrechtlicher Gruppenbegriff*).

There are legitimate concerns expressed in scholarly discussions about the above concept, particularly regarding constitutionality (the concept lacks an explicit legal basis) and legal certainty (it is often unclear how the criteria to qualify as a group should be applied in specific cases). Nonetheless, it seems fitting to use it also when analyzing DeFi protocols to the end that it should not matter whether a regulatory-relevant activity associated with a DeFi protocol is conducted individually or as a group in the sense of financial market law. For instance, if a DeFi protocol allows control of locked assets via majority of governance tokens, it would be necessary to examine whether either an individual *or* a group (as per applicable case law) actually exercises such control via the majority of these governance tokens. If so, this would establish a direct link to potential financial market activities for such a group (or the individual members of the group respectively). However, it should be emphasized that DeFi protocols (and blockchain-based systems in general) tend to very deliberately set economic incentives for various participants to symbiotically contribute and thus maintain the functioning of the protocol. Such 'group behavior' will, however, often not meet the case law's criteria for a financial group, given that participants in these setups pursue individual rather than collective interests without any close and legally relevant connection among them.

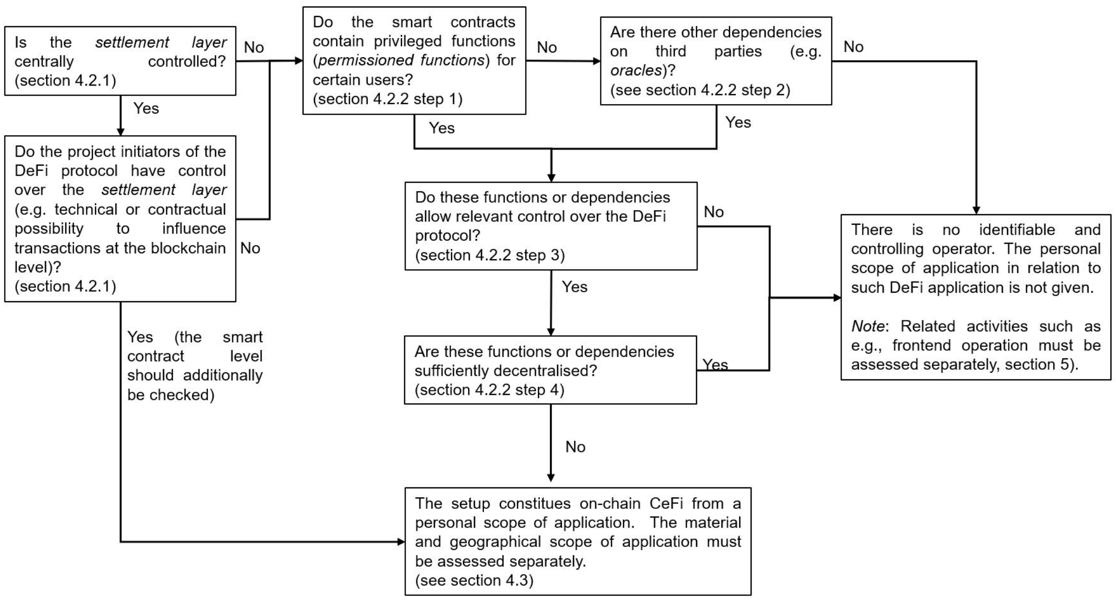
Pro memoria on legal definition of groups: According to Swiss case law, a mere loose connection between individuals is insufficient to constitute a group. Rather, it is necessary that (i) there exists a close economic, organizational, or personal connection among the individuals, and (ii) a holistic economic assessment of the setup is warranted, particularly due to economically unjustified, complex legal structuring that is created with the intention to circumvent regulatory provisions.

4. Framework for the classification of DeFi under Swiss financial market law

4.1. Introduction and overview

The framework for the applicability of Swiss financial market law to DeFi protocols is conducted across the three dimensions commonly used in legal assessment, which are (i) the *personal* (ii) the *material*, and (iii) the *geographical* scope. Thereby, the framework by Schuler/Cloots/Schär outlined above (section 2) proves particularly helpful when addressing the *personal* scope of applicability, in other words the question whether or not there is an identifiable operator or controlling operator to whom the activities of the DeFi protocol can be attributed.

Checklist for the *personal* scope of applicability of Swiss financial market laws to DeFi protocols


Is the *settlement layer* centrally controlled? (section 4.2.1)
No
Yes
Do the project initiators of the DeFi protocol have control over the *settlement layer* (e.g. technical or contractual possibility to influence transactions at the blockchain level)? (section 4.2.1)
No
Yes (the smart contract level should additionally be checked)
Do the smart contracts contain privileged functions (*permissioned functions*) for certain users? (section 4.2.2 step 1)
No
Yes
Are there other dependencies on third parties (e.g. *oracles*)? (see section 4.2.2 step 2)
No
Yes
Do these functions or dependencies allow relevant control over the DeFi protocol? (section 4.2.2 step 3)
No
Yes
Are these functions or dependencies sufficiently decentralised? (section 4.2.2 step 4)
Yes
No
There is no identifiable and controlling operator. The personal scope of application in relation to such DeFi application is not given.
Note: Related activities such as e.g., frontend operation must be assessed separately, section 5).
The setup constitues on-chain CeFi from a personal scope of application. The material and geographical scope of application must be assessed separately. (see section 4.3)

4.2. Personal scope of application

4.2.1. Centralisation at the blockchain level (*settlement layer*): Is the blockchain sufficiently decentralised?

4.2.1.1. Background

From a technical perspective, the degree of centralization of a blockchain is directly relevant for all DeFi protocols built on it, as they directly 'inherit' its centralization vectors. From a legal standpoint, however, the key question is whether or not launching a DeFi project on a 'centralized' blockchain in fact creates a personal point of attribution (*persönlicher Anknüpfungspunkt*) for the operators of the centralized blockchain and/or the project initiators.

4.2.1.2. Criteria

'Operation' of the blockchain: Firstly, on a technical level, it is necessary to determine which individuals have influence over the blockchain and whether they meet the financial market law's criteria for constituting a financial group. This aspect is particularly relevant for private blockchains. For instance, the 'Swiss Trust Chain,' operated by Swiss Post and Swisscom, featuring only two nodes owned by two companies with the same main shareholder, would likely not be considered sufficiently decentralized. Conversely, the majority of public blockchains, which may not achieve ideal decentralization technically, are typically not operated by a closely connected group.

Launching a DeFi protocol on a centralised blockchain: For project initiators launching a DeFi protocol on a 'legally centralized' blockchain, it is crucial to examine the legal relationship between the initiators and the operators of such blockchain. Launching a DeFi protocol on a blockchain that is not ideally decentralized does not itself establish a personal point of attribution if the project initiators have no ability to influence the blockchain. However, if legal or actual influence over the underlying blockchain exists (which in turn allows relevant control on the smart contract or user interface level of the DeFi application), it must be determined whether this influence can be attributed to an individual or a closely connected group in the sense of financial market law (see section 4.2.2, steps 3 and 4).

4.2.1.3. Legal consequences

For the 'operators' of the blockchain: If activities subject to financial market regulation are conducted using a centralized blockchain (e.g., issuing a native token that qualifies as a payment token), the operators of this blockchain assume legal responsibility for these activities. In terms of DeFi protocols deployed on top of this blockchain, the general question arises whether such operators should be held legally accountable for any third party activity (such as the deployment of a DeFi protocol) conducted on their blockchain. While we do not discuss in detail in this circular, we generally recommend falling back to the legal doctrine relating hosting provider liability. In essence, operating a centralized blockchain utilized by third parties mirrors in many ways the operation of other centralized and more traditional hosting infrastructures.

For project initiators: Project initiators who launch a DeFi protocol on a centralized blockchain may be attributed the activities of the DeFi protocol if they obtain relevant control over by way of collaborating with the blockchain operators, e.g., through contractual claims or other structuring.

4.2.2. Centralisation at smart contract level (*asset and protocol layer*): Do the smart contracts enable relevant control over functionalities or introduce relevant third party dependencies?

4.2.2.1. Background

Following the assessment of the blockchain level, it is necessary to assess at the subsequent smart contract level whether an individual or a closely connected group has control over the DeFi protocol. This control can be exercised directly through privileged functions within the smart contract (e.g., upgrade functions) or through external dependencies (e.g., control of oracles).

4.2.2.2. Criteria

The assessment is divided in four steps:

Step 1: Do the involved smart contracts grant certain users special, privileged rights (*permissioned functions*)?

In an initial step, all smart contracts of the DeFi protocol are technically analysed to determine whether they grant special access or control rights and whether such functions are accessible (or inaccessible) to all to just to certain users.

It should be noted that such *permissioned functions* can vary widely in their scope – from upgrades of the entire protocol logic (often implemented technically through so-called *proxy smart contracts*) to (direct or indirect) access to user assets, to the ability to influence individual transactions through the blacklisting of specific addresses, up to merely limited adjustments of predefined technical variables such as a 'fee switch'.

Step 2: Concurrently with step 1, we assess whether a DeFi protocol has *external dependencies*. Such dependencies may include 'off-chain' promises or the use of oracles for pricing assets. An off-chain promise may e.g., be seen in a stablecoin setup including a legal commitment by an individual or group to maintain stability by providing their own assets in the event of depegging. Another form of external dependency may e.g., be seen in an oracle providing critical price data to a DeFi protocol, whereby the delivery of false data could significantly impair or even break the protocol's intended functionality.

Step 3: Not *every permissioned* function or *external dependency* results in the same level of control over a DeFi protocol. There hence needs to be a case-by-case assessment of *how much* control is being exercised through these elements, or in other words, which potentially regulated activities could even be conducted using the level of control granted by these elements.

For instance, merely having the control (through a *permissioned function*) to impose a transaction fee for future transactions within a defined set of parameters (*fee switch*) does not constitute control over every activity conducted by the DeFi protocol, as it does not allow the person(s) with access to the *fee switch* to control user transactions or user assets. However, if an upgrade functionality pertains to broader elements of the protocol logic, it could certainly lead to significant control. Even in the case of such broader upgrade functionalities, one should consider industry standards such as built-in time delay for the go-live of upgrades (*timelocks*) that allow users to exit or opt-out of the DeFi protocol (*exit windows*) and that can drastically reduce the level of control on user transactions and user assets effectively exercised through an upgrade function.

Regarding external dependencies, we note that third parties are typically involved for very specific activities limited in scope. For example, a centralized external oracle providing price information might affect the DeFi protocol's functionality if incorrect data is delivered. Generally, however, the influence of such an oracle should not be extensive enough to allow it to gain targeted control over transactions, assets, or other relevant activities of the DeFi protocol.

Step 4: If there are *permissioned functions* or *external dependencies* that grant a relevant level of control over user transactions and user assets: Is the exercise of these functions or dependencies sufficiently decentralised?

From a *technical* point of view, the control of permissioned functions can be implemented across a spectrum ranging from (i) sole control by an individual via a private (admin) key, to (ii) a multi-signature setup involving several (independent) signing (admin) keys, up to (iii) on-chain governance, where control is typically exercised by a majority of votes from governance token holders.

For the *legal* assessment of whether control is sufficiently decentralized or not, we can once again rely on the regulatory concept of financial groups (*aufsichtsrechtlicher Gruppenbegriff*): For instance, if a *permissioned function* is controlled by a multi-signature address where the holders of the signing keys are so closely connected that they form a financial group, a personal point of attribution is established for the members of such group. The same applies to governance tokens: If a closely connected group of individuals exerts control over the permissioned function through a majority of governance tokens necessary for such actions, the control exercised through such function can be attributed to those individuals.

It should be noted that in practice, determining the facts about e.g., who holds signing keys or governance tokens, can be challenging. This was particularly highlighted by FINMA before However, considering the principles of proportionality, legal equality and technological neutrality, difficulty or complexity in establishing factual circumstances (*Sachverhaltsfeststellung*) do not provide a *carte blanche* to legally treat all sort of similar control mechanisms in the same manner.

4.2.2.3. Legal consequences

If there are no permissioned functions or external dependencies that grant significant control (steps 1, 2 and 3), or if such control is sufficiently decentralized (step 4), there is no 'controlling' operator, and the activity of the DeFi protocol cannot be legally attributed to any person. This constitutes 'genuine' DeFi. Where this is not the case, i.e., the setup constitutes on-chain CeFi, it is necessary to further assess the material and geographical scope (section 4.3) to determine the applicability of financial market law.

4.3. Material and geographical scope of application

If the DeFi protocol does not have a controlling operator and there is therefore no personal link to an operator, the activity of the DeFi protocol falls outside the scope of the applicable financial market law.

In the case of on-chain CeFi, however, we need to further assess both the material and geographical scope of existing Swiss financial market laws.

Regarding the material scope of application, the principles of "*same risks, same rules*" (or "*different risks, different rules*"), which have already been established and are applied in FINMA practice, can be utilized to assess the activities from a holistic and economic standpoint. In that context, a common issue in practice is whether some level of centralization should still be allowed or tolerated in the initial starting or incubation phase of a project. There have been various initiatives in the industry that advocate for creating such a "road to decentralization" exemption to create legal certainty for market participants. However, we find that no such explicit exemption exists in current Swiss legislation. Therefore, if relevant control is present, there is little room for initial centralization absent from certain thresholds typically provided in the context of whether a regulated activity is provided in a commercial manner. Lastly, regarding the geographical scope, it one needs to evaluate whether there is a significant link to Switzerland or the Swiss market based on established legal doctrine on the subject.

5. Regulation of DeFi related activities

There are a multitude of activities associated with the development and usage of a DeFi protocol, including writing code (*development*), deployment of code to the respective blockchain (*deployment*), services involved in operating the underlying blockchain (*node operation, validation, staking, mining, block building,* etc.), providing wallet software like MetaMask, providing off-chain internet infrastructure (*programming and hosting a frontend, transferring data packets, internet browsers*, etc.), marketing the DeFi protocol through social media channels, providing data (*oracles*), interacting with the DeFi protocol (*liquidity provision, voting, trading*, etc.), and more.

For the sake of providing legal certainty to market participants, it is important to distinguish such activities from the actual operation of a DeFi protocol itself as much as possible. Even though these related activities do not constitute the operation of the DeFi protocol, they can still represent independently regulated activities of their own. We hence try to address some of the most important of such activities below:

Framework for the legal classification of DeFi and related activities under Swiss financial market law

1. **Participation in the settlement layer**: Participation in the operation of an underlying blockchain (such as *block building, validation, staking or mining*) is generally not regulated in case of a decentralised blockchain. For the operators of a centralised blockchain, however, there may be legal requirements for (i) the activities of the blockchain itself, such as the issuance of native tokens qualifying as payment tokens, or (ii) in terms of liability analogous to the liability of hosting service providers for the DeFi protocols operating on the centralised blockchain.

2. **Development, deployment & updates**: The development and deployment of genuine DeFi protocols are generally not regulated by existing financial market law. However, how subsequent developments (*updates* or *upgrades*) are integrated into an already launched DeFi protocol is pertinent. We cover this in our framework outlined above (section 4.2.2).

3. **Participation in on-chain governance**: Mere participation in an on-chain governance process typically does not constitute an activity relevant under financial market law. However, if an individual or a group controls a permissioned function or external dependency granting relevant control, a personal point of attribution may be established with respect to such control. We cover this in our framework outlined above (section 4.2.2).

4. **Oracles**: The mere sale or provision of price or other information to DeFi protocols should typically not even fall within the material scope of financial market law in the first place; hence, even fully centralized oracles are typically unregulated. However, operating an oracle could constitute an activity relevant to financial market law if the oracle deliberately exercises relevant control over the DeFi protocol.

5. **Licensing conditions and intellectual property rights**: In principle, the specific license under which the software code of a DeFi protocol is published, and whether the license involves a fee, does not matter – once the software operates in a decentralized manner on the settlement layer, the license itself does not grant the licensor any control over the DeFi protocol. Furthermore, licensing software, such as core banking solutions or payment system software, is not in itself an activity covered under financial market law in the traditional finance sector. Also, no '*ongoing business relationship*' relevant under Swiss anti-money laundering regulations can be assumed merely from software licensing: The materials regarding the Swiss DLT Act state that the mere licensing part of the activity of 'non-custodial wallet providers,' who typically operate and develop their software continuously, does not by itself lead to the applicability of anti-money laundering regulations. In this context, we want to also highlight that it is appropriate that authorities have not considered the fee arrangement (whether free, subject to a licensing fee, etc.) of the license as a relevant criterion for non-custodial wallet providers. Lastly, the ownership of intellectual property rights (such as trademarks, domains, or social media accounts) related to the DeFi protocol is generally not suitable as a personal point of attribution (*persönlicher Anknüpfungspunkt*), as these elements do not grant any control over the DeFi protocol as discussed previously.

6. **Generating income or 'commerciality'**: Generating income or revenue is typically addressed in financial market law in the context of certain thresholds that need to be reached before a regulated activity requires a license. Consequently, individuals operating on-chain CeFi do not fall within the material scope of a specific law if they remain below the commerciality or professionality thresholds set out in a specific legislation. Separately from that, the flow of funds in a DeFi protocol may be a helpful factor in determining the facts to assess legally relevant control in the DeFi protocol. However, there is no legal basis that merely 'earning money', for instance if a genuine DeFi protocol allocates a portion of the protocol's fees to developers or holders of governance tokens, would by itself constitute a personal point of attribution for the operation of a DeFi protocol.

7. **User interfaces**: User interfaces (frontends) are often the most visible elements of a DeFi protocol and one may be tempted to simply attribute the operation of the DeFi protocol to the operator of the interface. However, this assumption does not hold under a more detailed assessment: Any frontend is typically purely optional and not necessary for the actual operation of the DeFi protocol, nor is it involved in the direct interaction with the DeFi protocol. Consequently, the operator of a frontend has no control or influence over the DeFi protocol and thus cannot legally be considered its 'operator'. Nevertheless, the operation of a frontend may still be relevant under other specific legislation, such as in relation to advertising financial instruments or public offerings of financial services under the Swiss Financial Services Act, or in terms of unfair competition under the Swiss Unfair Competition Act.

6. Conclusion

This circular shows that Swiss legislators, administration and academia as well as many international players have already engaged with the topic of DeFi, and that there is consensus on key issues: On the one hand, on-chain CeFi offerings fall within the personal scope of financial market laws, and operators may be subject to regulatory obligations under the *'same risks, same rules'* principles. On the other hand, genuine DeFi currently falls outside the personal scope of financial market laws in Switzerland.

Given the existing legal uncertainty that hinders market participants from advancing innovation in the DeFi sector in Switzerland, this circular suggests a practical framework for the case-by-case assessment of DeFi protocols under Swiss financial market laws. Building on technical groundwork by Schuler/Cloots/Schär, the framework sets high requirements for decentralization at every step, and aims to provide both project initiators with clear guidance to direct development as well as simplify the legal analysis of existing DeFi protocols.

Finally, the framework includes examples of related activities within DeFi protocols that do not constitute their operation, providing clear criteria to differentiate these activities.

Christian Meisser *is a partner at www.LEXR.com and advises many of the leading Web3 projects on their legal structuring.*
Florian Prantl *is General Counsel at Chronicle Labs, a oracle data provider, and former Managing Associate at www.LEXR.com with a focus on Web3 clients.*

Dr. Fabio Andreotti *is Deputy General Counsel at Bitcoin Suisse AG and a member of the Board of Directors of RealUnit Schweiz AG, listed on BX Swiss. He earned his doctorate at the University of Zurich, focusing on decentralized trading platforms in Swiss financial market law.*
Prof. Rolf H. Weber *is a Law Professor at the University of Zurich's Faculty of Law and an Attorney-at-Law at the law firm Bratschi in Zurich, Switzerland with extensive expertise in regulatory, fintech, and distributed ledger technology (DLT) law.*

Vietnam Blockchain Ecosystem: Regulatory Roadmap & Investment Implications

By Nguyen Tran Minh Quan

Vietnam's blockchain sector is accelerating into the mainstream. A new *Digital Technology Industry Law (2025)* – taking effect Jan 1, 2026 – establishes Vietnam's first comprehensive legal framework for digital and crypto assets. This memo reviews the law's crypto provisions and related policies, focusing on investment risk and opportunity. Key takeaways for funds and VCs: *cryptoassets are now formal property rights*, bolstering collateral and user protection; *crypto businesses will face explicit AML/CFT obligations* (improving institutional-grade compliance); *alignment with FATF standards* is a priority (reducing country risk); *Da Nang and Ho Chi Minh City* are being built as fintech hubs with generous incentives; local *RegTech innovations* and training partnerships are rising fast; the first crypto sandbox project (Basal Pay) signals concrete fintech dealflow; and further regulations (centralized exchanges law, blockchain governance decree) are in the works. Throughout, we note timing, clarity, and downside factors for allocators evaluating Vietnamese crypto investments.

Market Context: Crypto Adoption & Flows

Vietnam is already *one of the world's largest crypto markets*. Roughly 20–21% of Vietnamese adults hold crypto, ranking among the highest global adoption rates. Annual crypto flows in Vietnam have been estimated at > $100 billion per year (2022–24) – many times larger than Vietnam's foreign direct investment. (By comparison, 2024 FDI inflows were roughly $16–20 billion.) *Chart:* Vietnamese crypto inflows dwarf traditional FDI.

Vietnam's regulators have taken note of this scale. The *Digital Technology Industry Law (DTIL)* explicitly acknowledges "digital assets" (tài sản số), including two new legal categories: virtual assets (tài sản ảo) and crypto assets (tài sản mã hóa). Importantly, the law now *recognizes digital assets as property*: their creation, ownership and transfer are governed under civil law principles. In practical terms, this means blockchain tokens are no longer legally ambiguous "non-assets"; they have recognized property rights, which can underlie contracts, collateral, and enforcement. As the Vietnamese press explains, the DTIL "ensures ownership, trading and security of digital assets" and protects users from fraud or loss due to legal gaps.

Key insight: *Crypto tokens = legally protected assets.* The law mandates that the government issue detailed rules on digital asset issuance, storage, custody, and ownership rights. Once implemented, this framework should clarify how crypto can be used as collateral in transactions and loans. Indeed, regulators are already working on explicitly recognizing crypto collateral: the Vietnam Asset Management Corp (VAMC) has noted a *"roadmap to recognise digital assets as valid collateral"* is under development. For investors, this means asset protection and enforceability – e.g. pledged tokens can be legally seized or enforced under civil remedies – are becoming more concrete.

Simultaneously, the new law confirms that *any crypto-token that looks like a security (e.g. an ICO project token, investment token, or e-wallet token)* will be regulated as such. By excluding securities and fiat from the crypto category, Vietnam signals that "true" crypto (like decentralised tokens or stablecoins) will be in a distinct sandbox, but attempts to *repackage securities as crypto* will be disallowed. This should give VC investors more clarity on structuring tokenized equity or fundraising vehicles.

AML/CFT Mandates (Article 48.2)

A major theme of the DTIL is institutionalizing AML/CFT and cyber-security in crypto. Article 48 of the law explicitly lists *"measures to prevent money laundering, terrorist financing, cybersecurity, etc."* under digital asset management. In practice, this means licensed crypto service providers (exchanges, custodians, payment apps) must implement enterprise-grade AML/CFT controls. Although the law text does not show "Article 48.2" verbatim, the effect is that crypto firms will be subject to anti-fraud rules on par with banks and securities firms.

Key insight: *Mandatory AML/KYC reduces risk and aligns with global standards.* The government will require licensed VASPs to maintain risk-based AML programs (customer due diligence, transaction monitoring, reporting) – filling a previous legal void. Vietnam's new digital law explicitly empowers regulators to impose international-standard AML measures on crypto businesses. This serves two investor concerns: first, it mitigates regulatory risk (no more "Wild West" environment with banned/legit ambiguity); second, it forces projects to build robust compliance tech *upfront*. For example, Vietnam's largest private bank, Techcombank, has already built a state-of-the-art AML platform (on Oracle/AWS) to screen transactions and customers across its entire book, winning an industry innovation award. Similar enterprise-grade systems will soon be deployed by crypto platforms.

For allocators, this means the exit and onchain risk profile of portfolio companies should improve. Investors can expect licensed exchanges and fintech to be audit-ready on AML. If an investor has concerns about chain-of-custody or FIU reports, the path is becoming clearer: Vietnam's FIU (financial intelligence unit) has been strengthened recently, and crypto businesses will feed into that system. The VBA–ACAMS alliance is another positive sign: the Vietnam Blockchain Association has partnered with ACAMS to certify dozens of Vietnamese AML/CFT professionals. This capacity-building effort explicitly aims to help Vietnam *"exit the FATF grey list"* by raising compliance standards.

In short, the new regime forces all crypto-related firms to install "bank-grade" controls. This level of oversight usually reassures institutional investors: as the law's framers note, it "ensures transparency, security, and user rights". For instance, one Vietnamese analysis highlights that regulated asset rules *"help protect users from risks like fraud or loss"*. In practice, expect licensed crypto companies to perform KYC on customers, report suspicious flows, and cooperate with authorities – just like fintechs and banks. That clarity reduces one major concern for funds: compliance and illicit-use risk.

FATF Alignment & Sovereign Risk

Vietnam remains on the Financial Action Task Force (FATF) "grey list" (increased monitoring) as of mid-2025. That listing cites past deficiencies in anti-money laundering controls, especially involving virtual assets. The DTIL and related measures are explicitly intended to address FATF concerns. By creating a legal framework for crypto and strict AML rules, Vietnam signals it is aligning with global AML/CFT standards.

Key insight: *Clearing FATF "grey" status will lower country risk and cost of capital.* Grey-list economies face higher compliance burdens from foreign banks and investors (due diligence surcharges, reduced correspondent banking). Vietnam's leadership publicly links crypto lawmaking to exiting this list. The CoinDesk report notes: *"This legal recognition comes as Vietnam seeks to improve its stance in the FATF rankings… The country is designated on the FATF's grey list for insufficient AML controls"*. In parallel, Vietnam's regulators have drafted an ambitious FATF action plan (which includes VA/VASP regulation) and established FIU independence. The DTIL's requirements – e.g. state-supervised crypto exchanges and mandatory reporting – are steps toward satisfying FATF's recommendations (Recommendations 15–22 on designating VASPs, CDD, licensing, etc.).

For global investors, this matters. Vietnam's sovereign risk premium (for banks/trade) is partly a function of AML compliance. Demonstrable progress – like passing a digital assets law and rigorous sandboxes – will help Vietnam attract foreign capital by reducing the "AML liability" investors face. We expect Vietnam's grey list status to be reviewed again soon; positive regulatory moves (crypto law, ACAMS training, FIU reforms) could yield an upgrade. Bottom line: capital allocators should factor improving sovereign risk post-DTIL – potentially making Vietnam financial services more investable internationally.

Blockchain-Forward Financial Centers: Da Nang & Ho Chi Minh City

Vietnam is decentralizing its financial infrastructure into two flagship hubs: Da Nang (Central Vietnam) and HCM City. Each is to become an International Financial Centre (IFC) with a focus on innovative fintech and capital markets. Crucially, both hubs will explicitly encourage blockchain and crypto activities through sandboxes, tax incentives, and specialized regulations.

- Da Nang Digital Finance Hub: Da Nang has branded itself a *"financial innovation hub"*. With modern infrastructure and open policies, it aims to trial cutting-edge models. City officials emphasize digital finance, fintech and blockchain as *"key pillars for driving its digital and economic transformation"*. For example, Da Nang is already constructing *"digital financial sandboxes and free trade zones"* where fintechs and crypto firms can *test new products in an open testbed environment*. Regulators have allocated land for an IFC, and a separate decree (94/2025) has established live banking sandboxes (for P2P, credit scoring, API data sharing) starting July 2025. All of this suggests Da Nang will be a controlled environment to trial blockchain payments, asset trading, and trade finance. Key insight: investors should watch Da Nang for pilots: stablecoin remittances, blockchain KYC networks, or tokenized bond sales could first appear here under supervision. Public-private events (e.g. the Vietnam Blockchain Week 2025 in Da Nang) underscore strong local support.
- Ho Chi Minh City International Financial Centre (IFC): HCMC will remain Vietnam's commercial powerhouse and take on a global trading role. The city government has proposed ambitious 2030 targets to rival other ASEAN hubs. Importantly, the IFC is being backed by significant incentives. The government's recent resolution on IFCs grants *preferential tax and visa treatment* for companies and talent in both hubs. For example, qualifying IFC-based firms can pay a 10% corporate tax (CIT) for 30 years (with the first 4 years exempt, 9 years at half-rate) if they operate in encouraged sectors (e.g. fintech, green finance). Skilled experts in the zones get personal income tax exemption on salary through 2030. Transfers of equity and capital contributions between investors and IFC entities may even be tax-exempt until 2030.

Table: Summary of IFC incentives (selected items):

Incentive	Benefit / Duration
Corporate Tax (CIT)	10% for 30 years (incl. 4-yr exemption, 9-yr @50%); 15% for 15 years for other sectors.
Personal Income Tax	100% exemption for experts working in IFCs, thru 2030.
Capital Gains Tax	Exemption on transfers of shares/capitals, thru 2030.

Da Nang and HCMC are coordinating to avoid overlap: Da Nang will focus on *experimental fintech (P2P, digital financing, sandboxed trials)* while HCMC focuses on *capital markets and cross-border banking*. For crypto investors, the takeaway is that any crypto or blockchain startup that locates in the Da Nang or HCMC IFC may enjoy streamlined licensing and tax perks. These hubs are effectively Vietnam's blockchain-special economic zones: expect regulator "sandboxes" and support for innovative projects (see next section). In HCMC's case, major banks and VASPs have already pledged to pilot services in the IFC environment.

Domestic RegTech & Compliance Infrastructure

Vietnam's own tech ecosystem is stepping up to the compliance challenge with new RegTech solutions and training. Three highlights: 1) 1Matrix – a homegrown blockchain network initiative; 2) Techcombank's AML platform – already live; and 3) VBA–ACAMS partnership – building AML expertise.

- 1Matrix ("Make in Vietnam" Blockchain): 1Matrix is a new joint project backed by Techcombank, the Masterise and One Mount conglomerates, and BCG, aiming to build a *Vietnam-designed Layer-1 blockchain network*. Launched May 2025, it explicitly aims to give Vietnam "complete control over blockchain technology". While 1Matrix is positioned as an infrastructure effort (not an exchange), its emergence is significant: it signals confidence in Vietnam's ability to engineer blockchain solutions. For investors, 1Matrix could become a compliance layer or ecosystem on which token projects operate (e.g. domestic stablecoins, supply chain tokens). The initiative also underscores regulatory support for "Make in Vietnam" digital platforms, which may translate to preferential treatment (e.g. if 1Matrix gains official recognition as a "trusted network" for data or payments).
- Techcombank AML Stack: As noted, Techcombank – one of VN's largest banks – has built a sophisticated AML/KYC system with Oracle OFSAA and AWS. It has streamlined all KYC, screening and transaction monitoring into a single platform, achieving efficiencies that earned an international prize. This demonstrates Vietnam's tech sector can develop enterprise compliance software. Techcombank's "Innovation Excellence" award for AML highlights that Vietnamese firms can meet global standards. Going forward, these capabilities will be spun off or offered to fintechs – for example, Techcombank is part of the 1Matrix ecosystem – meaning crypto startups can plug into proven AML engines. For global funds, it means due diligence on Vietnam deals can focus on technology (as local banking-grade solutions exist), not on whether basic compliance is possible.
- VBA–ACAMS Training Alliance: The Vietnam Blockchain Association (VBA) has partnered with the international ACAMS organization to train and certify Vietnamese AML/CFT professionals. VBA leaders themselves recently earned CAMS accreditation and are arranging ACAMS courses via the ABAII Academy. This is the first dedicated push to grow a *"globally recognized pool of AML specialists"* in Vietnam. That means banks, VASPs and regulators can hire locally certified experts, accelerating compliance maturity. The stated aim is to bolster Vietnam's global credibility and support implementation of the new AML law. From an investor's standpoint, this effort reduces the operational risk: projects can recruit trained compliance officers domestically, and regulators will feel more comfortable granting licenses to teams with ACAMS-certified management.

Key insight: *Local RegTech and training are catching up quickly.* In practice, expect Vietnamese crypto/fintech firms to adopt enterprise AML/KYC stacks and hire ACAMS-certified officers. These developments are rarely headline-grabbing, but they matter a great deal for funds: they mean portfolio companies won't have to "re-skill" compliance teams or import all compliance controls. Instead, the domestic ecosystem is delivering solutions (like 1Matrix's infrastructure, Techcombank's software, and VBA's training programs) that plug into the new regulatory regime.

Fintech Sandboxes & Pilot Projects

Vietnam is institutionalizing *regulatory sandboxes* for fintech innovation, and blockchain is at the center. A new Decree (94/2025, effective July 2025) authorizes trialing fintech models in a controlled environment (up to 2-year pilots). Initially focused on banking (P2P lending, credit scoring, open APIs), the sandbox framework is expected to expand. Notably, a National Assembly draft resolution in early 2025 explicitly extends the sandbox to crypto trading platforms and tokenized assets. In other words, Vietnam is setting up a *legal experimentation zone for crypto projects*.

Basal Pay – First Crypto Sandbox Project: Against this backdrop, one Vietnamese startup has announced that it is the first crypto fintech to enter the sandbox. Basal Pay (by AlphaTrue JSC) is a travel/QR payment app that allows users to load stablecoins (USDT/USDC) and spend them via local merchant QR codes (displayed rates in local currency). In July 2025, Basal Pay shared that it had received sandbox approval to pilot its cross-border stablecoin payment solution in Vietnam's hubs. This means Basal Pay can operate its wallet in a limited fashion, giving it legitimacy without needing a full license. While official details are sparse, Basal Pay's entry signals regulators' willingness to greenlight practical crypto use-cases (remittances, tourism spending) under supervision.

For investors, Basal Pay's sandbox slot is a proof of concept that private crypto fintechs can work with regulators and launch real products. The key lesson is that Vietnam is moving from "crypto grey area" to test-and-learn. If Basal's pilot goes smoothly (e.g. enabling thousands of tourists to pay in crypto at shops), we can expect a wave of sandbox applications: USDC/USDT remittance schemes, NFT payment solutions, tokenized FX platforms, etc. Funds should watch the sandbox for dealflow: once the approval process proves workable, well-funded fintechs (both local and regional) will flock to try their products in Vietnam's regulated arena.

Pipeline: Upcoming Regulations

Vietnam's blockchain roadmap doesn't stop at the DTIL. Several important rules are in gestation:

- Draft Law on Centralized Crypto Exchanges: Industry sources report that Vietnam will soon formalize licensing for centralized crypto exchanges. A leaked *"draft resolution"* from June 2025 would allow trading of cryptoassets only on licensed centralized platforms. In plain terms, peer-to-peer trading or unlicensed DEXs would be prohibited. Blockchain companies have pushed back – warning that overly strict rules could stifle innovation – but policymakers seem intent on eliminating the current unregulated grey market. We can therefore expect the final law (or a revised draft) to require VASPs to obtain finance ministry licensing, maintain full AML oversight, and restrict crypto trading to these approved venues. For investors, this means future exchange projects will need to plan for licensing compliance; but it also means a legitimized "official" market will emerge, which is ultimately positive for institutional participation.
- Decree on Blockchain Governance in Financial Hubs: Authorities have indicated that special rules will govern blockchain in the new IFC zones. While the final text is not public, the idea is to create a clear policy and incentives for blockchain projects in Da Nang and HCMC. This may include things like defined roles of regulators (MoF/SBV) in each hub, tax treatments for crypto issuances, tech transfer requirements, and coordination on sandbox approvals. In essence, investors should expect a "one-stop shop" for blockchain in these zones: dedicated licensing procedures, perhaps relaxed KYC limits for pilot programs, and integration with the free trade zone frameworks. The existence of such a decree will further differentiate the hubs as crypto-friendly enclaves.

  Note: As of mid-2025, detailed drafts of these instruments are not publicly available. We therefore advise ongoing monitoring of official gazettes and press releases. However, the broad trend is clear: Vietnam is building a multi-layered legal architecture around crypto – a specialized law, plus hub-specific regulations – rather than a single piece of law.

Investment Implications & Risks

Regulatory Clarity: The big takeaway is that legal and regulatory clarity in Vietnam's crypto space is increasing dramatically. Tokens are now state-recognized assets. AML rules are being codified. Sandboxes and IFC laws are coming online. For capital allocators, this means *policy risk is transitioning from "unknown" to "known unknown"*. Yes, Vietnam's crypto laws remain strict (no mixing crypto and unregulated finance), but at least they are defined. This favors institutional capital.

Timing: Key effective dates: DTIL enforcement begins 1 Jan 2026; the IFC resolution (tax incentives) is effective Sep 1, 2025; Decree 94 (banking sandbox) starts July 1, 2025. The first crypto sandbox projects (like Basal Pay) are launching by mid-2025. The General Assembly is expected to debate the new IFC/centralized exchange rules by mid-2025. Therefore, we see a wave of regulatory rollouts through 2026. Early movers (Q3–Q4 2025) in Vietnam's crypto sector may secure "sandbox" grace periods before full licensing is required.

Upside: Once implemented, the framework could unlock Vietnam's huge latent crypto demand. Funds that get into Vietnamese blockchain infrastructure, token projects, or regulated exchanges early may capture outsized market share. Also, the tech workforce incentives (e.g. tax breaks for personnel) will draw overseas talent, potentially fostering local blockchain R&D hubs. Domestic companies like 1Matrix might become partners or investees, as Vietnam seeks to build national champions in blockchain technology.

Residual Risks: Of course, enforcement is key. The law contains many high-level mandates, but the devil will be in the implementing decrees and licenses. The finance ministry and central bank will shape final rules (for example, capital requirements for VASPs, or criteria for exchanges). There is some industry pushback: for instance, Vietnamese blockchain firms have asked the government to exclude pure technology development activities from harsh crypto-trading rules. If regulators respond by carving out exemptions for "blockchain developers," that would benefit software-oriented startups. But if not, some business models (like running a blockchain protocol node, or offering crypto wallets without trading) could be restricted.

Sovereign risk: Vietnam's continued grey-list status implies external pressure to keep tightening. There is a chance that stricter measures (e.g. onerous suspicious transaction thresholds) could be imposed if FATF deadlines are not met. However, the government appears committed to balancing innovation and compliance, as seen by its multi-pronged approach (laws + sandboxes + training).

Key Insights Summary:

- Crypto Assets = Assets: Digital tokens (blockchain-based) are now explicitly treated as property under Vietnamese law baodautu.vn. This enhances legal certainty for tokenized business models.
- Mandatory AML/KYC: All licensed crypto businesses must implement strong AML/CFT controls. Vietnam's new law requires state-of-the-art compliance, aligning with international norms coindesk.com. This mitigates illicit-use risk and paves the way for institutional investors.
- FATF Alignment: By codifying crypto and strengthening AML, Vietnam aims to exit the FATF grey list coindesk.com. Improved AML compliance will lower Vietnam's risk premium and facilitate foreign capital flows.
- Dual-Hub Incentives: Da Nang and HCMC are designated blockchain/fintech zones with special privileges (sandbox access, 10% CIT, tax breaks for experts) kpmg.com. Investee companies locating there will benefit from these incentives.
- RegTech & Training: Local solutions (Techcombank's AML platform, 1Matrix blockchain network) and capacity-building (VBA-ACAMS) are filling gaps. This means portfolio companies can tap domestic tech and talent to meet compliance standards quickly globenewswire.com.
- Sandbox-Driven Innovation: The approval of Basal Pay's stablecoin payment pilot heralds a broader fintech sandbox program vir.com.vn. Expect a surge of crypto-related sandbox projects (especially in payments, remittance, small-scale tokenization).
- Upcoming Laws: Be aware of draft rules on exchange licensing and hub governance. The crypto trading space will soon be formalized (only licensed exchanges allowed tuoitre.vn), which may dampen unregulated trading but boost compliance.

In conclusion, Vietnam's regulatory overhaul represents both a de-risking and an enabling event for blockchain investors. While strict by global crypto standards, the emerging framework offers far more clarity than the prior limbo. Global capital allocators should now be actively evaluating Vietnamese blockchain ventures and pipelines, with close attention to compliance evolution, the competitive landscape in the IFCs, and the progress of pending decrees. Vietnam's rapid trajectory – from regulatory grey to structured experimentation – makes it one of Asia's most dynamic emerging markets for digital finance.

Sources: Vietnamese government releases and leading press have been used throughout (see citations, e.g. Vietnamese digital asset law commentary baodautu.vnbaomoi.com, FATF updates fatf-gafi.orgcoindesk.com, and official news on hubs/incentives vietnamnews.vn). All quoted figures and legal points are drawn from these sources.

***Nguyen Tran Minh Quan** is a leading legal expert in Vietnam's blockchain and digital asset sector. He serves as Chief Legal Officer of the Vietnam Blockchain Association, CEO of Krysos Trust, and Director of Chaintracer — Vietnam's national anti-fraud and transaction monitoring initiative. Quan is a Certified Anti-Money Laundering Specialist (CAMS) and brought ACAMS, the world's largest AML training organization, to Vietnam. He directly advises the Vietnamese Government on existing and upcoming legal frameworks for digital assets, with a focus on compliance, AML/CFT, and international regulatory alignment.*

Brazil’s Crypto Regulation at a Crossroads: Between Regulatory Maturity and Legislative Overreach

By Anna Lucía Berardinelli

Abstract: Brazil has emerged as one of the most proactive jurisdictions in the development of a regulatory framework for crypto assets. Anchored in Law No. 14,478/2022 and its phased regulatory implementation by the Central Bank (BACEN) and the Securities and Exchange Commission (CVM), the country has embraced a principle-based, risk-sensitive, and technologically neutral approach to supervision. This institutional architecture has been reinforced by public consultations, interpretive guidance, and constructive engagement with market stakeholders. Together, these elements reflect a commitment to legal certainty without sacrificing regulatory adaptability.

However, the regulatory landscape is now at a crossroads. A draft Complementary Law under debate in the National Congress proposes to revoke the current framework and replace it with a more rigid, fragmented structure—raising concerns over legal coherence and institutional continuity. Simultaneously, a Provisional Measure issued by the Executive Branch introduces a sweeping overhaul of crypto taxation rules that may undermine market viability and financial inclusion.

This article critically assesses Brazil’s evolving crypto regulatory regime in light of these developments. It argues that preserving regulatory stability, reinforcing the technical autonomy of supervisory bodies, and fostering convergence with international standards are indispensable to ensuring Brazil’s credibility as a hub for financial innovation in the global digital economy.

I. Institutional Maturity and the Rise of a Principle-Based Framework

Brazil’s journey toward a robust legal and regulatory framework for crypto assets has evolved from a context of normative ambiguity to a stage of institutional consolidation and strategic foresight. For over a decade, crypto-related activities in Brazil operated in a legal vacuum—subject to scattered administrative acts, isolated judicial decisions, and interpretive circulars from tax authorities, with no comprehensive statutory framework to govern them. This fragmented landscape began to shift meaningfully with the enactment of Law No. 14.478/2022, a milestone legislation that introduced, for the first time, a unified and principle-based legal architecture for the crypto economy in Brazil.

Rather than imposing overly granular and technology-specific prescriptions, Law 14.478/2022 opted for a minimalist but conceptually sound approach. It defined “virtual assets” in functional and technologically neutral terms and introduced the category of “virtual asset service providers” (VASPs), inspired by the FATF glossary but adapted to Brazil’s regulatory tradition. The law expressly excluded from its scope assets already classified as financial instruments, securities, or national currencies, thereby preserving regulatory coherence with existing financial and capital markets laws. It also mandated the licensing and supervision of VASPs by a competent federal authority to be designated by the Executive, thereby ensuring institutional flexibility in adapting to evolving market practices.

This legal foundation was operationalized through Decree No. 11.563/2023, which designated the Central Bank of Brazil (BACEN) as the competent authority for supervising VASPs not engaged in activities relating to securities or other instruments under the jurisdiction of the Brazilian Securities and Exchange Commission (CVM). The choice of BACEN was not merely administrative—it reflected a strategic alignment with Brazil’s broader financial regulatory architecture and recognized BACEN’s institutional capacity in prudential oversight, AML/CFT enforcement, and financial market infrastructure regulation.

Critically, Brazil’s regulatory authorities resisted the temptation to front-load the system with exhaustive secondary rules. Instead, BACEN adopted a **phased, consultative approach** to norm development, grounded in stakeholder dialogue and regulatory benchmarking. In 2024 and 2025, it launched three comprehensive **public consultations**: CP 109/2024, CP 110/2024, and CP 111/2025.

- **CP 109/2024** proposed a licensing regime for VASPs based on prudential segmentation, differentiated capital requirements, mandatory segregation of client assets, internal controls, and cybersecurity protocols. This reflected a sophisticated calibration of risk proportionality and institutional maturity, aligning with the regulatory logic seen in the EU’s Markets in Crypto-Assets Regulation (MiCA) and Singapore’s Payment Services Act.
- **CP 110/2024** addressed the integration of cryptoassets into the traditional financial system. It delineated the conditions under which regulated financial institutions may offer custody, trading, or settlement of crypto assets, subject to enhanced risk management and disclosure. Notably, it imposed limitations on proprietary trading with client funds and established segregation mechanisms between legacy and tokenized systems.
- **CP 111/2025** turned to cross-border operations and the applicability of foreign exchange rules to crypto asset transfers. It offered technical clarifications on how existing FX frameworks under Law No. 14,286/2021 and CMN Resolution No. 277/2022 apply to blockchain-based remittances and international stablecoin flows, recognizing both their potential and associated regulatory risks.

These consultations reveal not only a willingness to adapt but a degree of regulatory introspection rarely seen in emerging markets. The process fostered dialogue among regulators, industry actors, civil society, and academia—echoing global standards of *regulatory sandboxing* and *co-regulation*. BACEN's deliberate and transparent sequencing of regulatory interventions reflects institutional maturity and provides a model for jurisdictions navigating similar challenges in digital asset supervision.

Brazil's choice to evolve its regulatory system through incrementalism—rather than sudden legislative overhaul—stands in contrast to jurisdictions that have sought to codify entire token taxonomies in law. By building regulatory capacity through administrative tools, Brazil retains the agility to accommodate future innovations such as decentralized finance (DeFi), tokenized RWAs, and programmable money, without sacrificing legal certainty or systemic integrity.

II. CVM's Functional Approach and Tokenization

In parallel to BACEN's prudential and systemic orientation, the Brazilian Securities and Exchange Commission (CVM) has adopted a functional, context-sensitive, and forward-looking methodology for assessing crypto assets that may fall under the securities regime. This approach was consolidated through **Guidance Opinion No. 40**, issued in October 2022, which marked a paradigmatic shift in the Commission's interpretive stance. Rather than relying on formalistic or purely technological classifications, the CVM embraced a **substance-over-form** doctrine: digital assets are to be qualified based on the economic rights they embody and the functions they perform, regardless of their nomenclature or technological architecture.

Under this analytical framework, a crypto asset is likely to be treated as a security if it represents an expectation of return derived from the entrepreneurial or managerial efforts of third parties, especially in cases where there is asymmetry of information or passive investment. This interpretation aligns the Brazilian approach with the jurisprudence of the U.S. SEC (Howey Test) and the evolving criteria of IOSCO, while preserving autonomy within the Brazilian legal context.

Yet, the regulatory environment for **tokenized receivables, structured finance tokens, and other real-world assets (RWAs)** remains nascent. In the absence of a bespoke regime for these instruments, the CVM resorted to an interim solution by analogically applying the **crowdfunding framework**—originally designed for early-stage equity issuance by small businesses—under **Instruction CVM No. 88/2022**. This analogical application was detailed in **SSE Letters Nos. 4 and 6**, which outlined minimum governance and disclosure requirements for platforms operating with tokenized receivables. While imperfect, this temporary alignment has enabled market continuity while buying regulatory time for a more tailored solution.

Importantly, the CVM's public communications have underscored that this analogical use of the crowdfunding rules is provisional and context-bound. The Commission has recognized that receivables tokenization does not fully overlap with traditional equity fundraising and may require its own sui generis regulatory pathway—potentially in conjunction with BACEN and the National Monetary Council (CMN). This recognition reflects an institutional openness to **regulatory interoperability** and cross-sectoral collaboration.

Tokenization, as a technological and legal phenomenon, raises **complex supervisory challenges**. First, it demands a rigorous assessment of the **underlying asset's legal nature**—whether the token represents credit rights, equity participation, payment obligations, or future revenue streams. Each configuration triggers different legal regimes, including securitization law, financial market rules, and civil obligations. Second, it requires the development of **robust custody frameworks** capable of ensuring investor protection in decentralized environments. This includes clarifying the legal enforceability of smart contracts, the hierarchy of claims in insolvency, and the mechanisms for dispute resolution in token-based environments.

Moreover, the **emergence of secondary markets** for tokenized assets amplifies concerns about market manipulation, insider trading, and liquidity fragmentation. These risks cannot be addressed solely through analogies with traditional securities law; they demand regulatory creativity and granular engagement with blockchain-specific dynamics.

To its credit, the CVM has exercised **regulatory prudence**. It has not rushed to impose overly broad restrictions that might stifle innovation or drive activity offshore. Instead, it has chosen to foster legal certainty by issuing clear, though flexible, interpretive guidance—allowing market actors to innovate within known parameters. This equilibrium between innovation and investor protection has positioned the CVM as a credible and pragmatic authority in the global debate on token regulation.

III. Market Engagement and the Role of Self-Regulation

One of the defining features of Brazil's evolving crypto regulatory landscape is the proactive engagement of industry associations in shaping normative expectations and promoting good practices. While the state has made commendable progress in crafting formal rules, much of the groundwork in developing operational, ethical, and technical standards has been led by the private sector through self-regulatory efforts.

Among the most prominent entities is the Brazilian Association for the Crypto Economy (ABCripto), which has developed widely recognized Codes of Good Practices on topics such as tokenization, anti-money laundering (AML) procedures, investor protection, and crypto asset custody. These instruments—though not legally binding—have gained significant legitimacy by aligning with international benchmarks, such as the Financial Action Task Force (FATF) guidelines and IOSCO's principles for the regulation of digital assets. Their adoption by exchanges, fintechs, and infrastructure providers has contributed to the normalization of compliance procedures in an industry traditionally resistant to formal oversight.

However, ABCripto is not alone in this role. Other organizations have emerged to represent more specialized segments of the cryptoasset and fintech markets. The Brazilian Association of Tokenization (ABToken), for instance, focuses specifically on standards and educational outreach related to real-world asset tokenization, including receivables, real estate, and commodities. Similarly, Zetta, a coalition of digital-native financial institutions, has contributed to the debate on data governance, open banking, and the interoperability of token-based systems with existing financial infrastructure. Additional voices such as the Brazilian Fintech Association (ABFintechs) and Blockchain Brasil have also been active in legislative hearings and regulatory consultations, offering distinct technical and economic perspectives.

The coexistence of these associations reflects the diversity and decentralization of the crypto economy itself. Rather than competing, these entities often play complementary roles: ABCripto acts as a generalist umbrella for crypto market participants; ABToken contributes technical depth in asset tokenization; Zetta brings the viewpoint of consumer-facing platforms; while others fill institutional, academic, or advocacy gaps. This plurality of voices enriches the policy debate and mitigates the risk of regulatory capture by any single interest group.

From the regulators' standpoint, this ecosystem of self-regulation enhances regulatory intelligence. Standards developed by these associations frequently serve as preliminary references in public consultations, working groups, and interpretive guidance by BACEN and the CVM. The procedural legitimacy of these standards—derived from transparent elaboration processes, expert committees, and broad consultation—has helped integrate them into Brazil's evolving regulatory architecture without formal delegation of public authority.

Moreover, this multi-actor governance model improves Brazil's regulatory agility. By allowing industry-led codes to fill normative gaps and preempt risk factors, regulators can focus on setting baseline principles and enforcing compliance in high-risk areas. This dynamic is particularly valuable in fast-evolving contexts like decentralized finance (DeFi), where state-led norm creation may lag behind market developments.

Ultimately, self-regulation in Brazil is not about deregulation. It is about anticipatory governance, where private actors—through collective coordination and public transparency—develop standards that are flexible enough to evolve with the technology but robust enough to promote market integrity and consumer trust. As long as these initiatives remain inclusive, technically sound, and responsive to societal needs, they will continue to play a vital role in complementing the public regulatory apparatus.

IV. Legislative Interference and the Risk of Regression

Notwithstanding the institutional maturity demonstrated by BACEN and the CVM, Brazil's regulatory progress faces a growing threat from the legislative branch. In 2024, a draft **Complementary Law** introduced by Representative Lafayette de Andrada sought to **revoke Law No. 14.478/2022** in its entirety and replace it with an entirely new—and deeply prescriptive—framework. While presented under the guise of harmonization and modernization, the proposal betrays a **legislative logic rooted in formalism**, categorical rigidity, and centralized state control.

The draft bill introduces an **excessive taxonomy of digital assets**, including classifications such as "payment tokens," "exchange tokens," "utility tokens," and "real-world tokens" (RWAs), each of which is linked to different regulatory authorities. This fragmented approach departs radically from the **principle-based structure** of the current regime and would impose **duplicative or conflicting obligations** on actors who today operate under a coherent institutional alignment between BACEN and the CVM.

Most alarmingly, the proposed law contemplates the participation of **administrative entities with little or no technical expertise in financial regulation**—including **commercial registries and notary offices**—in the supervision of tokenized assets and the certification of smart contracts. This would not only dilute regulatory accountability, but also expose digital asset markets to bureaucratic inefficiencies and institutional insecurity. It represents a fundamental misreading of the complex, cross-jurisdictional nature of crypto assets and their supporting infrastructures.

Even if well-intentioned, the legislative effort reflects a flawed assumption: that **expanding the regulatory net ex ante guarantees legal certainty ex post**. In practice, such expansive codification risks triggering **regulatory fragmentation**, introducing **overlapping mandates**, and ultimately **eroding investor confidence**. Instead of preserving the adaptability that has characterized Brazil's successful regulatory trajectory so far, the proposal enshrines **rigidity** and procedural complexity—precisely the kind of legal architecture that rapidly becomes obsolete in the face of technological change.

The risk is not only conceptual, but also institutional. The new bill disregards the results of years of regulatory consultation and stakeholder engagement already undertaken by BACEN and the CVM. If approved, it would represent a **politically motivated legislative reset**, rather than a continuation of regulatory refinement. Such a rupture could set back the credibility Brazil has earned in international forums as a measured and technically competent jurisdiction.

V. Fiscal Measures and Their Chilling Effect on Adoption

In addition to legislative interference, Brazil’s crypto regulatory equilibrium is now threatened by developments in the fiscal domain. In May 2025, the Ministry of Finance issued a Provisional Measure proposing sweeping changes to the taxation of crypto assets. Among the most significant is the imposition of a flat 17.5% capital gains tax on all crypto transactions—both domestic and cross-border—along with the elimination of the current R$35,000 monthly exemption that allows individuals to dispose of crypto assets tax-free below this threshold.

While the measure does not take immediate effect, its provisions would apply starting January 1, 2026, if converted into law by the National Congress. In addition to changing tax rates and thresholds, the Provisional Measure introduces quarterly reporting obligations, restricts the carryforward of capital losses to five fiscal quarters, and extends certain corporate tax rates (CSLL)—raising them from 9% to 15%—to crypto-native financial service providers. These combined effects could disproportionately penalize startups and small operators, who already face high compliance costs under existing rules.

Even more troubling is the structural impact of the proposed regime: every crypto transaction, regardless of size, frequency, or purpose, would become a taxable event. This undermines the economic viability of microtransactions, cross-border remittances, and payment systems based on stablecoins or tokenized fiat equivalents. The introduction of a transaction-triggered tax logic deviates from international best practices, where thresholds, intent, and functionality are used to distinguish taxable gains from ordinary asset use.

Furthermore, the proposed measure ignores the diversity of crypto asset use cases—treating all assets as speculative instruments and disregarding payment, utility, governance, or collateral functions. This one-size-fits-all fiscal treatment risks chilling innovation and may cause actors to migrate to offshore structures, adopt self-custody solutions, or revert to informal markets—precisely the scenarios that regulators and tax authorities aim to avoid.

Though the stated goal is fiscal neutrality, the practical outcome may be reduced compliance, increased opacity, and diminished competitiveness. Rather than leveling the playing field, the tax asymmetry may reinforce incumbency advantages and punish actors who voluntarily operate under the current regulatory perimeter. The proposed CSLL increase, for example, aligns crypto-native institutions with large banks without recognizing their disparate risk profiles, margins, and operational constraints.

To ensure legal certainty and policy coherence, any tax reform in the crypto space must be developed through interagency dialogue and public consultation, incorporating economic data, comparative models, and technological nuance. Premature or disproportionate tax treatment may undo the very compliance incentives that Brazil has worked to institutionalize through BACEN and the CVM.

VI. Conclusion: Preserving Coherence Through Continuity

Brazil’s regulatory architecture for crypto assets stands today as a product of deliberation, technical consistency, and a strategic commitment to **institutional equilibrium**. Far from being reactive or haphazard, the country’s framework—anchored by **Law No. 14.478/2022**, interpreted by the **CVM** and **BACEN**, and reinforced through consultative mechanisms—has favored **principle-based adaptability over legislative maximalism**. This model, while still under construction, already offers valuable lessons for jurisdictions seeking to regulate without stifling innovation.

At this juncture, the risk Brazil faces is not one of regulatory vacuum or inaction. On the contrary, the **threat now comes from legislative and fiscal overreach**—a sudden pivot away from calibrated regulatory development toward fragmented legal experimentation. The **draft Complementary Law**, by replacing a coherent system with an excessively prescriptive taxonomy, risks destabilizing the fragile balance of competencies that has been carefully constructed between BACEN and the CVM. Similarly, the **Provisional Tax Measure**, by conflating all crypto activities into a single taxable framework, ignores the diversity of use cases and may drive responsible actors out of the regulated space.

In such a scenario, the imperative is not to overhaul the system but to **deepen its institutional core**. BACEN and the CVM have demonstrated both the technical capacity and institutional legitimacy required to guide Brazil’s crypto ecosystem through its next phase of development. Their legitimacy stems not from statutory fiat, but from their engagement in **transparent rulemaking, functional interpretation, and regulatory proportionality**. These values must not be sacrificed in the name of expedience or political visibility.

More broadly, the Brazilian experience illustrates a foundational truth: **effective regulation of emerging technologies does not depend on legislative omniscience, but on regulatory humility and continuity**. Overregulation—especially when driven by fragmented political incentives—risks destroying precisely what makes Brazil attractive as a digital asset jurisdiction: legal certainty, institutional predictability, and openness to innovation.

Going forward, **regulatory convergence** must be prioritized. This includes harmonizing tax treatment with regulatory goals, integrating credible self-regulatory initiatives into formal supervisory models, and developing specialized guidance for areas such as DeFi, DAOs, and tokenized RWAs. Equally important is the need to strengthen inter-agency coordination, reduce regulatory overlaps, and maintain **ongoing dialogue with market participants** to ensure responsiveness without volatility.

If Brazil maintains this trajectory—grounded in **regulatory stability, legal clarity, and proportional risk management**—it will not only consolidate its leadership in Latin America, but may also serve as a **template for emerging economies** seeking to navigate the convergence of digital finance, technological innovation, and legal order.

The challenge now is to preserve what has been wisely initiated: a regulatory path that privileges **evolution over rupture**, **trust over coercion**, and **technical merit over political impulse**. In doing so, Brazil can turn its **incipient leadership into a lasting institutional legacy** in the governance of digital assets.

*With over 20 years of experience, **Anna** has extensive expertise in Digital Law, Blockchain, and Web3, working on innovative projects that range from the “new capital markets”, leveraging blockchain technology for the tokenization of financial assets (security tokens), to the development of utility tokens applicable across various industries.*

Anna played an active role in the structuring of pioneering projects in Brazil, contributing to the development of business models and tokenization platforms for Real World Assets (RWA), as well as the securitization of judicial assets. Her work involved strategic interaction with regulators and key players in the digital assets industry, helping to advance the sector’s regulatory framework.

Grow with us as we influence the future of DeFi regulation and Blockchain law.

Follow us to find out all the latest news from the blockchain & legal world.

HOST AN EVENT

Would you like to host an event? We are always looking for members who want to contribute to our community. If you would like to collaborate by hosting an event in your office, please **click the icon above**.

UPDATE YOUR INFO

Please take a moment to fill out our update form for current members by **clicking on the icon above**. Having up to date information ensures that we can tailor events and reach those who move organizations.

BECOME A MEMBER

Would you like to join BLF? **Click on the icon above** to apply for a free membership and find out about upcoming events, access our content for members and be part of the BLF network

Matthieu Gueissaz
Founder
matthieu@blf.io
LinkedIn

Ross Barbash
Founder
ross@blf.io
LinkedIn

Kam Dylan
Non-Executive adviser

Julieta Borlenghi
Global Coordinator

Blockchain
Lawyers
Forum