UAB

Universitat Autònoma de Barcelona

Private international law confronted to blockchain and cryptocurrencies.

Louis Rambert

1. Resume

The dissertation delves into the complexities of private international law (PIL) as it encounters the revolutionary yet challenging landscape of blockchain and cryptocurrencies. This legal field, traditionally grounded in resolving conflicts through territorial connections, faces significant hurdles due to the inherently decentralized and intangible nature of blockchain technology.

A central theme of the research is the adaptation of PIL to effectively govern and integrate cryptocurrencies, smart contracts, decentralized autonomous organizations (DAOs), and initial coin offerings (ICOs). The research underscores the urgency for harmonized regulations within the European Union to address the novel realities posed by these digital technologies, ensuring a stable and secure legal environment conducive to innovation and economic growth.

Key findings include:

Cryptocurrencies: Advocating for the classification of significant cryptocurrencies as financial instruments to provide clarity and enhance legal coherence across EU states.

Smart Contracts: Highlighting the technological essence of smart contracts, suggesting a restrained regulatory approach to avoid overemphasizing their legal significance beyond their functional role in executing predefined actions.

DAOs: Proposing that DAOs be recognized as legal entities where governance is enacted through token-based collective decision-making, thereby necessitating legal frameworks that recognize and address the collective nature of these entities.

ICOs: Drawing parallels between ICOs and traditional IPOs, recommending that absent specific national legislation, ICOs should be regulated under existing frameworks applicable to IPOs to maintain market integrity and investor protection.

Jurisdiction Challenges: Addressing the multifaceted nature of determining jurisdiction in blockchain-related disputes, particularly emphasizing the need for legal frameworks that can adapt to the decentralized operations of blockchain technologies.

The dissertation argues for a forward-looking regulatory approach that not only addresses current technological integrations but also remains adaptable to future advancements in blockchain technology. This approach is vital for ensuring that PIL can continue to protect individuals and businesses while supporting a digital economy characterized by technological innovation and complex international interactions.

2. Abstract

This paper explores the intricate challenges and necessary adaptations within private international law (PIL) in response to the evolving landscape of blockchain technology and cryptocurrencies. As these digital technologies grow in complexity and prevalence, they disrupt traditional legal frameworks and necessitate a reevaluation of existing regulatory approaches. The paper addresses key areas of concern including the classification of cryptocurrencies, the legal interpretation of smart contracts, the recognition of decentralized autonomous organizations (DAOs) as legal entities, and the regulatory alignment of Initial Coin Offerings (ICOs). Additionally, it examines the determination of jurisdiction in disputes involving digital assets. The aim is to highlight how European PIL can effectively integrate blockchain technologies into its legal framework, ensuring stability, transparency, and fairness. Through a detailed analysis, the paper advocates for a regulatory environment that not only accommodates current technological innovations but is also adaptable to future

advancements, thereby supporting the dynamic nature of digital finance within a structured legal context.

3. Index

4. Abbreviations

BTC : Bitcoin
CEX : centralized exchange
Crypto : cryptocurrencies
DAO : Decentralized autonomous organization
DEX : decentralized exchange
ICO : Initial coin offering
IPO : Initial Public offering
KYC : Know your Customer
PIL : Private International Law

5. Introduction

Blockchain technology, akin to a decentralized digital ledger spread across numerous computers worldwide, revolutionized data management by recording transactions in a secure, transparent, and immutable manner. This innovation, introduced in 2008 by an entity or group known as Satoshi Nakamoto, was primarily motivated by the desire to facilitate direct

online payments between parties without the need for financial intermediaries, through the creation of Bitcoin, a peer-to-peer electronic cash system.

As an extension of blockchain's capabilities, cryptocurrencies emerged as digital or virtual currencies utilizing cryptography to ensure secure transactions on this decentralized network. The hallmark of cryptocurrencies is their operation without a central authority, thereby offering a decentralized alternative to traditional financial systems. Every transaction conducted with cryptocurrency is verified and recorded on the blockchain, enhancing transparency and security within this digital financial ecosystem.

In response to the volatility often associated with cryptocurrencies, stablecoins were developed. These are a special category of cryptocurrencies designed to minimize price fluctuations by being pegged to stable assets such as fiat currencies or precious metals. The introduction of stablecoins has been instrumental in bridging the gap between the traditional financial system and the cryptocurrency market, offering the benefits of digital currency—speed, security, and privacy—alongside the stability of the asset to which they are tied.

To manage these digital assets, wallets play a crucial role, functioning similarly to digital bank accounts for cryptocurrencies. They enable users to store, send, and receive cryptocurrencies, with security and ease of access varying between software-based and hardware-based wallets. The unique cryptographic keys associated with these wallets ensure secure access to one's digital assets. With software-based wallet, the private key is stored within interface accessible via a device, hardware-based wallets store the private key in a hardware physical device.

Further expanding the utility of blockchain, smart contracts emerged as self-executing contracts with the terms directly embedded into code. These digital contracts autonomously enforce and execute agreements upon meeting predefined conditions, facilitating a wide range of decentralized applications and transactions without the need for intermediaries.

The innovation continued with the introduction of Initial Coin Offerings (ICOs), a blockchain-based crowdfunding mechanism. Through ICOs, startups have the opportunity to raise capital by selling tokens or coins of a new cryptocurrency project at an early stage, often at a discount, providing a novel way to bypass traditional capital-raising processes.

Decentralized Autonomous Organizations (DAOs) represent another breakthrough, offering a model for a completely autonomous and democratic organization governed by smart contracts. In DAOs, participants have direct say in decision-making processes, exemplifying a new paradigm in organizational governance and investment strategies, free from conventional management hierarchies.

Through these interconnected developments, the blockchain and cryptocurrency landscape not only challenges conventional financial and organizational systems but also paves the way for a more decentralized, transparent, and equitable digital economy.

6. Justification

The blockchain technology by its essence is international and decentralized. And its democratization has posed a challenge in Private international law. The problem is that it's a non-identified legal object. Unlike traditional transactions or operations, blockchains operate on a set of rules that are not grounded in the laws issued by private individuals in accordance with national rights. This characteristic, inherently international due to the diverse actors involved in any given transaction, poses a significant legal conundrum. The core issues stem from the anonymity of users and the decentralized protocols that do not conform to the status of conventional companies. Moreover, the international scope of blockchain transactions exacerbates the difficulty of applying traditional legal frameworks designed around territorial attachments. Recently the FTX case has brought on the light the crypto ecosystem, with the failure of what was the second biggest crypto centralized exchange.

I) Blockchain legal status in Private international law

A. The applicable law for blockchains

Decentralization vs. Territorial Legal Systems

Private International Law traditionally relies on resolving conflicts of laws by identifying a legal system with a territorial connection to the transaction or relationship. However, the immaterial and decentralized nature of blockchain transactions challenges this approach. Notably, the Principle of Relevant Intermediary Approach (PRIMA), from the Hague Convention of July 5, 2006, for determining the applicable law for certain rights held with an intermediary, loses its relevance in blockchain contexts[1]. This is primarily because blockchain technology eliminates the need for traditional intermediation. It's also incredibly difficult to locate an account in the blockchain world but we'll get to that later. Moreover PRIMA refers to "securities" defining them as : "securities" means any shares, bonds or other financial instruments or financial assets (other than cash), or any interest therein. Well, is a token a security? For instance, the Security Exchange Commission do not consider Bitcoin as a security [2](we see that PRIMA exclude cash in this definition). This bring the subject of the stablecoins, I will not talk about algorithmic ones, that I will address them in my second part. So a stablecoins is a crypto which is supposed to keep a stable price indexed on another asset. The biggest one is the USDC, which is indexed on the dollar, so, for each USDC emitted, Circle, the company that produce it, keeps a dollar to assure the value of the token. So, for each USDC you have, Circle hold a dollar, guarantying that is price is all the time one dollar. Circle has for a long time battled with the SEC to not be categorized as a security, for now it's still not considered as such, but there is a possibility that it could be in the future. [3]

---

[1] Audit, Mathias. « Le droit international privé confronté à la blockchain ». *Revue critique de droit international privé* 4, nº 4 (2020): 669-94. https://doi.org/10.3917/rcdip.204.0669.

[2] « SEC.gov | Crypto Assets and Cyber Enforcement Actions ». Consulté le 24 avril 2024. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[3] « SEC.gov | Crypto Assets and Cyber Enforcement Actions ». Consulté le 24 avril 2024. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

Although the status of a cryptocurrency in PIL is a challenge, the problem of the lack of physicality of the accounts are probably the biggest challenge. A wallet is nowhere, it can be accessed anywhere on earth at any moment, so it has no territoriality element to be used to ascertain the applicable law and competent jurisdiction to any given transaction.

A possible solution to this jurisdictional puzzle is focusing on the physical location of private keys, which are essential for controlling blockchain assets. If a private key is stored on a physical device like a Ledger wallet, its location can be determined. However, if the wallet is purely software-based, such as MetaMask, pinpointing its location becomes challenging due to its accessibility from multiple devices across different countries. This situation complicates the application of law, as the digital wallet does not have a physical existence but is merely accessed through devices that serve as temporary access points. Moreover, it would be against the principle of legal certainy because, due to the anonymity, it will be impossible to foresee in advance the potential applicable law and / or competent jurisdiction. [4]

National Approaches to Blockchain Regulation

Another problem is that if we search the applicable law, we must have an applicable law. And in internal law, there is often few or nothing to apply in terms of blockchain transaction and cryptocurrency.
Different countries have taken varied approaches to the legal recognition and regulation of blockchain technology and cryptocurrencies. Monaco, for instance, explicitly states that Monegasque law applies to blockchains, smart contracts, algorithmic enterprises, and cryptocurrencies that produce effects within its territory.[5] However, the criteria of "effect on

---

[4] Guillaume, Florence. « Aspects of Private International Law Related to Blockchain Transactions ». In *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, édité par Daniel Kraus, Thierry Obrist, et Olivier Hari. Edward Elgar Publishing, 2019. https://doi.org/10.4337/9781788115131.00009.

[5] Article 24 Loi n° 1.528 du 7 juillet 2022 portant modification de diverses dispositions en matière de numérique et réglementation des activités des prestataires de services sur

the Monegasque territory" may not be relevant due to the dematerialized nature of blockchain effects.

France has defined cryptocurrencies as "digital assets" in its Monetary and Financial Code. In the French legal framework, cryptocurrency transactions have been accorded a measure of recognition, illustrating an openness towards digital currencies and their integration into the financial ecosystem[6]. However, this acknowledgment does not extend to equating cryptocurrencies with fiat currency in terms of their ability to discharge debts. The distinctive feature here is the absence of a liberatory character for cryptocurrencies: a creditor in France is legally entitled to reject a payment if offered in cryptocurrency instead of traditional money.

In a landmark decision by the Court of Justice of the European Union on October 22, 2015, in the case of Skatteverket v. David Hedqvist, the Court explicitly acknowledged that "the virtual currency 'bitcoin' is a contractual means of payment." [7]Furthermore, the Court observed that "it is a well-established fact that the virtual currency 'bitcoin' has no other purpose than to serve as a means of payment and that it is accepted for this purpose by certain operators." This pivotal ruling underscore the legal acceptance of cryptocurrencies, such as Bitcoin, as a valid form of payment within the EU, provided there is contractual agreement to this effect.

While in the United States, the Securities and Exchange Commission (SEC) has legislated extensively on cryptocurrencies, not defining Bitcoin as a security but classifying numerous other cryptocurrencies as such. But, all of those only give an existence for cryptocurrencies by attributing them a financial status, but do not address the legal regime of the blockchain, as a whole.

---

actifs numériques ou sur crypto-actifshttps://legimonaco.mc/tnc/loi/2022/07-07-1.528/index.html#zioOiMXu38d6mvVpb9sU5d

[6] Article L54-10-1 of the Code monétaire et financier

[7] Skatteverket v David Hedqvist, No. Case C-264/14 (ECJ 22 octobre 2015).

The Role of Party Autonomy in Blockchain Transactions

Given the inadequacies of traditional conflict of laws systems to address the unique aspects of blockchain transactions, the simplest solution may lie in allowing parties to choose the applicable law. This choice provides the necessary legal certainty regarding the juridical existence of transactions conducted on the blockchain. For instance, parties to a smart contract or transaction can mitigate the risk of legal uncertainty by selecting the law of a state that recognizes the legal existence of smart contracts or cryptocurrencies. This elective approach, however, remains specific and does not establish a general legal principle.

The challenge of applying traditional principles of Private International Law to blockchain technology underscores the need for a new legal paradigm. The decentralized, immaterial nature of blockchain transactions requires a subjective criterion based on the parties' agreement to ensure legal certainty. And most of blockchain transaction (from a wallet to a DEX, from a wallet to a game platform, from a wallet to a DAO…) are done between people or entities that do not know each other, and do not even know the geographical location of the other part. [8]

However, we can believe that in the future exchange (such as Binance, kraken, crypto.com…) will be used more and more for crypto transaction. Despite, the FTX crisis has not led to increase the trust in those. They are already being often used to exchange, in the first place, currency for cryptos, and many people hold their assets on this platform instead of a ledger. Many “crypto traders” keep sometimes very large amount as token there, because those people need to trade fast, and only those platforms allow to do so, according to them. In addition, they provide trades interfaces with financial metrics, which wallet do not. We cannot predicted the futures, but even though wallet interfaces like ledger live or Metamask has much improved in accessibility, it’s not unreasonable to think that in the future the share

[8] Audit, Mathias. « Le droit international privé confronté à la blockchain ». *Revue critique de droit international privé* 4, nº 4 (2020): 669-94. https://doi.org/10.3917/rcdip.204.0669.

of user of centralized exchange increase to the detriment of wallet. Those exchanges hold the crypto for you in wallet, with and undifferentiation of storages of assets, they just have pools of each crypto for alle the clients. In this case, all those companies are based somewhere. So there, crypto transaction has a "*for*", it's the place where the company have the headquarter or is incorporated. Plus, all those platforms now require a KYC to comply with anti-laundering laws. So here, even though it's still a "purely" blockchain transaction (technically you still send the money to a public key), you have a known individual A with a "crypto bank account" 1 sending money to a known individual B with a "crypto bank account" 2. So here the provision of classical PIL for financial transaction apply. Even though all of this is obvious, and do not the challenge and classical problematics of blockchain transactions, I still wanted to address it because, here the transposition of rules of PIL are much easier.

But generally, we have seen that is impossible to regulate the blockchain by addressing the technology. So, we must regulate it by addressing all the specific usages it allows. We can base this reasoning on the principle that law regulates better human behaviour than technology itself. [9]

B. The legal status of the smart contract

At their core, smart contracts are autonomous code blocks that execute predefined actions, such as payments, based on "if, then" logic. This autonomy implies that once deployed, the execution of smart contracts is determined solely by their internal logic, making them immutable by any of the parties involved. The principle "code is law" underpins the supposed "core" of smart contracts, suggesting that the code itself enforces the agreement between parties.

However, the term "contract" in "smart contract" might misleadingly evoke the legal notion of a contract, which traditionally encompasses elements such as offer, acceptance, and mutual consent. In contrast, smart contracts are essentially scripts that automate specific actions

[9] Reyes, Carla L, Nelson M Rosario, Rachel M Cannon, et Richard Tall. « PANEL I: BLOCKCHAIN AND THE LAW », s. d.

without necessarily incorporating these legal fundamentals. The diversity among smart contracts is significant; they can involve tokens or not, require permissions for execution or operate without it, and may or may not include cryptocurrency.

Despite the seemingly autonomous nature of smart contracts, they do not exist in a legal vacuum. The initial agreement or contractual backdrop to a smart contract's execution implies a pre-existing consensus that precedes the technology's operation. This relationship highlights the inapplicability of smart contracts as standalone legal entities, detached from national laws. Especially in areas concerning "peri-contractual" rules, regulations pertaining to the execution of a contract without defining or establishing its regime, such as competition law, consumer protection, financial, banking, or insurance regulation, where the protection of the weaker party is paramount, smart contracts cannot be considered in isolation from the specific legal domain they touch upon.[10]

In traditional obligations between private individuals, it is the pre-existing obligation that is subject to national law, not the smart contract, which merely facilitates the transfer of that obligation. Analogously, a scheduled bank transfer is not viewed as an autonomous part of an obligation but as a payment tool resulting from the main obligation. However, integrating a smart contract as a mode of executing a contract, such as in an insurance contract that compensates automatically, via a smart contract, a passenger for transport delays based on official announcements of the transport company, can imbue it with legal legitimacy. This integration could extend to Ricardian contracts[11], which are both machine-executable and

---

[10] Rühl, Giesela. « Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts? » In *Blockchain, Law and Governance*, édité par Benedetta Cappiello et Gherardo Carullo, 159-80. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-52722-8_11.

[11] Rühl, Giesela. « Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts? » In *Blockchain, Law and Governance*, édité par Benedetta Cappiello et Gherardo Carullo, 159-80. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-52722-8_11. (about the Ricardian contract)

human-readable, offering a more nuanced approach to blending digital execution with legal comprehensibility.

Despite these possibilities, a significant challenge arises from the anonymity prevalent in smart contract interactions. Many users engage with smart contracts without knowledge of the other parties involved. This anonymity complicates legal disputes, especially in private international law (PIL), where one of the general principle applies the law of the defendant's domicile. Without information on contract execution location or defendant domicile, legal proceedings stall. To address this, it might be prudent to apply the law of the plaintiff's domicile in cases of total anonymity, aligning with the fallback provision in Article 4.2.4 of the Rome I Regulation on the law applicable to contractual obligations, which dictates applying the law with the closest connection to the contract, often the plaintiff's domicile in anonymous smart contract scenarios.

This exploration into smart contracts within the blockchain context reveals their complex interplay with legal frameworks, underscoring the necessity for legal adaptation to accommodate the unique characteristics of blockchain technology while ensuring protection and fairness for all parties involved.

C. The legal status of DAO

A Decentralized Autonomous Organization (DAO) represents a novel approach to organizational governance, characterized by decentralization and automated operations via blockchain technology. Unlike traditional organizations, DAOs operate without centralized control, relying on smart contracts to enforce rules and execute decisions based on member consensus. These smart contracts are programmed agreements that automatically perform actions when specific criteria are met.

The essence of a DAO lies in its democratic governance structure, where decision-making power is distributed among its members through cryptographic tokens that represent voting rights. This setup promotes transparency, inclusivity, and equity, allowing members to directly influence organizational policies and actions.

In essence, DAOs offer a revolutionary model for organization management, leveraging blockchain technology to facilitate secure, transparent, and autonomous operations. This model challenges conventional organizational hierarchies, advocating for a more decentralized and democratic approach to governance. For example, a DAO can be used for investment purposes. For an investment DAO, each members send an amount of money to a smart contract, in return they receive a token of governance that will serve to vote to decide where to allocate the commons funds of the pools.

DAOs represent a significant innovation in the business and blockchain technology world, offering a unique organizational structure where decisions are made collectively by its members. However, their intangible nature and operation based on smart contracts pose significant legal challenges. One of the major issues with DAOs is that they often lack legal personality and were not created with the status of a traditional company. This situation raises several questions regarding their regulation and legal recognition.
[12]

Although participants and creators of DAOs may not seek to submit themselves to a national legal status, preferring to self-regulate under the principle of "code is law," it is important to nuance this principle. Indeed, DAO members are capable of voting to cancel or rectify actions retroactively, showing that nothing is theoretically untouchable within a DAO.

However, even if DAO members wished to obtain legal recognition, it is not always clear what company status would be attributed to them by national laws. The state of Wyoming in the United States has been a pioneer (and is to these days the only one) in this area by allowing DAOs to register as Limited Liability Companies (LLCs), with specific requirements tailored to their nature.[13] These requirements include the explicit mention that the entity is a DAO, identification of all smart contracts used for its operation, and a declaration explaining how decisions are made within the DAO, particularly what portion of

---

[12] Metjahic, Laila. « DECONSTRUCTING THE DAO: THE NEED FOR LEGAL RECOGNITION AND THE APPLICATION OF SECURITIES LAWS TO DECENTRALIZED ORGANIZATIONS ». *CARDOZO LAW REVIEW* 39 (s. d.).

[13] Wyoming Secretary of State Business Division Decentralized Autonomous Organization (DAO): Frequently Asked Questions https://sos.wyo.gov/Business/Docs/DAOs_FAQs.pdf

these decisions is made algorithmically. Wyoming thus treats DAOs the same way as other LLCs, granting them the same legal protection and offering real legal security to DAOs.

Outside of Wyoming, American legal doctrine tends to assimilate DAOs, by default, to "registered partnerships," a position confirmed by the "Sarcuni v. bZx DAO" case law[14]. So, in the US, a DAO has very great chances to be qualified by the judge as a registered partnership. A "registered partnership" is an association of two or more persons aiming to generate profits, not needing to be a separate legal entity. However, these legal principles are mainly limited to the United States, [15]and private international law struggles to assign a specific commercial structure type to DAOs, especially when they are not registered anywhere and when no national law or jurisprudence allows assigning a default status to these entities.

In this context, two scenarios seem possible for private international law facing DAOs: either apply an existing default status, like the "registered partnership" in the United States. Or, for example the "société de fait" in France, the "de facto company" in France, applies when a company is formed in deviation from the standard formation rules (capital deposit, statutes, etc.) or in cases where the founders did not intend to create a company and no legal act was performed, but the criteria of Article 1832 of the French Civil Code, that define the company, are still met. Article 1832 of the French Civil Code states :
“"La société est instituée par deux ou plusieurs personnes qui conviennent par un contrat d'affecter à une entreprise commune des biens ou leur industrie en vue de partager le bénéfice ou de profiter de l'économie qui pourra en résulter. Elle peut être instituée, dans les cas prévus par la loi, par l'acte de volonté d'une seule personne. Les associés s'engagent à contribuer aux pertes."
"The company is established by two or more persons who agree by contract to allocate to a common business their goods or industry with the aim of sharing the profit or benefiting from

---

- [14] Sarcuni v. bZx Dao, United States District Court, Southern District of California, Mar 27, 2023 22-cv-618-LAB-DEB |. https://casetext.com/case/sarcuni-v-bzx-dao.

[15] Reyes, Carla L, Nelson M Rosario, Rachel M Cannon, et Richard Tall. « PANEL I: BLOCKCHAIN AND THE LAW », s. d. (page 14 about registered partnership)

the economy that may result from it. It can be established, in cases provided for by law, by the act of will of a single person. The partners commit to contribute to the losses."
The French legal commentators mostly think that DAO could not escape, in front of a judge, to this qualification.
The second conditions would be to seek the closest possible company status in domestic law.
Either way, the immateriality of blockchain suggests that the applicable law should be that of the place of damage, that would be the victim's residence location, in the absence of other choices.[16]

This situation highlights the need for deep legal regulation on DAOs, to provide them with a legal framework suited to their unique nature.

D) The legal status of ICO

Initial Coin Offerings (ICOs), are a fundraising mechanism inspired by Initial Public Offerings (IPOs), project initiators seek public contributions in cryptocurrencies. In return, investors are granted tokens that provide rights or benefits, such as voting on project decisions, a share of the profits generated by the project, or access to the technology developed.

For now, most of ICO just don't comply with any type of compliance that is required in most country of the world for product that calls the consumer. But one of the first things to note is that for now, there are no contracts between the investor and the seller during ICO, contrary to the investment in classical financial products. So the relation between the seller and the investor must be qualified as extra-contractual.

Regarding the application of national laws in financial regulation and public offerings, several complex questions arise. The first question is whether these laws aim to extend their

[16] Audit, Mathias. « Le droit international privé confronté à la blockchain ». *Revue critique de droit international privé* 4, nº 4 (2020): 669-94. https://doi.org/10.3917/rcdip.204.0669. (page 694, about the residual forum of that is the victim's reidence)

legislation to Initial Coin Offerings (ICOs). This point, which concerns the scope of application ratione materiae of national laws, is often not clearly defined. Generally, it is not apparent that a token can be qualified as a financial instrument, which would be necessary for it to fall under the legislation applicable to public offerings. [17]The second question stems from the first and pertains more to conflicts of laws: it involves determining which ICO operations are covered when these laws intend to substantively regulate them. ICOs, being able to target investors worldwide, present significant challenges for their promoters who must adjust their operations to comply at least with the legislation of the main financial markets, which could complicate their processes. A more practical solution might involve restricting access to ICOs to investors from specific countries, where the ICO's code would have anticipated and complied with the relevant legislations when engaging with an investor. However, it is notable that the 25 countries receiving the most ICOs have very diverse legislations, further complicating this approach.[18]

1. **United Kingdom**
   - The Financial Conduct Authority (FCA) in the UK treats ICOs as potentially falling within or outside of its regulatory perimeter based on specific characteristics of the ICO. The FCA does not uniformly classify all ICOs as securities; instead, it employs a case-by-case analysis to determine the applicability of its regulatory framework. Such an analysis considers the rights and obligations attached to the tokens issued. Despite its rigorous framework, the FCA acknowledges limitations in its jurisdiction, especially regarding ICOs based overseas that do not engage in regulated activities within the UK.[19]

---

[17] Reyes, Carla L, Nelson M Rosario, Rachel M Cannon, et Richard Tall. « PANEL I: BLOCKCHAIN AND THE LAW », s. d. (page 2 and page 21 to 24)

[18] Kaal, Wulf, Professor at University of Saint Thomas School of Law, Director of the Private Investment Funds Institute, et Minneapolis. « Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses (as of May 2018) ». *Stanford Journal of Blockchain Law & Policy*, 23 juin 2018. https://stanford-jblp.pubpub.org/pub/ico-comparative-reg/release/2.

[19] FCA. « Initial Coin Offerings », 12 septembre 2017. https://www.fca.org.uk/news/statements/initial-coin-offerings.

2. **Switzerland**

- Regarded as a blockchain-friendly jurisdiction, Switzerland, through its Financial Market Supervisory Authority (FINMA), has adopted a more facilitative approach towards ICOs. FINMA's guidelines categorize tokens into different types based on their functionalities—such as utility, payment, or asset tokens—and apply regulatory principles accordingly. This nuanced classification helps in aligning regulatory responses with the specific risks and characteristics of each token type. Furthermore, FINMA has voiced strong support for the underlying blockchain technology, recognizing its potential to innovate financial markets.[20]

3. **Germany**

- The approach taken by Germany's Federal Financial Supervisory Authority (BaFin) focuses heavily on the specific rights that tokens confer on holders. German regulation is meticulous in determining whether a token should be treated as a security, an investment, or a new form of digital asset. This determination hinges on the detailed functionalities and the legal claims associated with the token. BaFin's guidelines emphasize a regulatory assessment that is grounded in the language and spirit of existing securities supervision laws.[21]

4. **France**

- France has pioneered a novel regulatory pathway for ICOs through the introduction of an optional visa regime under its PACTE law. This regime is particularly notable because it provides a framework for token offerings that do not meet the traditional definition of financial instruments. ICOs that successfully obtain this visa from the Autorité des Marchés Financiers (AMF) must meet stringent informational and operational standards, thereby ensuring a higher degree of investor protection. This approach distinguishes between ICOs

---

[20] Eidgenössische Finanzmarktaufsicht FINMA. « La FINMA pubblica una guida pratica sulle ICO ».. https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/.

[21] BaFin. « Crypto Tokens ». Consulté le 27 avril 2024. https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/DLT_Blockchain_Krypto/Kryptotoken/Kryptotoken_node_en.html.

based on the nature of the tokens issued, providing clarity and security for both issuers and investors.[22]

5. **United States**

- In the United States, the Securities and Exchange Commission (SEC) applies the Howey Test to determine whether an ICO constitutes an offer or sale of securities. This determination fundamentally affects the regulatory treatment of ICOs, requiring compliance with stringent securities laws if the tokens are deemed securities. The SEC has been proactive in pursuing enforcement actions against ICOs that fail to comply with its regulatory [23]standards, underscoring a commitment to investor protection and the integrity of its financial markets.[24]

The variability in national regulatory approaches presents significant legal and operational challenges for ICO promoters, especially given the international scope of ICOs that target a global pool of investors and are accessible across national borders. Legal uncertainty arises from the lack of uniform standards and definitions for digital tokens, adding layers of complexity for entities attempting to launch ICOs. Companies must navigate a labyrinth of regulations that may differ drastically from one jurisdiction to another. Furthermore, adhering to multiple regulatory frameworks can be prohibitively expensive and complex. ICO issuers often need to tailor their offerings to meet the specific legal requirements of each country where their tokens are marketed, which can stifle innovation and limit market access. Additionally, when disputes arise, the applicable legal framework can be unclear, particularly

---

[22]Article 82 LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1), 2019-486 § (2019).

[23] « SEC.gov | Cryptocurrency/ICOs ». Consulté le 27 avril 2024. https://www.sec.gov/securities-topics/ICO.

[24] Kaal, Wulf, Professor at University of Saint Thomas School of Law, Director of the Private Investment Funds Institute, et Minneapolis. « Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses (as of May 2018) ». *Stanford Journal of Blockchain Law & Policy*, 23 juin 2018. https://stanford-jblp.pubpub.org/pub/ico-comparative-reg/release/2.

if multiple jurisdictions are involved. This uncertainty can deter investment, complicate enforcement of rights, and lead to inconsistent legal outcomes.

II) Decentralization and localization of the damage

A. Determining the applicable law to theft and hack

In the complex digital world of Web 3.0, cryptocurrency wallets, due to their anonymous nature, become prime targets for cyberattacks. This vulnerability is exacerbated by the fact that users, often poorly informed, can interact with malicious smart contracts or respond to phishing attempts, thereby jeopardizing their digital assets. The blockchain, with its decentralized and virtual character, raises thorny questions regarding territorial jurisdiction and the responsibility of intermediaries and interfaces with which users interact to access their cryptocurrencies.

European private international law, through Article 7.1 of the Brussels I bis Regulation, offers a criterion based on the place where the damage occurred or the risk of its occurrence, thus attempting to address the difficulties related to the geographical localization of damage in the virtual context of the blockchain. Since 1976, the CJEU has made a distinction between the place of actual occurrence of the damage and the place of the causative event, thereby offering flexibility in the choice of jurisdiction (CJEU, *Mines de potasse d'Alsac*e). However, the specificity of financial damage and the anonymity inherent to the blockchain complicate the application of this jurisprudence to cases of theft and loss of cryptocurrencies.[25]

Decentralized exchanges (DEXs), which keep no information on users, contrast with centralized exchanges (CEXs), comparable to crypto banks, which hold key information on their clients through the Know Your Customer (KYC) process. This difference is crucial in the context of cryptocurrency theft, since CEXs, with their clearly established structures and

[25] Lehmann, Matthias, et Emeric Prévost. « La Localisation Du Dommage Dans Le Web3 ». SSRN Scholarly Paper. Rochester, NY, 2021. https://papers.ssrn.com/abstract=4453652. (page 7 and 8)

regulatory authorizations, can serve as legal anchorage points. In the case of a hack of a DEX account, the place where the account is could be the place of the materialization of the damage[26]. Although is it interesting to note that in European PIL, the CJEU retains that the place of where the bank account is located is relevant in financial damage as the forum of the localization of the damage (CJEU, *Kolassa*), but under the light of "*Helga Löber v. Barclays Bank plc preliminary question from the Austrian Supreme Court, the Oberster Gerichtshof*.", [27]it seems that in practice, the place of the bank account is only relevant when it coincide whit the place of the domicile of the defendant, to establish the place of materialization of the damage as the place of domicile of the defendant. But, in the world of CEX, it is difficult to determine where the" account", are domiciled, because they do not have a clear place of localization as classical bank account. Ans as says previously, the CEX just retain the crypto for you, and those crypto have no real place of storage, just an access key. But, it is probable that a European court could interpret that a for example, a French user accessing Binance via Binance.fr, while the company is registered in the AMF (French authorities of regulation), have then a "French account" on Binance. And so on with every European country.

When cases do not fall within the framework of CEXs, an alternative approach would be to consider the network itself as a criterion for territorial attachment, given the inadequacy of the server criterion for determining applicable law. This approach is grounded in the jurisprudence of the CJEU, which has highlighted the importance of users' relationship with web interfaces, regardless of their tangible nature.[28]

---

[26] Buonanno, Luigi. « La responsabilité civile à l'heure des nouvelles technologies : l'influence de la blockchain », s. d.(page 33)

[27] « CURIA - Documents ».. https://curia.europa.eu/juris/document/document.jsf;jsessionid=289B6BD70C7715CBCCBC754BDF5BE92A?text=&docid=205609&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1780236.

[28] Lehmann, Matthias, et Emeric Prévost. « La Localisation Du Dommage Dans Le Web3 ». SSRN Scholarly Paper. Rochester, NY, 2021. https://papers.ssrn.com/abstract=4453652. (paeg 9 and 10).

The administration of blockchains by identifiable entities suggests that the headquarters of these companies could serve as a criterion for territorial attachment. This is all the more relevant for major blockchains managed by well-identified companies, with the notable exception of Bitcoin. Determining the liability of these network administrators could, in the context of European law, characterize the place of administration of the blockchain as the "place where the harmful event occurred or may occur," thus offering a solution to the challenge posed by the anonymity and virtual nature of the blockchain.[29]

In the absence of clear geographical criteria, the defendant's forum becomes a pragmatic solution, reflecting the logic that those responsible for a wrongful act should be subject to the jurisdiction of their own tangible location. This approach, albeit suboptimal, acknowledges the necessity to adapt traditional legal principles to the complex and rapidly evolving ecosystem of Web 3.0 and the blockchain.

B. Characterization of scam and abuse of trust

Scams within the blockchain and cryptocurrency sector, while less frequent now than in the past, still occur with much greater regularity than in traditional financial spaces. This disparity is chiefly due to the blockchain sector's lax regulatory environment coupled with its history of significant financial gains, as seen in Bitcoin's remarkable performance. Such conditions have attracted a mix of highly speculative investors, whose approach often mirrors gambling more than genuine investment strategies, and young individuals new to both the cryptocurrency world and investing at large.[30]

These newcomers are particularly vulnerable to what are known as "scams," where creators of new cryptocurrencies or NFTs promise unrealistic returns on investment behind what are,

---

[29] Lehmann, Matthias, et Emeric Prévost. « La Localisation Du Dommage Dans Le Web3 ». SSRN Scholarly Paper. Rochester, NY, 2021. https://papers.ssrn.com/abstract=4453652. (page 18 and 19 about the anchorage point constituted by the CEX)

[30] Dakroub, Roy, Bernadett Koles, et Helmi Issa. « Crypto consumers' personality traits, and the impact of brand personality on cryptocurrencies' identity ». *Journal of Customer Behaviour* 20 (1 janvier 2022). https://doi.org/10.1362/147539221X16356770010749.

essentially, projects with no substantial value or foundation. This type of scheme is not unique to the blockchain; it mirrors traditional financial scams, including overblown promises by banks or investment funds designed to lure in unsuspecting investors.

Navigating the complexities of litigation surrounding the issuance of financial instruments can be particularly challenging when it comes to identifying the competent court. At first glance, the issuance of financial instruments seems ideally suited for the application of jurisdictional rules specifically related to contractual matters. Indeed, issuing financial instruments typically involves entering numerous contracts: the issuer will enlist one or more banking institutions to support the operation, with distinctions made based on the level of involvement they have in the issuance process.[31]

Beyond this pronounced contractual dimension, financial investment litigation may also engage specific rules related to tort liability. This aspect is especially evident concerning the liability of those marketing financial instruments, be it cryptocurrencies or NFTs. Here, the challenge lies not only in navigating the contractual relationships but also in addressing issues of tortious conduct that may arise in the marketing and sale of these instruments.

But of course, the crypto ecosystem have cut most of the intermediaries between the creator of the “financial product” and the consumer. Especially via the ICO.

In the realm of private international law, the adaptation to blockchain technology, particularly regarding smart contracts, does not primarily encounter significant obstacles in identifying applicable law. The traditional conflict-of-law methods are capable of determining the relevant legal framework without the need for modification. The real challenge lies within the smart contracts themselves, which necessitate an adjustment, specifically the lifting of user anonymity, to fall under a national legal regime.

[31] « Localisation du préjudice financier au lieu du compte bancaire : vers un quasi forum actoris ? | La base Lextenso . https://www.labase-lextenso.fr/gazette-du-palais/GPL333r1.

In exploring the implications of where damage in digital asset fraud can be localized, it becomes pertinent to consider the scenario where the damage is associated with the location of the digital asset portfolio. Drawing an analogy from the CJEU cases of Kolassa and Löber, financial harm caused by misleading or incorrect information at the time of acquiring digital assets could be localized at the victim's domicile, particularly if the digital account or wallet used for payment was held there, provided the acquisition was subject to prior information or disclosure requirements. This approach is in line with the existing regulatory trend that mandates disclosure obligations, often in the form of a white paper, when issuing certain digital assets not already covered by financial instrument laws.[32]

However, applying this rationale becomes complex with digital assets like bitcoins or ethers, where identifying any specific issuer is challenging. In these cases, analogizing the Kolassa and Löber jurisprudence could be deemed precarious. The CJEU, in its "Kolassa[33]" case, permits a multiplicity of forums for jurisdiction competence according to the Brussels I bis Regulation, following the principle of its jurisprudence "Mines de potasse d'Alsace", which interprets that the place of materialized damage is where the harm is suffered.

When considering scams involving digital assets, the domicile of the defendant can play a crucial role if their account is in their country of domicile, as established in the Kolassa and Helga Löber v. Barclays Bank [34]plc cases. If the person holds their cryptocurrency in a centralized exchange (CEX) account, this forum could likely be applicable. However, if the assets are stored in a decentralized exchange (DEX), the applicability of this jurisdictional rule becomes uncertain, potentially complicating the legal landscape for victims seeking redress for digital asset fraud.

---

[32] Lehmann, Matthias, et Emeric Prévost. « La Localisation Du Dommage Dans Le Web3 ». SSRN Scholarly Paper. Rochester, NY, 2021. https://papers.ssrn.com/abstract=4453652.

[33] C-375/13 – Kolassa Judgment of the Court (Fourth Chamber) of 28 January 2015 Harald Kolassa v Barclays Bank plc

.

In European private international law, a notable development occurred with the May 2021 CJEU judgment in Vereniging van Effectenbezitters v. BP plc[35]. The Court of Justice of the European Union (CJEU) introduced a new criterion for judicial jurisdiction based on the location where financial securities are listed. This decision stemmed from a lawsuit initiated by a Dutch shareholder association against British Petroleum (BP) following the dissemination of what were deemed misleading and incomplete information regarding the 2010 Deepwater Horizon oil spill. BP, listed in London and Frankfurt, saw its shares devalued following these revelations, leading to losses for shareholders.

The CJEU adopted an approach that focuses not on the victim but rather on the issuer of the securities, dismissing the location of the victim's bank account in favor of the market where the securities are listed and where the issuer is obligated to meet disclosure requirements. This orientation suggests that jurisdiction should be based on the stock listing location, considered reasonably predictable for the issuer. However, this jurisprudence does not change the rules applicable to unlisted securities, which remain subject to previous criteria.

The challenge of localizing damage in transactions involving cryptocurrencies further complicates this framework. Given the transnational and anonymous nature of the blockchain, identifying the "market" affected by a fraudulent ICO can be complex. However, it might be worth considering the possibility that the headquarters of the company managing the blockchain involved in the fraudulent ICO could constitute a competent forum. This would make sense in a Web3 context where the network not only creates the community but also the market. Indeed, the administrators of a blockchain are not detached from the projects that circulate on it, which could legitimately attract jurisdiction to the location of the blockchain's management, in the sens of the CJEU judgment in Vereniging van Effectenbezitters v. BP plc.

C Legal responsibility for the value of a stablecoin

[35] Case C-709/19, made by decision of 20 September 2019, received at the Court on 25 September 2019, in the proceedings
Vereniging van Effectenbezitters V BP plc,

A stablecoin is a type of cryptocurrency designed to maintain a stable value relative to a specific asset, typically a fiat currency like the US dollar or the euro. This stability is achieved through various mechanisms such as pegging the stablecoin to a reserve of the corresponding fiat currency, using other cryptocurrencies as collateral, or employing algorithmic formulas that automatically adjust the supply of the stablecoin based on its market performance. The primary aim of stablecoins is to combine the instant processing, security, and privacy of cryptocurrency transactions with the stable valuations of fiat currencies, thus avoiding the high volatility typically associated with cryptocurrencies like Bitcoin. Stablecoins are widely used in the digital finance world for transactions, trading, and as a store of value, providing a digital alternative to traditional banking without the turbulence seen in many other digital currencies.

Pegged stablecoins and algorithmic stablecoins represent two fundamentally different approaches to achieving price stability in the cryptocurrency world. Pegged stablecoins, also known as fiat-collateralized stablecoins, maintain their value by holding a reserve of a stable asset, typically a fiat currency like the US dollar, in a 1:1 ratio. This means that for every stablecoin issued, there is an equivalent amount of fiat currency kept in reserve, ensuring that the stablecoin can always be redeemed for its fiat counterpart. This method provides a high degree of stability and trust because the value of the stablecoin is directly backed by tangible, real-world assets held by a centralized authority.

On the other hand, algorithmic stablecoins do not rely on reserves of other assets to maintain their value. Instead, they use a software algorithm to control the supply of the stablecoin, expanding or contracting it in response to changes in demand. The goal is to mimic the mechanisms of a central bank but in a decentralized and automated way, adjusting the supply based on predefined rules to maintain a stable price. While this approach offers the benefit of decentralization and eliminates the need for large reserves, it also introduces a greater risk of volatility and instability, as seen in various high-profile failures of algorithmic stablecoins where the mechanisms could not maintain the peg under extreme market conditions. Algorithmic stablecoins, such as Terra LUNA, highlight complex issues of accountability and responsibility in the realm of digital currencies. Terra LUNA, designed to maintain a peg of one token to one US dollar, dramatically failed to uphold its value during a market stress

period. The underlying algorithm, intended to adjust supply dynamically to stabilize price, was unable to manage the sudden fluctuation in demand effectively. As a result, the stablecoin depegged, causing its value to plummet nearly to zero[36]. This incident raises critical questions about the nature of the damage incurred by users. While token holders did not technically lose their tokens, they faced substantial financial losses due to the drastic drop in the token's value. The situation complicates the issue of liability: although the promise was that the stablecoin would maintain its peg, determining who is responsible for the resultant loss of trust becomes problematic. The brief period during which the token's value sagged below one dollar triggered a panic among holders, leading to a sell-off that further depressed its price. This sequence of events underscores the challenges in assigning responsibility when algorithmic mechanisms fail to perform as expected, particularly in the absence of traditional, tangible collateral that might otherwise offer recourse to investors.

The complexity in attributing financial damage in the context of cryptocurrency investments often stems from whether the information that guided an investor's decision was misleading or inaccurate. However, in the case of investments in algorithm-regulated tokens, one must question if the information was indeed false[37]. Users invested in a token governed by an algorithm that functions similarly to a classic arbitrage system (buying at $0.99 and selling at $1.01), primarily based on the users' trust in the system. This scenario raises an analogous question: could a gold seller be blamed for a sudden devaluation of gold, a commodity whose value historically rests solely on its status as a safe haven? In both these instances, there isn't a lack of information as might be found concerning the performance of a company or a derivative product. Therefore, the responsibility for financial losses becomes a nuanced issue, revolving not around the accuracy of the information but rather the inherent risks and the nature of the trust placed in the financial instruments themselves.

---

[36] Bana, Anurag, et Ammar Osmanourtashi. « Blockchain and Private International Law: Implications for Crypto, Payment Systems, Digital Wallets and Jurisdictional Concerns » 24, nº 2 (2023).

[37] « Localisation du préjudice financier au lieu du compte bancaire : vers un quasi forum actoris ? | La base Lextenso . https://www.labase-lextenso.fr/gazette-du-palais/GPL333r1.

For stablecoins pegged to assets or fiat currencies, the situation is clearer: if the value of the token falls significantly below that of its underlying asset, causing it to collapse, the institution supposed to have stored the commodity in an amount equal to the number of tokens issued should provide a refund or use the commodity to restore the value of the token. The approaches for determining the location of damage previously mentioned should then be applicable. It could be envisioned that the stablecoin voluntarily places itself under the jurisdiction of a national law, although this is currently not the case for any stablecoin. It seems that the place where the "materialization of damage" occurs could either be where the cryptocurrencies (if we can determine this place) are held or the domicile of the defendant. However, it also appears that the location of the "causative event" could be either the headquarters of the company managing the stablecoin or the facility holding the underlying assets equivalent to the tokens.

III) Proposition for regulation at the European level

The blockchain ecosystem is experiencing a period of rapid growth and institutionalization. This innovative technology, characterized by its immaterial and anonymous nature, presents unique challenges and opportunities. As the adoption of blockchain continues to expand across the European Union, there is an increasing need for harmonized regulation, particularly in the realm of private international law. A unified regulatory approach will ensure a stable and secure environment for blockchain technologies to flourish while protecting the interests of all stakeholders involved. The EU's commitment to regulatory harmonization is essential to support innovation and maintain the integrity of the digital economy. To effectively manage this dynamic and largely intangible technology, European PIL must first recognize and categorically address the legal statuses of various blockchain-based entities such as cryptocurrencies, smart contracts, decentralized autonomous organizations (DAOs), and initial coin offerings (ICOs). Moreover, it is essential to establish a system that enables the harmonized localization of damages. This will facilitate the determination of applicable laws and the competent jurisdiction for resolving disputes. By addressing these critical elements, the PIL framework can provide a solid foundation for blockchain technology to thrive securely and predictably across the EU.

To effectively integrate blockchain technologies within the European Union's regulatory framework, a foundational step involves the classification of cryptocurrencies in private international law. It is essential that European PIL stipulates that all cryptocurrencies with inherent value and traded on platforms—excluding utility tokens—should be recognized as "financial instruments." This classification should align with the definitions provided in established regulations, such as the Rome I Regulation.

Such a designation is crucial not only in member states where cryptocurrencies are already distinctly defined under national laws but also in countries where they are currently assimilated with traditional financial instruments, such as securities. By standardizing the status of cryptocurrencies across the EU, the PIL system will enhance legal clarity and ensure a consistent approach to regulation, thus facilitating smoother transactions and more robust protections within the digital asset space.

As previously discussed, a smart contract is essentially code programmed to execute specific actions. It does not exist in a legal vacuum. [38]A smart contract can facilitate various contractual executions, such as the transfer of money pursuant to an agreement. Furthermore, as observed, it can form the basis of a Decentralized Autonomous Organization (DAO), which may be regulated as a specific legal entity. However, the term "contract" in "smart contract" can be misleading, as it primarily serves as a technical tool rather than a traditional legal contract.

Given this context, European PIL should carefully consider its approach to regulating this informatics object. Smart contracts function primarily as mechanisms to enforce agreements automatically and should not be conflated with the contracts themselves. Therefore, including the term "smart contract" within regulatory texts could inadvertently assign undue legal significance to what is, in essence, a post-contractual technical tool. By refraining from over-regulating smart contracts, the European PIL can avoid unnecessary complexities and focus on creating clear and effective regulations that address the substantive legal entities and actions facilitated by these technologies.

[38] Reyes, Carla L, Nelson M Rosario, Rachel M Cannon, et Richard Tall. « PANEL I: BLOCKCHAIN AND THE LAW », s. d.

When it comes to DAOs, European regulation should adopt a nuanced approach recognizing the unique nature of these entities. Any smart contract that utilizes governance tokens to manage a common liquidity pool or to make decisions through user voting should be considered a legal entity. This recognition is crucial as it reflects the operational reality of DAOs where collective decision-making governs the use of pooled resources. Internally, some EU countries have already recognized DAOs as legal entities, whereas others have not. It is likely that in the absence of specific legislation, national courts would classify DAOs akin to "unregistered partnerships" found in various national laws.
Given these factors, it is imperative that European PIL clarifies that participants in a DAO are not merely independent users but associates within a structured legal entity. This legal clarity would help in establishing responsibilities and rights among members, ensuring that DAOs operate within a framework that acknowledges their collective governance while providing legal protections typically afforded to partners in a business.
By addressing DAOs explicitly within its regulatory framework, the EU can provide a stable environment for these innovative organizational structures to thrive, promoting transparency and accountability while fostering the growth of decentralized business models.

As for ICOs, many member states have already initiated regulatory measures, predominantly through national legislations, although it is often the market authorities that have clarified the practical application of these regulations. This clarification is crucial given the substantial similarities between ICOs and a well-established financial mechanism—the Initial Public Offering (IPO). Like IPOs, ICOs involve raising capital by issuing tokens to investors, a process that closely mirrors the sale of shares to the public in traditional financial markets. Given these parallels, European regulation should mandate that in the absence of specific national legislation or regulations governing ICOs, local courts must treat them in accordance with the existing frameworks established for IPOs.

European PIL should recognize the complexity and multiple potential forums for adjudicating disputes involving cryptocurrencies. When assets are held in a decentralized exchange (DEX), one possible forum for localizing the damage is where the DEX has its place of incorporation, including any subsidiaries located within Europe. Another potential forum is the domicile of the defendant, with the provision that the choice of forum should generally be at the election of the defendant to encourage fairness and jurisdictional appropriateness.

However, in cases involving allegations of scam or abuse of trust—issues previously discussed—there should be flexibility to designate an alternative forum. This could appropriately be the central administration or the place of incorporation of the company managing the blockchain network.

One could argue that the Bitcoin blockchain presents a particular case where typical forums based on place of administration do not apply. Unlike many other blockchain networks, the Bitcoin blockchain operates without a centralized administrative authority and does not have an identifiable entity managing its operations. This characteristic might suggest that this legal frameworks for determining jurisdiction are not applicable.

However, this situation is justifiable for the Bitcoin network due to its limited functionality compared to other blockchains. The primary—and essentially only—function of the Bitcoin blockchain is to facilitate the trading of Bitcoin. It does not support activities such as decentralized finance (DeFi), use of cross-chain bridges, or Initial Coin Offerings (ICOs). These limitations significantly reduce the scope for scams or abuse of trust typical of more complex platforms where multiple types of transactions and contracts are executed.

In instances where a stablecoin deviates from its pegged value, determining the locus of legal recourse becomes crucial. A third forum to the two general one should be added. Typically, a stablecoin is designed to maintain parity with a specific underlying asset or a basket of assets, providing stability unlike more volatile cryptocurrencies. However, should this stability fail—the stablecoin "depeg"—the place of damage could significantly impact legal proceedings.

It is proposed that the legal jurisdiction in cases of stablecoin depegging should primarily be where the company that manages the stablecoin has its central administration. This location typically has the most substantial connection to the operational decisions and governance of the stablecoin. If the central administration is not clearly established or applicable, an alternative jurisdiction could be where the entity responsible for maintaining the collateral is located. This could provide a tangible connection to the financial resources backing the stablecoin.

These specific forums should complement the general jurisdictional options, which include the place where the tokens are held or the domicile of the defendant.

D. Conclusion

In conclusion, the rapid evolution of blockchain technology and the proliferation of cryptocurrencies present both novel opportunities and unique challenges for private international law within the European Union. As this paper has discussed, the decentralized and often intangible nature of blockchain-based assets necessitates a reevaluation and adaptation of existing legal frameworks to address new legal realities effectively.

Firstly, the classification of cryptocurrencies as financial instruments, akin to those defined in regulations such as Rome I, is crucial for establishing a consistent legal foundation across EU member states. This classification provides clarity and stability, ensuring that all parties engage with a mutual understanding of the legal implications of their transactions.

Secondly, the specific nature of smart contracts, while innovative, should not overshadow the fact that they are fundamentally tools for executing predetermined agreements. European PIL must recognize this and avoid attributing undue legal weight to the technology itself, thus preventing unnecessary legal complexity and potential misinterpretation.

Moreover, the legal recognition of DAOs as entities akin to unregistered partnerships and the alignment of ICO regulatory treatments with established IPO frameworks demonstrate a pragmatic approach to integrating new technologies within traditional legal structures. These adaptations ensure that the blockchain ecosystem is supported by a legal environment that promotes both innovation and accountability.

Additionally, the determination of jurisdiction in disputes related to digital assets like stablecoins, especially in scenarios of depegging, highlights the need for legal jurisdictions that reflect the operational and financial realities of these assets. By establishing clear guidelines for jurisdictional determination, PIL can provide effective legal remedies that uphold the principles of justice and equity in the digital age.

Ultimately, the goal of European PIL should be to create a regulatory environment that not only addresses the current landscape but is also agile enough to adapt to future technological developments. By doing so, the European Union will ensure that its legal frameworks continue to protect individuals and businesses while fostering an environment conducive to technological advancement and economic growth.

E. Bibliography

- Audit, Mathias. « Le droit international privé confronté à la blockchain ». *Revue critique de droit international privé* 4, nº 4 (2020): 669-94. https://doi.org/10.3917/rcdip.204.0669.
- Buonanno, Luigi. « La responsabilité civile à l'heure des nouvelles technologies : l'influence de la blockchain », s. d.
- Guillaume, Florence. « Aspects of Private International Law Related to Blockchain Transactions ». In Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law, édité par Daniel Kraus, Thierry Obrist, et Olivier Hari. Edward Elgar Publishing, 2019. https://doi.org/10.4337/9781788115131.00009.
- Kaal, Wulf, Professor at University of Saint Thomas School of Law, Director of the Private Investment Funds Institute, et Minneapolis. « Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses (as of May 2018) ». *Stanford Journal of Blockchain Law & Policy*, 23 juin 2018. https://stanford-jblp.pubpub.org/pub/ico-comparative-reg/release/2.
- Lehmann, Matthias, et Emeric Prévost. « La Localisation Du Dommage Dans Le Web3 ». SSRN Scholarly Paper. Rochester, NY, 2021. https://papers.ssrn.com/abstract=4453652.
- Metjahic, Laila. « DECONSTRUCTING THE DAO: THE NEED FOR LEGAL RECOGNITION AND THE APPLICATION OF SECURITIES LAWS TO DECENTRALIZED ORGANIZATIONS ». *CARDOZO LAW REVIEW* 39 (s. d.).
- Poncibò, Cristina. « Blockchain and Comparative Law ». In *Blockchain, Law and Governance*, édité par Benedetta Cappiello et Gherardo Carullo, 137-56. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-52722-8_10.
- Reyes, Carla L, Nelson M Rosario, Rachel M Cannon, et Richard Tall. « PANEL I: BLOCKCHAIN AND THE LAW », s. d.
- Rühl, Giesela. « Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts? » In Blockchain, Law and Governance, édité par Benedetta Cappiello et Gherardo Carullo, 159-80. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-52722-8_11.
- Patiño, G. Cosío. « Lex Cryptographia Guidelines for Ensuring Due Process in Transnational Blockchain-Based Arbitration: Study on the Kleros Model ».

Transnational Dispute Management (TDM) 19, nº 5 (1 septembre 2022). https://www.transnational.dispute.management.com/article.asp?key=2937.

- Evans, Tonya M. « Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes ». *Wayne Law Review* 65 (2020 2019): 1.
- Guillaume, Florence. « Blockchain: le pont du droit international privé entre l'espace numérique et l'espace physique ». *Le droit international privé dans le labyrinthe des plateformes digitales*, 2018, 163-89.
- Le *smart contract* et le droit des contrats : dans l'univers de la mode – Mélanie Clément-Fontaine – Dalloz IP/IT 2018. 540
- La *blockchain* au prisme du droit international privé, quelques remarques – Fabienne Jault-Seseke – Dalloz IP/IT 2018. 544
- La lutte contre le blanchiment à l'épreuve de la territorialité des crypto-actifs – Julien Goldszlagier – Arnaud Le Teurnier – AJ pénal 2021. 465
- Metjahic, Laila. « DECONSTRUCTING THE DAO: THE NEED FOR LEGAL RECOGNITION AND THE APPLICATION OF SECURITIES LAWS TO DECENTRALIZED ORGANIZATIONS ». *CARDOZO LAW REVIEW* 39 (s. d.).
- Dakroub, Roy, Bernadett Koles, et Helmi Issa. « Crypto consumers' personality traits, and the impact of brand personality on cryptocurrencies' identity ». *Journal of Customer Behaviour* 20 (1 janvier 2022). https://doi.org/10.1362/147539221X16356770010749.
-
- https://sos.wyo.gov/Business/Docs/DAOs_FAQs.pdf
- Sarcuni v. bZx Dao, United States District Court, Southern District of California, Mar 27, 2023 22-cv-618-LAB-DEB |. https://casetext.com/case/sarcuni-v-bzx-dao.
- « Localisation du préjudice financier au lieu du compte bancaire : vers un quasi forum actoris ? | La base Lextenso ». Consulté le 22 avril 2024. https://www.labase-lextenso.fr/gazette-du-palais/GPL333r1.
- « Sartori, C., « Détermination de La Compétence Int... - Strada Lex », 1 janvier 2017. https://www.stradalex.com/fr/sl_rev_utu/toc/rdc_tbh_2017_1-fr/doc/rdc_tbh2017_1p34.
- Skatteverket v David Hedqvist, No. Case C-264/14 (ECJ 22 octobre 2015).
- 82 LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1), 2019-486 § (2019).

- Eidgenössische Finanzmarktaufsicht FINMA. « La FINMA pubblica una guida pratica sulle ICO ». Consulté le 27 avril 2024. https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/.
- FCA. « Initial Coin Offerings », 12 septembre 2017. https://www.fca.org.uk/news/statements/initial-coin-offerings.