Model Framework for Consumer Protection and Crypto-Exchanges Regulation

Aleksandr P. Alekseenko

Laboratory for Analysis and Forecasting of Integration Processes in Modern Eurasia of Institute of Philosophy and Law, Novosibirsk State University, 630090 Novosibirsk, Russia; alekseenko.a.p@gmail.com

Abstract: Cross-border insolvency of crypto-exchanges, cyber-risks, transnational character of activities with cryptocurrencies, and financial frauds on the Internet are among the key threats for individuals who use Bitcoin as an investment. Moreover, crypto-exchanges impose consumer agreements containing provisions limiting their liability for hacker attacks and other clauses promoting inequality in relations with investors. All the named obstacles highlight the vulnerability of unsophisticated individuals investing in digital assets and have pointed out the necessity to adopt an internationally recognized model of rules for crypto-exchanges, otherwise, it will be impossible to effectively protect the rights of investors engaged in the activities of intermediaries exchanging and keeping decentralized cryptocurrencies. The purpose of the study is to elaborate on the fundamentals for constructing an international legal framework protecting consumers from risks arising from the activities of crypto-exchanges dealing with decentralized cryptocurrencies. Based on the methodology of comparative legal study, this paper examines the judicial practice of various countries and the legislation of jurisdictions popular among crypto-exchanges. The research explores the nature of Bitcoin, describes the types of crypto-exchanges and discusses the main approaches to crypto-exchanges regulation. It argues that an international framework on crypto-exchanges should be based on understanding Bitcoin as a commodity which is situated in the place of crypto-exchange incorporation, licensing of crypto-exchanges, and self-regulation.

Keywords: Bitcoin; commodity; consumer protection; cryptocurrency; jurisdictional risks; liability; litigation; scam

1. Introduction

Investments are one of the key factors in the development of every business, but because of the risks of various scams, the financial market sphere is under strict regulation. Attracting investments by traditional means is a complex process with high costs; therefore, businesses are searching for alternative financing. Thanks to the global nature of the Internet and DLT technology, investments in digital assets have become a widespread phenomenon, having the potential to enhance the financial inclusion of start-ups (Jenweeranon 2022). During the last decade, different digital assets such as investment and utility tokens, cryptocurrencies and NFT have become popular among investors. According to Statista.com, in December 2022 capitalization of the global cryptocurrency market reached more than $857.13 billion, revenue from the use of cryptocurrencies amounted to 34.7 billion, with the prospect of doubling and increasing the number of users to 347.73 million by 2027.

Thus, an investor has many opportunities to invest through digital platforms (exchanges) including those established abroad. Meanwhile, the digital tokens industry in 2016–2017 and 2020–2021 was faced with bubbles when extremely highly overpriced digital tokens lost the biggest part of their market value because of heavy selloffs and profit-taking provoked by price manipulation. Additionally, there are many examples when
particular digital asset businesses were involved in scandals: the dubious loans of Lending Club, OnDeck Capital and LendUp, Greensill Capital’s risky debts, Bitstamp’s and Bitfinex’s loss of 19,000 and 119,756 Bitcoins, respectively. In November 2022 one of the world’s largest crypto-exchanges, FTX, collapsed after the misappropriation of client funds in the sum of US$10 billion conducted by its founder. The crash of the exchange was connected with bad corporate governance and the promise to buy its own FTT digital token at a fixed price while FTT itself had no value beyond this. Notably, the FTX collapse affected not only its users, but also the entire industry precipitating an almost 5% decline in a 24 h period, and Bitcoin prices decreasing from $20,000 a coin to $16,500.

Because of the transnational character of digital assets, there is not a generally accepted legal definition of digital assets. Moreover, even commonly adopted minimal requirements to regulate crypto-exchanges are absent. In order to minimize the impact of regulations, crypto-exchanges may choose any place of incorporation, including those which have very poor legislation but operate worldwide. Meanwhile, it is necessary to push FinTech businesses to take into account different obstacles affecting investors, including regulatory risks and data security (Mehrban et al. 2020), otherwise it raises risks concerning investors’ protection from the collapse of crypto-exchanges, various scams, as well as the vulnerabilities of digital platforms’ network systems and web-applications caused by the use of different standards (Alekseenko 2022).

This research aims to elaborate key directions for a legal framework giving guarantees for inexperienced investors involved in activities with decentralized cryptocurrencies. In order to reach this goal, the paper gives an analysis of the legal nature of Bitcoin. The term ‘Bitcoin’ was examined by a number of scholars and experts, from different points of view, but there is not a unified position on how to treat Bitcoin in legal science and practice. Based on the examination of different countries’ legislation as well judicial cases, it is argued that Bitcoin has features of a commodity because it does not have the function of money as it cannot be a payment instrument in routine activities, also Bitcoin is not a security because does not generate obligations for a person issued it.

Given the fact that investing in cryptocurrency is highly risky and individuals do not have a lot of opportunities to control financial intermediaries on the market, this research is focused on the issue of consumer protection against unfair actions by crypto-exchanges, in particular misleading information, and unequal customer agreements. This paper also describes the types of crypto-exchanges and legal approaches of different states to their regulation, provides a brief overview of risks arising from investments via crypto-exchanges, and discusses how to obey the rights of consumers using cryptocurrencies. The results of this research could be useful for elaborating the rules harmonizing public and private interests in the cryptocurrency industry.

This paper is composed of five sections including an Introduction and Conclusion. Section 2 will give a brief overview of the methods. Section 3 shows the nature of Bitcoins, illustrates the types of crypto-exchanges, and describes the main risks for consumers from cryptocurrencies, including scams concerning cryptocurrencies. Section 5 will discuss the legal framework for the protection of the rights of unsophisticated investors involved in the activities of cross-border crypto exchanges.

2. Methods

In order to achieve the main goal of the study, this research uses a number of scientific methods. Critical analysis and doctrinal interpretation provide a deep examination of international conventions, national laws, courts decisions and literature. In order to understand the legal nature of cryptocurrencies and differences in regulation of crypto-exchanges, this paper scrutinizes the Regulations of the European Parliament and of the Council; the Cayman Islands Virtual Asset (Service Providers) Act; Singapore Payment Services Act; Act of the Republic of Korea on Reporting and Using Specified Financial Transaction Information, etc. An analysis of judicial cases of the European Union (Case C-264/14, Skatteverket v. David Hedqvist), Singapore (B2C2 Ltd. v. Quoine Pte Ltd.), United
Kingdom (AA v. Persons Unknown), and the United States (CFTC v. McDonnell and CFTC v. My Big Coin Pay, Inc.) shows that Bitcoin is not money and shall be treated as a commodity.

The method of comparative legal study is applied to find similarities and differences in legislation of jurisdictions popular among crypto-exchanges (Cayman Islands, Republic of Korea, Seychelles and Singapore). The conducted comparative analysis shows how different national regulators treat crypto-exchanges, define their legal status, and impose different requirements concerning their activities. The examination of judicial practice, articles in mass media and literature review provides a demonstration of the main risks arising from crypto-exchange activities such as investment platform transnational insolvency, fraudulent practices in the FinTech industry, poor cyber security, and consumer agreements designed in favor of crypto-exchanges.

Based on an understanding of the different types of crypto-exchanges, this paper argues that it is important to elaborate on a legal framework giving guarantees for inexperienced investors for cross-border investment activities involving digital assets. Notably, there is a need to introduce legal treatment for investment platforms. Internationally adopted regulations could prevent crypto-exchange malpractice and increase the level of consumer protection. Fraud and misuse of customer funds, dubious corporate decisions, ambiguous customer agreements, hacker attacks on digital platforms, and the collapse and bankruptcy of transnational crypto-exchanges underline the necessity to establish minimum standards for the industry.

The method of legal modeling will allow us to demonstrate the possible directions in the construction of a consumer-friendly legal framework and propose particular steps in developing legal regulation of crypto-exchanges’ activities.

3. Findings

3.1. Nature of Crypto-Assets

The research is based on the idea of a wide diversity of cryptocurrencies (Gimigliano 2022) and the idea that some of them do not have a function as a payment method (Maume and Fromberger 2019). There are various opinions about what crypto-assets include, but it is clear that at least three types could be identified: asset-referenced tokens including utility and investment tokens, cryptocurrencies (decentralized payment tokens), digital currencies of central banks, and other crypto-assets with controversial nature. Consequently, crypto-assets do not and cannot have common rules of circulation. A crypto-asset is just a generalizing category for different digital objects.

Analysis of how investment tokens function shows that they may be treated as securities or transferable securities (see Article 4(1)(44) MiFiD2), while utility tokens are derivatives, similar to options which are traded on specialized platforms and give the right to receive goods, intellectual property rights or services. Gimigliano (2022) notes that “payment tokens may serve only as a means of exchange and unit of account; utility tokens allow holders to access or to purchase services provided or products sold and asset tokens are to some extent comparable to equities, bonds, or participatory financial instruments”. So, investment tokens (asset tokens) and utility tokens do not have a function that allows them to be used as a means of payment. In fact, some payment tokens (cryptocurrencies) are also not currencies. Scholars assert that “if a currency token combines payment functions with investment aspects that are not based only on rising rates or prices, it would not be classified as currency but an investment token. As a result, it would not be a payment instrument.” (Maume and Fromberger 2019). Therefore, payment tokens to be counted as such, shall have their main or only function as a means of payment, only in this case they are not deemed as transferable securities.

Despite the fact that digital currencies are not a new term anymore, existing legislation hardly describes and poorly regulates digital currencies such as Bitcoin and Ethereum (Plevri 2021). Legislators have made attempts to determine the legal nature of Bitcoin and
Ethereum. For example, in Italy, Singapore and Mexico, cryptocurrency is considered as a digital representation of value used as a means of exchange for the purchase of goods and services. Implementation of this approach helps to establish a framework for cryptocurrency transactions based on the legal rules for foreign currencies and urges international cooperation on the issue (Alekseenko and Gidigbi 2021). Of course, decentralized cryptocurrencies could play a role in measuring the value of transactions, but they are not legal tender, and therefore, do not have the function of money (Ammous 2018). Additionally, the absence of an issuer does not even allow considering crypto-currencies as a monetary surrogate. High volatility results in Bitcoin and Ethereum being rarely used as payment instruments in routine activities. Individuals purchase these cryptocurrencies mainly for the purpose of speculation and resale when their exchange rate will increase (Haykir and Yagli 2022). However, this feature does not exclude the possibility of trading cryptocurrency for goods and services.

Decentralized cryptocurrencies store value and could be used for settlements among groups of individuals. Simultaneously, they have the features of speculative assets with the price backed only by the trust of investors, but they are not securities or bonds. Common ground is that payment tokens are negotiable if they contain an unconditional promise or order to pay a sum of money and confer on the issuers or a redemption right on the reserve assets backing the value of the payment tokens (Gigliano 2022). Bitcoin and Ethereum are created on the basis of cryptography and do not generate obligations for the person to whom they are issued; furthermore, an obliged person is unknown and cannot be identified. The former owner of the cryptocurrency is not responsible to the new owner and does not guarantee that Bitcoin will be freely exchanged for money or goods. Hence, according to formal signs, cryptocurrency cannot be classified as securities. In Skatteverket v. Hedqvist, the Court of Justice of the European Union stresses that Bitcoin is neither a security conferring a property right nor a security of a comparable nature.

Bitcoin, Ethereum, etc., may not be treated as money or as securities, but they store value for their users which makes them similar to goods. In 2019 Sir Geoffrey Vos (2019), Chancellor of the High Court of Justice of England and Wales points out that there are not any barriers to classifying cryptocurrencies as property. British High Court Judge Bryan in AA v Persons Unknown stated that Bitcoin meets the criteria of property as it is definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence. The same position was taken by the Singapore International Commercial Court, which noted that “cryptocurrencies are not legal tender in the sense of being a regulated currency issued by a government but do have the fundamental characteristic of intangible property as being an identifiable thing of value.” The United States District Court for the Eastern District of New York indicated cryptocurrencies are more concrete and proclaimed them goods since they fall well within the common definition of commodity as all other goods and articles in which contracts for future delivery are presently or in the future dealt in.

Recognizing Bitcoin as property raises the question of applicable law because it exists only in digital form and is based on distributed ledger technologies. This issue is especially topical in connection with the cross-border activities of cryptocurrency exchanges. Malvagna and Sartori determine the location of cryptocurrencies as the place where private keys associated with a certain token are stored (Malvagna and Sartori 2022). In order to store these keys customers may exploit two types of digital wallets. The first one is hardware wallets guarded by a user, it could be USB-flash, hard disk, etc. The second one is a custodial wallet where a custodian, such as a crypto-exchange, stores the depositors’ private keys. Hardware wallets are movable devices and only their owner knows where they are situated. Custodians may use different servers all around the world to store customers’ private keys. Notably, scholars stress that “if the custodian’s activity is limited to storing depositors’ private keys without transferring deposited cryptos to its own blockchain address, it is argued that, as far as the deposit contract is concerned,
cryptocurrencies should be treated as non-fungible assets, provided that it is always possible to trace to which client any act of disposal relates” (Malvagna and Sartori 2022).

Therefore, the task of finding the location of cryptocurrencies and choosing applicable law is complicated even if the cryptocurrency would be treated as property, because “the qualification of the contractual and property law rights of crypto-investors is problematic” (Kokorin et al. 2020). The legal nature of Bitcoin is not completely clear, but it could be treated as property. However, this approach does not reveal uncertainty concerning the law applicable to cryptocurrency turnover. Crypto-exchanges are the cornerstone of the crypto-assets industry, and there are not any reasons not to regulate their activities, otherwise, there is a risk for individuals to lose their savings without legal protection. Hence, it is necessary to pay close attention to the elaboration of rules for interaction between crypto-exchanges and customers. This legal framework shall be based on the concept that crypto-exchanges store and trade different crypto-assets. Therefore, for activities involving commodities such as decentralized cryptocurrencies, it is needed to introduce special rules.

3.2. Crypto-Exchanges

Crypto-exchanges are Internet platforms providing customers with facilities for selling and purchasing digital assets or exchanging them for other assets. They also provide services similar to traditional financial exchanges which charge fees and take the bid-ask spread as a commission on a transaction (Scharfman 2023). According to Forbes, in 2022 there were nearly 600 cryptocurrency exchanges worldwide (Paz 2022) with a total of 24 h trading volume of $52.9 Billion, other sources name about 800 crypto-exchanges. Operators of the top ten largest cryptocurrency exchanges in terms of turnover are located in various jurisdictions, including offshore ones (Table 1); therefore, it is important to promote international cooperation between countries and find common points of contact allowing the effective regulation of trading and safekeeping of decentralized cryptocurrencies.

<table>
<thead>
<tr>
<th>No.</th>
<th>Crypto-Exchange</th>
<th>24 h Trade Volume, Billion U.S. Dollars</th>
<th>Place of Incorporation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Binance</td>
<td>16.91</td>
<td>Cayman Islands</td>
</tr>
<tr>
<td>2.</td>
<td>Deepcoin</td>
<td>5.52</td>
<td>Singapore</td>
</tr>
<tr>
<td>3.</td>
<td>Hotcoin Global</td>
<td>5.38</td>
<td>Australia</td>
</tr>
<tr>
<td>4.</td>
<td>ECXX</td>
<td>4.79</td>
<td>Singapore</td>
</tr>
<tr>
<td>5.</td>
<td>BiONE</td>
<td>4.6</td>
<td>Singapore</td>
</tr>
<tr>
<td>6.</td>
<td>CITEX</td>
<td>2.88</td>
<td>Republic of Korea</td>
</tr>
<tr>
<td>7.</td>
<td>Upbit</td>
<td>2.79</td>
<td>Republic of Korea</td>
</tr>
<tr>
<td>8.</td>
<td>XT.COM</td>
<td>2.34</td>
<td>Seychelles</td>
</tr>
<tr>
<td>9.</td>
<td>IndoEx</td>
<td>2.16</td>
<td>Great Britain</td>
</tr>
<tr>
<td>10.</td>
<td>MEXC</td>
<td>2.08</td>
<td>Seychelles</td>
</tr>
</tbody>
</table>

There are two types of crypto-exchanges: centralized and decentralized. According to Scharfman centralized crypto exchanges are intermediaries between buyers and sellers of digital assets which usually serve as custodians for digital wallets (Scharfman 2023). Decentralized exchanges (DEX) are networks where traders can directly trade cryptocurrency for other tokens without a third party and custodian. The DEX model of crypto-exchanges is becoming popular among users, but it does not provide for the exchange of fiat money for cryptocurrencies and is also acutely lacking a regulatory framework (Kaal 2020). While DEXs just provide an infrastructure for trade, centralized crypto-exchanges act as active players in the cryptocurrencies market and they may even organize an initial exchange offering (IEO) when the issuer of digital assets issues its tokens after
examination by the exchange and sells them through the exchange that listed the token offering (Kaal 2020). Additionally, centralized crypto exchanges have an agency relationship with their users as custodians of private keys (Malvagna and Sartori 2022). These obstacles raise the question of the ability of intermediaries to provide their clients with an adequate level of trust and protection. So, lawmakers should clearly distinguish between centralized crypto-exchanges and DEX.

Despite the transnational character of crypto-exchange activities, there are not any internationally recognized or supranational minimal standards for the regulation of their transactions. Nevertheless, the EU created the European Blockchain Observatory and Forum, and the European Blockchain Partnership which unites all Member States at a political level (Jasperse and Hammer 2022). The European Union also established a unified framework for state-members concerning the prevention of risks arising from cryptocurrencies, information disclosure by crypto-exchanges, combating money laundering and the financing of terrorism (AML/CFT) requirements for cryptocurrency trading. These rules were published in October 2022 in the Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive 2019/1937 (MiCA 2022).

MiCA 2022 obliges crypto-asset service providers (i.e., crypto-exchanges) to comply with prudential requirements, employ management and staff with adequate skills, knowledge and expertise, and establish sound internal control and risk assessment mechanisms as well as adequate systems and procedures to ensure integrity and confidentiality of information received, keep records of all transactions, orders and services related to crypto-assets that they provide, members of the board of directors and shareholders of crypto-exchanges should be of good repute and be fit and proper, including for the purpose of anti-money laundering and combatting the financing of terrorism. Additionally, MiCA 2022 ensures the consumer from dishonest practices. Art. 55 of the MICA 2022 reads as follows:

“In order to ensure consumer protection, market integrity and financial stability, crypto-asset service providers should always act honestly, fairly and professionally in the best interest of their clients. Crypto-asset services should be considered ‘financial services’ as defined in Directive 2002/65/EC13 of the European Parliament and of the Council, in case the criteria of that Directive are met. Where marketed at a distance, the contracts between crypto-asset service providers and consumers should be subject to that Directive as well, unless this Regulation expressly states otherwise. Crypto-asset service providers should provide their clients with clear, fair and not misleading information and warn them about the risks associated with crypto-assets. Crypto-asset service providers should make their pricing policies public, should establish a complaint handling procedure and should have a robust policy to identify, prevent, manage and disclose conflicts of interest”.

However, scholars criticize how MiCA 2022 deals with the turnover of different digital tokens and underlines the lack of rules for obtaining a license (Gimigliano 2022). No less important lacuna is the insufficient regulation of cooperation with non-EU countries in questions of consumer protection. Moreover, MiCA 2022 stays silent on how to determine the applicable law in case of bankruptcy and storage of private keys.

It is noted that many economies still lack well-designed supervisory technology and financial supervision for crypto-exchanges (Sancak 2023), including jurisdictions popular among participants of this industry. Despite cryptocurrency exchanges falling under the definition of a reporting financial institution, some states such as the Republic of Seychelles do not introduce any regulation for them. As Randolph Samson, Director at the Anti-Money Laundering and Terrorist Financing Department of the Seychelles Financial Services Authority noted, many of the cryptocurrency platforms receive the status of an international business company due to the lack of regulation, and in fact, their activities are carried out outside the jurisdiction of the state (Betymie 2021). It makes this country an attractive place for crypto-exchanges (2 of the 10 largest exchanges are registered in the
Seychelles). Meanwhile, after the case of the theft of 230,000 Bitcoins from users by a cryptocurrency exchange registered in this state, tensions with the US rose after this event (De Koker et al. 2022); the country’s financial authorities announced their intention to regulate the activities of virtual asset service providers. This move will help meet the standards of the Financial Action Task Force on Money Laundering (FATF) (Nicette 2022).

Unlike the Republic of Seychelles, another offshore jurisdiction—the British Cayman Islands—where the largest crypto-exchange Binance is registered, has detailed legislation on digital assets. In 2020 it adopted the Virtual Asset (Service Providers) Act which introduced the legal framework for operators of digital asset platforms, including DEX21. Moreover, the Cayman Islands amended a number of other laws: Monetary Authority Bill; Securities Investment Business Bill; Mutual Funds Bill; Stock Exchange Company Bill. Amendments allowed the Cayman Islands Monetary Authority to supervise virtual assets exchanges, and to apply key requirements to them regarding AML/CFT. These measures aimed firstly to prevent inclusion in the blacklist of the FATF and foreign national regulators.

The Virtual Asset (Service Providers) Act obliges all organizations carrying out transactions with digital assets or claiming to do so to obtain a license. There are different requirements for crypto-exchanges. In Art. 9, the Act establishes the general requirements for virtual asset service providers: auditor’s supervision of corporate governance, anti-money laundering system, qualification of the exchange’s senior officers, protection of personal data and virtual assets of its clients, registration of the office in the Islands, etc. Art. 10 of the Virtual Asset (Service Providers) Act contains the requirements of virtual asset custody services, including safekeeping, segregation and insurance of client assets, as well as cybersecurity measures. Art. 11 of the Act established requirements for virtual asset trading platforms aimed at preventing price manipulation and other unfair trading practices. Notably, the Virtual Asset (Service Providers) Act does not contain a non-closed list of requirements for a licensee, meaning that the Monetary Authority has the right to settle additional requirements for an applicant. According to Article 35(1) of the Virtual Asset (Service Providers) Act, a person who carries on, or purports to carry on, a virtual asset service in or from within the Islands for which registration is required who is not a registered person or the holder of a waiver under this Act, has committed an offense and is liable on summary conviction to a fine of twenty-five thousand dollars and to imprisonment for one year.

Singapore is another popular place of incorporation for crypto-exchanges where special legislation has been adopted, issuing regulatory warnings and strengthening enforcement actions to mitigate the risks of new technological applications (Lin 2019). The Singapore Payment Services Act20 in art. 6(4) established that cryptocurrency may be exchanged, traded and stored only by a licensed payment services provider having one of these types of license: money-changing license, standard payment institution license, and major payment institution license. According to Art. 6(9) of the Act, in order to obtain a standard license, a cryptocurrency exchange must have a registered office in the country, the acting manager of the organization must be a citizen or permanent resident of Singapore with the right to work, and the minimum authorized capital must be 100,000 Singapore dollars. The Payment Services Regulations21 issued by the Monetary Authority of Singapore (MAS) set up the rules for the application procedure, as well as the requirements for information disclosure, while Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, Digital Payment Token Service22 and Guidelines to Notice PSN02 23 established the requirements of crypto-exchanges concerning AML/CFT.

Thus, Singapore focuses on the identification of cryptocurrency holders and the prevention of criminal risks arising from the trade of cryptocurrencies. This approach is beneficial for individuals using Bitcoin and Ethereum as an object for investments because it allows protection of their investments from unfair crypto-exchanges (Alekseenko 2022a). Meanwhile, in cases of bankruptcy, it seems that the registered office of a crypto-exchange
will not be able to compensate consumers. Additionally, the Singapore Payment Services Act and the MAS’s regulations say nothing concerning the specifics of custodial services.

The Republic of Korea is also attractive for crypto-exchanges. This state does not have special laws concerning crypto-exchanges, but in 2020 it amended the Act on Reporting and Using Specified Financial Transaction Information which equalized virtual asset service providers, i.e., persons engaged in the sale, purchase, exchange, and storage of virtual assets for financial organizations. It means that crypto-exchanges are obliged to obtain a license from the Financial Services Commission and AML/CFT. Thus, the Republic of Korea has banned the use of anonymous accounts when trading cryptocurrencies. Transactions with digital currencies are possible only if a client has a verified bank account for sending money to a digital wallet. A violator of license requirements, under section 7(1) of the Act, is punishable by imprisonment with correctional labor for up to five years or a fine not exceeding 50 million won.

Thus, it is apparent that the principles of supervising crypto-exchanges are not unified (Table 2). States have disparate approaches on how to regulate cryptocurrency trading, non-identical levels of cyber security, and different requirements towards the quality of minimal corporate governance of digital services providers. So, depending on the place of incorporation there are different standards for crypto-exchanges. The common ground is that countries are aiming to minimize undermining behavior of crypto-exchanges dealing with decentralized cryptocurrencies on the country’s sovereignty and regimes by obliging them to comply with AML/CFT. Some regulators have established rules decreasing information asymmetry between consumers and digital platforms, as well as introducing measures to increase the cybersecurity of intermediaries. It will help to overcome vulnerabilities of the digital platforms’ networks and make consumers aware of scams.

<table>
<thead>
<tr>
<th>No.</th>
<th>Jurisdiction</th>
<th>Law</th>
<th>Status of Crypto-Exchanges</th>
<th>Verified Users</th>
<th>Types of Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cayman Islands</td>
<td>Virtual Asset (Service Providers) Act</td>
<td>Virtual asset custody services; Virtual asset trading platforms</td>
<td>Yes</td>
<td>Virtual asset service licence; Sandbox licensee</td>
</tr>
<tr>
<td>2</td>
<td>Republic of Korea</td>
<td>Act on Reporting and Using Specified Financial Transaction Information</td>
<td>Financial organizations</td>
<td>Yes</td>
<td>Financial organization License</td>
</tr>
<tr>
<td>3</td>
<td>Seychelles</td>
<td>No</td>
<td>Unregulated</td>
<td>Unregulated</td>
<td>Unregulated</td>
</tr>
<tr>
<td>4</td>
<td>Singapore</td>
<td>Singapore Payment Services Act; Regulations and Guidelines of MAS</td>
<td>Payment services provider</td>
<td>Yes</td>
<td>Money-changing license; Standard payment institution license; Major payment institution license</td>
</tr>
</tbody>
</table>

Meanwhile, in shaping their regulatory frameworks, some countries do not take into consideration that it is necessary to introduce special rules for service providers dealing with decentralized cryptocurrencies. It is preferable if regulators were to target crypto-exchanges and other intermediaries that provide services related to Bitcoin and other decentralized cryptocurrencies (Kibwage 2021). Otherwise, an asymmetry of regulations will arise which, in turn, would provoke regulatory arbitrage and create uncertainty regarding the definition of competent jurisdiction and the applicable law when crypto-exchanges operate internationally (Broby and Quimbayo 2021). It is important not only to support public order by enforcing AML/CFT tools but also to introduce standards for protecting the rights of investors.
3.3. Risks for Consumers

Because of Bitcoin’s digital nature and difficulties with regulation, crypto-investors are vulnerable to different risks. Scharfman demonstrates that typical threats include wallet hacks, ransomware frauds, celebrity and corporate impersonation, social media hijacking, goodwill airdrop fraud, romance scams, pig butchering, and giveaway/multiplier scams (Scharfman 2023). Unsophisticated investors are targeted by unfair crypto-exchanges which breach their contracts26, use Ponzi schemes, trade fake cryptocurrencies, or just steal clients’ money. Usually, scammers attract investors by promising them high gains from playing on the cryptocurrency exchange rates, and new investment strategies (Bele 2020).

Unregulated advertisement through social media and the absence in some countries of regulatory rules impede the process of different crypto-exchanges and other intermediaries from promoting themselves, including illegal ones (Liebau and Schueffel 2019). For example, pseudo exchange BitKRX disguised itself as a legitimate trading platform; however, when customers tried to access their funds, they found that their money was gone and they never bought Bitcoins via this intermediate. One more pseudo exchange BKEX just copied the trading history of Binance to demonstrate its activities and attract money, and after receiving some funds, the scammers just closed the platform.

Some scammers promote fake cryptocurrencies such as “My Big Coins”27 and One-Coin28 which are not cryptocurrencies and are not transferable. This type of scam is easy to detect by analyzing leading registered crypto-exchanges or websites of the crypto-community. It is rightly noted that “if you cannot find a certain currency listed on the biggest exchanges, it is a good sign that you should be extremely careful” (Bele 2020). Meanwhile, the lack of individuals knowledge concerning digital assets makes possible the existence of counterfeit intermediaries trading with fake cryptocurrencies.

Numerous naive customers in pursuit of profit accept invite links that are applied to involve individuals in financial pyramids, in particular, “Ponzi” schemes (Nizzoli et al. 2020). A Ponzi scheme is a kind of sophisticated financial pyramid where a scammer generates profits and pays rewards collected from funds of those who joined the scheme later. A Ponzi scheme works until the time when it becomes impossible to attract new investors or when individuals decide to withdraw all their savings. Involvement in Ponzi schemes is a typical assertion in lawsuits brought by individuals or public bodies against various intermediaries in the sphere of digital finances. In many cases, these claims occurred alongside parallel allegations of money laundering, fraud, and conspiracy (Yahya and Pecharsky 2022). For example, in 2016, the New York Bitcoin Savings and Trust cryptocurrency exchange fraudulently received about 146,000 Bitcoins from investors. Its founders guaranteed weekly gains at the rate of 7%, which they made from receiving new investments while spending funds on their own personal needs.29

The United Nations has guidelines for consumer protection establishing that financial services providers should have a written policy on conflict of interest to help detect potential conflicts of interest,30 but not all crypto-exchanges follow this recommendation and exercise effective corporate governance. Investors may be misled by the commercial practice of digital services providers (Mauduit 2022) or by fraudulent statements and practices when an intermediary assures a client that the price of tokens would stay at a certain level but after the deal unilaterally changes the token’s price (Yahya and Pecharsky 2022).

Crypto-exchanges may use ineffective audit systems, raise debts and not share this information with clients. It is noted that crypto suits are often connected with tort actions, such as negligent misrepresentation and fraud (Ghodoosi 2022). For example, the FTX crash in 2022 demonstrates that one of the world’s largest crypto-exchanges failed to exercise corporate control, keep proper books, records or security controls for the digital assets it held for customers, used software to conceal the misuse of customer funds, used an unsecured group email account, and paid the debts of Alameda hedge fund closely related to FTX’s CEO (Shubber et al. 2022). Finally, because of poor investment strategies, crypto-exchanges may lose their funds as well as clients’ money and become insolvent.
The insolvency of crypto-exchanges underlines a question of compensation for investors, especially when a platform’s operator is domiciled abroad. Therefore, risks exist even if there is not any misleading behavior from the side of a crypto-exchange because typically customers are not able to evaluate the financial situation of a crypto-exchange.

Moreover, problems with leading participants in the market could affect the other players and lead to sound difficulties in the industry. The collapse of a token named Luna provoked a cascade of crypto hedge funds, brokers and exchanges towards insolvency comparable to the downfall of Lehman Brothers (Ghodoosi 2022). It underlines the necessity to introduce preventive measures for the industry, including the implementation of an internationally recognized sound system of control and audit. Of course, this would not protect customers from intermediaries’ bankruptcy, but it would raise the stability of the industry.

The lack of information about the nature of cryptocurrencies intensifies the risks connected with price manipulation. Bitcoin is characterized by a high level of volatility, as it is one of the most attractive assets for financial speculation (Nizzoli et al. 2020). Price manipulations on crypto-exchanges are based on the pump-and-dump scheme where market participants collude to coordinate the sale and purchase of a particular cryptocurrency and affect the Bitcoin exchange rate. Kamps and Kleinberg make the suggestion that price manipulations are less likely if a crypto-exchange is licensed and situated in a jurisdiction with a sound system of control (Kamps and Kleinberg 2018). Price manipulations are difficult to eliminate in financial markets, but it is possible to introduce a clear system of monitoring scammer groups, decreasing the frequency of pump-and-dumps, which would be on behalf of regulators, investors and recognized crypto-exchanges. It is noted that the expected crackdown by US securities regulators on crypto intermediaries and potential shakeups in insider trading cases are among the topical issues for the year 2023 (Bultman 2022). As it is rightly stated “trading cryptocurrencies comes with a big risk. We pay real money for cryptocurrencies without ever knowing if our investment will be fungible in the future, i.e., if we will be able to trade it back for money or other goods” (Bele 2020).

Crypto-exchanges and custodians are among the popular targets for cyber attacks and hacking in order to steal Bitcoins from clients’ digital wallets. According to Bloomberg in 2017–2022, American customers brought at least 50 individual lawsuits and proposed class actions against intermediaries unable to protect clients’ crypto-assets from hackers and claimed losses ranging from as low as $4,600 to as high as $55 million (Witley 2023). Problems with cybersecurity are common in the industry. In November 2022, FTX and FTX. US crypto-exchanges reported that more than $400 million was drained from wallets. So, owners of Bitcoins and other cryptocurrencies need confidence in ensuring the security of digital wallets, the ability of the crypto-exchange to minimize cyber risks, and protection against cyber threats. Despite the fact that digital services providers use different protection measures such as encryption with symmetric and asymmetric algorithms, and attribute-based access control so that ‘only trustable parties are allowed to either partially or fully decrypt their data (Mehrban et al. 2020), cyber-risks still exist.

In order to evade losses, crypto-exchanges push their users into accepting customer agreements where they disclaim the platform’s responsibility for any cyber risks. For example, according to the Binance Terms of Use, the user acknowledges that he is aware of the risks associated with transactions with digital currencies, agrees to assume all risks and that Binance is not liable for any risks or adverse results. Moreover, Binance’s General Risk Warning informs that it is not possible for Binance to eliminate all security risks and users are responsible for keeping their Account password safe and that customers may be responsible for all the transactions under their Binance Account, whether they authorized them or not. The crypto-exchange highlights that transactions in Digital Assets may be irreversible, and losses due to fraudulent or unauthorized transactions may not be recoverable.
Thus, crypto-exchanges decline to guarantee the safety of customer assets as well as compensation in case of losses. In fact, digital platforms use their powers to make individuals responsible for the protection of data stored on the network infrastructure, and customers shall bear any losses because of the wrong tools and/or methods of cybersecurity applied by the crypto-exchanges. This situation in conjunction with an increasing number of cyber attacks makes investors extremely vulnerable. If digital platforms do not ensure information security and data privacy, they must not shift responsibility to individuals but instead should find a way to secure their clients’ money.

The issue of applicable law in the lawsuit is highly topical for courts, governments and investors, but the unclear status of transnational crypto-exchanges and the controversial nature of Bitcoins bring difficulties in understanding how to compensate investor losses. Meanwhile, cryptocurrency-related litigation arising from traditional private law claims and consumer protection statutes is on the rise (Ghodoosi 2022). Therefore, it is more than necessary to provide individuals with instruments to eliminate jurisdictional risks which prevent their access to justice.

Scholars note that “the presence of defendants abroad, despite their use of local banks, may serve as jurisdictional obstacles for having a case heard in the first place” (Yahya and Pecharsky 2022). In Reynolds v. Binance Holdings Ltd., the court dismissed a claim to the crypto-exchange for lack of personal jurisdiction, motivating that the plaintiff failed to show any connection with the defendant to the place where the court and claimant are situated.34 In the FTX case, the U.S.-based bankruptcy team and Securities Commission of the Bahamas disputed the seizure of $426 million from FTX by the Bahamas (Shubber et al. 2022), while FTX customers filed a class action lawsuit against the platform and its former top managers (Hals and Knauth 2022). Therefore, in cases of transnational insolvency of crypto-exchanges, consumers have less opportunity to find judicial protection and claim compensation.

Jurisdictional risks are also connected with arbitration clauses included in the consumer-digital platform agreement. For example, users of the Binance crypto-exchange are bound by the terms of the User Agreement on Dispute Resolution, which prescribes to resolve all disputes exclusively in the Hong Kong International Arbitration Center (HKIAC) in accordance with Hong Kong law, as well as prohibits filing class action lawsuits35. Moreover, Hong Kong does not have special regulations concerning crypto-exchanges providing transactions involving Bitcoins. So, these contractual clauses limit the possibility for an unsophisticated investor to bring a suit under arbitration on their own, as it is extremely burdensome and further complicated by the high cost of arbitration fees collected by HKIAC. De facto, Binance uses its power to set favorable conditions for its own activities to the detriment of private investors.

4. Discussion

As transactions with cryptocurrencies have a transnational nature, regulators are able to adjust these activities only if they would cooperate and harmonize basic rules concerning the crypto-exchanges, including data security (Morton 2020) and pivotal definition (Maume and Fromberger 2019). Otherwise, the lack of regulation for intermediaries, including those that provide Bitcoins storage services, will fuel regulatory arbitrage and poorly affect consumer safety (Kibwage 2021). Therefore, it is much more preferable if international institutions adopt model laws, guidelines or elaborate international agreements where they respond to the issues concerning the protection of customers who trusted their funds to crypto-exchanges. It should not contain rules that bring the legal framework into line with a particular state’s practice, as has been proposed (Maume and Fromberger 2019), but it could construct pillars for effective interaction.

Based on understanding the nature of decentralized cryptocurrencies, the types of crypto-exchanges as well risks from their activities, it is possible to introduce a legal framework for centralized crypto-exchanges which corresponds with the UNCTAD regulatory principles for consumer protection in digital financial services (Mauree 2016). This
regulatory framework will not be suitable for the activities of decentralized cryptocurrency exchanges which do not provide services for storing private keys or exchanging money for cryptocurrency. However, it does not mean that this sphere should be left out of the key principles for digital financial services as proclaimed by the UNCTAD (mechanisms for dispute resolution, fraud prevention, information disclosure and transparency, data, privacy funds and protection).

First of all, it is necessary to define Bitcoin as a property or commodity owned by a customer. This step will help to decide the bulk of issues, in particular, the well overdue difficulties connected with crypto-exchange bankruptcy cases when regulators raise the question of whether or not they should separate client Bitcoins from the assets of a custodian (Malvagna and Sartori 2022). In this case, consumers will be protected from the situation when all assets under the management of a crypto-exchange are counted as its funds and liquidated during insolvency. Understanding Bitcoin as a commodity gives investors an opportunity to claim their cryptocurrencies from a custodian and reduces the number of grantees losing their funds. So, regulators are recommended to recognize Bitcoin as a commodity because it is not in the interest of a state’s customers’ well-being if it would be treated the same way as money.

Presently it is uncertain how judges will conduct themselves with claims from the use of Bitcoins in transnational operations. If Bitcoin were to be recognized as a tradable commodity, it would make it clearer how to choose the applicable law, otherwise, it is extremely hard to apply international private law principles to find the right jurisdiction and overcome a conflict of laws. Recognizing the proprietary nature of Bitcoin, it is necessary to find a site where the commodity is situated. As was previously noted, such a place could be a crypto-exchange or a custodian registration. In Great Britain, an algorithm was presented on how to qualify if the court has jurisdiction over litigation in dealing with cryptoassets. It includes the following steps: determine where and by whom a centralized control over cryptocurrency is excised; reveal a place where a private key is stored and find if parties choose a law applicable to the relevant transfer (Akka et al. 2019). The site of a private key keeper is a key point in deciding where Bitcoins are. Therefore, it will be much more preferable if states and international bodies who are shaping legislation on cryptoassets indicate the site of custodian incorporation as the place where Bitcoins are situated.

Addressing the issue of scams, it is necessary to settle on an effective system of control over the crypto-exchanges. Regulators should focus on areas of vulnerability, such as wallets, exchanges, and the financial institution’s exposure (Bains et al. 2022). Licensing could be a good method to mitigate the number of scams in the industry. Of course, there are no, and cannot be, unified requirements to licensing, but regulators could agree to oblige crypto-exchanges to have minimum authorized capital, conduct independent audits of its funds, provide insurance for client funds, and implement other standards similar to financial companies. Of course, there should be additional requirements for licensing concerning the exchange of cryptocurrency for money. In this regard, central banks should adopt a model that will spread the rules for customer authentication, anti-money laundering, etc., on operations with Bitcoins. These rules will help law enforcement bodies react more promptly to the use of cryptocurrencies for tax evasion, money laundering, illegal trade, and financing of terrorism (Saiedi et al. 2021).

In order to decrease the level of price manipulations, it will be highly preferable to implement a model similar to FOREX markets within crypto-exchanges. Regulators may encourage crypto-exchanges to prevent insider trading, establish a maximum limit price on cryptocurrencies, and introduce mechanisms regulating a maximum quantity of orders from an investor per day, and the maximum amount of cryptocurrency for sale or purchase issued by one order (Fratrič et al. 2022). This model will work if only crypto-exchanges implement the ‘Know your customer’ system, exclude information asymmetry and develop sound standards of trading in cryptocurrencies.
As the European Parliament noticed, the limited capacity of regulators in areas of new technology may make it difficult to define appropriate safeguards in a timely manner in order to ensure the proper and reliable functioning of DLT applications when or even before they grow so large as to become systemically relevant. Thus, it is critical to develop self-regulation in the industry because regulators are not able to react in time to rapid changes in digital business. Based on the experience of stock trading, it is also important to force crypto-exchanges to elaborate rules of trade on Bitcoins for money and their exchange for other cryptoassets (cryptocurrencies, investment tokens, NFTs). Additionally, as part of self-regulation and self-control, crypto-exchanges could develop a system to detect and prevent financial bubbles.

It is crucial to make customers aware of fraud in the sphere of FinTech as well as the risks connected with trade in Bitcoins, including price manipulations. Therefore, regulators should oblige crypto-exchanges willing to obtain a license to provide customers with clear information about investor rights and obligations in using their products, the method, costs, and any other consequences of selecting and changing particular investment portfolios or strategies (Chien et al. 2017). It could be more effective if intermediaries would teach consumers financial literacy in the frames of self-regulation and before granting them access to financial services (Malady 2016). Further, it is important to encourage and apply the balancing of innovation with international standards of accountability and investor protection for the cybersecurity of crypto-exchanges. Of course, different websites and web-applications use different mechanisms; therefore, it is impossible to implement a technical standard applicable to all custodians and crypto-exchanges, but regulators could highlight that it is compulsory for market participants to test their software for resistance to errors, hacker attacks, fraud or ill intent (Demertzis and Wolff 2018). Ultimately, regulators already have standards for digital banking and trading. There are not any reasons why these rules cannot also be applicable to crypto-exchanges.

As previously noted, intermediaries diminish their liability by contractual clauses. Meanwhile, crypto-exchanges must be responsible to consumers for the safety of funds and be liable for losses, as they collect fees from users. Otherwise, it could be counted as poor execution of duties and breach of contract. Additionally, it is unjust when custodians do not guarantee the safety of customer assets from fraud and cyber hacks. Based on the doctrine of secondary liability, some scholars propose to develop provisions for a special type of liability for digital platform operators (Kozhemyakin and Mironova 2022). However, there is no need to elaborate something new. From one side, regulators could agree to prohibit intermediaries from including clauses disclaiming the platform’s responsibility for any cyber risks in consumer-cryptocurrency exchange agreements, and from another side, they could develop compulsory cybersecurity risk insurance.

This paper, using the example of Binance’s Agreement, shows how arbitration clauses are constructed in favor of the digital platform and generate inequity between consumers and crypto-exchanges. Some analysts designate that “contractual provisions on exclusive jurisdiction and applicable law may render the enforcement of users’ claims more difficult” (Katona 2021). This state of affairs is unacceptable. If customers are limited to bringing a claim before the court, it would go against the fundamental principles of investor protection. Correct and fair resolution of conflicts between consumers and digital platforms is crucial (Kozhemyakin and Mironova 2022) and shall be a cornerstone of investors’ protection in the digital epoch. Therefore, it is better for governments to promote the rule when customers may decide the method of conflict resolution; it means that when entering into a contract, crypto-exchanges shall give investors a choice among different mechanisms of conflict resolution: a court of the customer’s nationality, a state court of the place where an exchange is incorporated, or an arbitration institution proposed by a crypto-exchange. A named approach will equalize customer and crypto-exchange rights in the question of judicial protection as well as decrease the conflict of jurisdictions in transnational trade with Bitcoins.
Summarizing the proposals on how to arrange crypto-exchange regulation, it is necessary to emphasize that it is better to introduce them in conjunction as a ground for a model law, which could be adopted by international institutions, for example, the United Nations Organization. This model law shall provide a definition of Bitcoin as a tradable commodity stored by the crypto-exchange or a custodian for an investor. It is necessary to clarify the legal status of crypto-exchanges and indicate them as organizations that must be registered and licensed in accordance with domestic laws applicable to financial institutions, i.e., particular requirements will be under the competence of national regulators. The model law should oblige crypto-exchanges to provide customers with clear information, launch education of consumers, and implement sound standards of trading in cryptocurrencies and cyber security. It is necessary to include in the model law provisions concerning the responsibility of crypto-exchanges to keep investors’ funds safe and compensate for any losses caused by hacker attacks. It should be prohibited to conclude consumer agreements that infringe upon the consumers’ rights and limit them in a question of judicial protection. The model law also should promote self-regulation in the industry and push crypto-exchanges to establish standards of conduct.

5. Conclusions

The United Nations Organization in the General Assembly’s Resolution N70/186 declares that Member States should cooperate in combating fraudulent and deceptive cross-border commercial practices. In cases of crypto-exchanges, cooperation is more than necessary. The character of blockchain technology demonstrates that all the proposed measures will be effective only if national regulators promote coordination and harmonization in this area. Otherwise, crypto-exchanges may find a convenient jurisdiction where they will be untouchable for customers if there is a dispute. Additionally, it is necessary to focus on consumer rights and promote rules obligatory for consumer agreements which will increase the level of individual protection.

It would be much more preferable if international organizations prepared a model law or introduced a framework that standardizes and harmonizes the basic principles for activities with cryptocurrencies. This paper proposes the key directions for shaping a comprehensive international legal framework that could be applied to crypto-exchanges dealing with decentralized cryptocurrencies. They include the following main points: licensing of crypto-exchanges, education of consumers, recognition of Bitcoin as a commodity, implementation of self-regulation in the industry, the responsibility of crypto-exchanges for cyber security, the liability of intermediaries to their customers for losses caused by hacker attacks, and the prohibition of unequal consumer agreements.

Funding: The research is implemented at the expense of grant No. 22-28-01031 of Russian Science Foundation, https://rscf.ru/en/project/22-28-01031/.

Data Availability Statement: Not applicable.

Acknowledgments: I am grateful for the support I have received from the Russian Science Foundation within grant No 22-28-01031 of, https://rscf.ru/en/project/22-28-01031/.

Conflicts of Interest: The author declares no conflict of interest.

Notes

4. Id.
5. Any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.


10. see note 9 above.


18. see note 4 above.


20. See note 7 above.


25. Compiled by the author.


References


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.