REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 1, 2026, 47-53

Cryptocurrencies in the Digital Age: Global Legal Challenges

Hoang Le Buu[1]

Abstract

Cryptocurrency has rapidly emerged as a vital pillar of the digital economy, introducing transformative changes to the financial system and fostering unparalleled levels of innovation and efficiency. However, its swift expansion and decentralized characteristics have emphasized pressing legal challenges that require urgent attention and resolution. A significant issue is the lack of clear legal frameworks for resolving disputes and ensuring accountability in cryptocurrency transactions, which has intensified the complexity of legal risks. This article aims to shed light on the critical legal risks tied to cryptocurrency, such as regulatory gaps, the dangers of fraud and cybercrime, concerns about money laundering, and the urgent necessity to protect consumer rights.

Article History
Received 27 September 2025
Revised 22 February 2026
Accepted 25 February 2026
Published 26 February 2026

OPEN ACCESS

Keywords
Virtual currency, legal risk, global

Introduction

In the context of globalization and the explosion of digital technology, cryptocurrencies have emerged as a revolutionary financial trend, challenging traditional financial systems. With superior advantages such as decentralization, transparency, and the ability to conduct rapid cross-border transactions, cryptocurrencies are gradually becoming an indispensable part of the digital economy. However , the rapid development of cryptocurrencies also brings with it serious legal risks, from the lack of a consistent legal framework to the risk of fraud, money laundering, and infringement of consumer rights.

The lack of clear regulations and coordination among countries in managing cryptocurrencies has created a legal vacuum, making it difficult for authorities to control and protect public interests. Simultaneously, the complexity in determining legal liability and resolving disputes related to cryptocurrencies further exacerbates these challenges. Given this situation, researching and proposing appropriate legal solutions for effective cryptocurrency management has become an urgent requirement, not only to ensure the sustainable development of this new financial technology but also to contribute to economic and social stability.

An Overview of Cryptocurrencies

The European Central Bank defines virtual currency *as "a digital currency, unregulated, issued and typically controlled by a creator, used and accepted by members of a particular virtual community* ." (European Central Bank, 2012)

According to the U.S. Government Accountability Office , *" Virtual currency is a digital value, not issued by the government. Virtual currency can be used in the virtual economy and cannot be converted into currencies issued by governments or used to buy and sell goods and services in*

[1] Thu Dau Mot University, Vietnam. Email: buuhl@tdmu.edu.vn

the real economy and converted into currencies at a virtual currency exchange rate ." (Thi Nhu Y, 2017)

The South African Reserve Bank (SARB) has defined *" virtual money as something that is electronically or digitally stored, can be bought or sold, is capable of functioning as a medium of exchange and as a store of value or unit of account but does not have the status of legal tender. "* (South African Reserve Bank (SARB), 2014).

Legal challenges of cryptocurrencies

Money laundering

Money laundering is becoming a major problem in cryptocurrency-related criminal activities, especially as criminals exploit the anonymity of cryptocurrencies to legitimize illicit funds. Through both on-chain and off-chain methods, offenders transform funds obtained from illegal activities, including traditional crime, cybercrime, online fraud, or even cryptocurrency theft from exchanges, into "clean" money. To achieve this, criminals often use diverse methods and services, transferring funds through multiple wallet addresses or businesses to conceal their illegal origin. Next, this money is transferred to a seemingly legitimate source, often through cryptocurrency exchanges, for liquidation. This complex process not only obscures the flow of funds but also makes tracing back the original illegal activities a significant challenge for law enforcement agencies. The sophistication of money laundering methods in the cryptocurrency world necessitates international cooperation and stricter oversight measures to effectively prevent this type of crime.

Money launderers launder money through a “three-stage money laundering” process (Moodley, 2008) , which consists of three stages: arrangement, layering, and integration. (United Nation, ed.)

First stage of the money laundering cycle begins with profiting from illegal activities, such as drug trafficking or bank robbery. Once the illicit money is obtained, it is transferred into legitimate financial markets. There are various methods of arrangement, for example, opening multiple bank accounts and depositing small amounts of cash into them to avoid arousing suspicion from authorities. This method often depends on how the illicit money was generated.

The segregation phase is the stage where many financial transactions take place. During this phase, the funds involved are converted or moved with the aim of separating, to the extent possible, illicit activities from the proceeds of those activities.

The third stage , or integration, typically involves returning these proceeds to the criminal entities. At this stage, the proceeds are "cleaned" of their illegality through three stages. Success in these three stages allows the criminals to evade criminal liability as well as the proceeds from the crime. Therefore, the introduction of a new platform, such as cryptocurrency trading, exacerbates the potential problems that law enforcement and regulatory agencies may face in preventing money laundering.

The reasons criminals choose cryptocurrencies as a means to carry out money laundering are: (1) Cryptocurrencies are created with anonymity from the outset, resulting in the laundering phase often being unnecessary. (2) Creating an account takes only seconds and is free, with each account used only twice for receiving and sending money. (3) A large-scale money laundering scheme can be executed with thousands of transactions at low cost through computer scripts. (4) With soaring exchange rates , some cryptocurrencies can grow by as much as 10,000%, easily creating a justification for sudden wealth accumulation through cryptocurrencies (United Nation, nd).

Acts of financing terrorism

The United Nations Security Council defines terrorism as "criminal acts, including those targeting civilians, committed with the intent to cause terror in the general population or against a particular group or individual, to intimidate a population or to compel a government or international organization to take or refrain from taking action." The UN further emphasizes that a terrorist act is a deliberate act intended to cause serious consequences, including death or serious physical injury. The purpose of such an act is to intimidate, possibly targeting a group or government. (UN Security Council Resolution 1566, ed.)

One criminal offense associated with cryptocurrencies is the purchase of illegal items such as weapons, child abuse materials, and drugs. (Office on Drugs and Crime (UNODC), 2014) Cryptocurrencies, such as Bitcoin, are often used on the "dark web"—an anonymous online marketplace accessible only to tech-savvy individuals. The dark web functions as an online "black market," trading in a wide variety of illegal goods without revealing the identities of buyers or sellers. This facilitates the purchase of weapons or tools for crime by criminals, including terrorists, with little chance of detection. The anonymity of cryptocurrencies and the dark web makes them ideal tools for illicit activities.

A prime example of a website used to purchase illicit tools is Silk Road (K. Goldman et al., nd) . This website accepts Bitcoin for the purchase of illicit tools such as malware and fake passports. When law enforcement discovered it, they seized 174,000 Bitcoins worth approximately $34 million (approximately 544,800,000 R) at the time. The FBI, DEA, and criminal agencies from multiple countries participated in the Silk Road investigation to verify the illicit transactions involving virtual currency and dark websites. FFI research showed that terrorists use the internet to transfer money using virtual currency, another example of cybersecurity risk. (Normark & Ranstorp, 2015)

Due to their perceived anonymity, cryptocurrencies have attracted terrorist organizations and, in recent years, have begun to adopt them to finance their criminal activities.

Tax evasion

Tax evasion is the act of failing to pay taxes in cases where the law requires a person to pay taxes. (Viljoen, 2016) Tax evasion falls under the broader category of financial crime and is therefore carried out through illegal means.

Anonymity is one of the most prominent features of cryptocurrencies (Na'el Al-Tawil, 2022) . Unlike traditional bank accounts that require customer identity verification, cryptocurrencies allow users to conduct transactions anonymously through alphanumeric addresses, which include a public key and a private key. The public key acts as a public blockchain address, used to create one or more cryptocurrency addresses. This characteristic facilitates individuals who want to evade taxes to easily transfer large sums of money without leaving a clear trace. For example, a person can sell valuable assets for cryptocurrency and transfer that amount to a foreign wallet without linking the transaction to their real identity, thus avoiding paying taxes. The cryptocurrency system allows users to transact without revealing their identity, making it difficult for tax authorities to track asset ownership or transfer transactions. This creates opportunities for taxpayers to conceal ownership and transfer large amounts of assets without scrutiny. As a result, individuals can evade taxes on capital gains, personal income, or inheritances without being easily detected. The high degree of anonymity of cryptocurrencies makes it difficult for tax authorities to link specific transactions to the identity of a particular individual or entity, increasing the challenges in managing and collecting taxes.

The decentralized nature means that cryptocurrency transactions occur directly between users without intermediaries such as banks or governments. Therefore, there is no supervisory or control body, such as a tax authority, to collect information for tax purposes. In many countries, taxpayers are responsible for self-reporting cryptocurrency income, which creates opportunities for deliberate omission or misrepresentation of taxable transactions. (Yan, 2024)

Because the cryptocurrency ecosystem lacks a central reporting authority, there is no automated system for tax authorities to inspect, monitor transactions, or report suspicious activities from organizations. This makes tax compliance difficult to enforce. As a result, individuals and organizations can conduct multi-million dollar transactions without notifying regulatory authorities, creating opportunities to conceal taxable income or assets.

Some solutions for managing virtual currencies in several countries around the world.

Japan

Japan began regulating cryptocurrencies by amending the Payment Services Act No. 59 of 2009 in June 2016, which came into effect on April 1, 2017. Due to continued incidents of cryptocurrency leaks following the amendments, Japan revised the relevant laws again in 2019. (An, 2022) .

In Japan, only businesses registered with the relevant authorities are permitted to purchase cryptocurrencies for business or profit purposes. These companies must have offices in Japan and at least one senior executive from the country. The business must be a holding company or a company from another country established under laws similar to Japanese law.

According to the Cryptocurrency Act, one of the primary responsibilities of these businesses is managing their customers' cryptocurrencies, and this must be overseen by a qualified accountant. They also need to maintain appropriate records and have agreements with specialized cryptocurrency dispute resolution centers. These records must be submitted annually to the Financial Services Authority (FSA) (Crypto Council For Innovation, 2023) .

Japan has adopted an approach to addressing issues related to cryptocurrencies, aiming to mitigate the potential for terrorist financing and money laundering, while protecting consumers from risks. This policy demonstrates a serious commitment to regulating and supervising the cryptocurrency market, ensuring transparency and security for transactions.

South Korea

South Korea allows cryptocurrencies to operate legally, but subject to strict legal conditions. To use cryptocurrencies, users need a bank account and a real identity. From January 1, 2018, South Korea stipulated that only those meeting these requirements are allowed to trade cryptocurrencies. (FreeMan Law, nd) Cryptocurrency dealers must also sign contracts with banks to conduct transactions. Before signing a contract, the bank will check the dealer's books and network systems to ensure quality management. (Nguyen, 2018) On June 30, 2023, the Financial Services Commission (FSC) passed the Virtual Asset User Protection Act, aimed at protecting user assets, ensuring transaction transparency, and maintaining market discipline; officially enacted on July 18, 2023, and effective from July 19, 2024. (Financial Services Commission, 2024) . Measures aimed at ensuring the protection of cryptocurrency users, transaction transparency, and market discipline will be implemented in 2024. This is a crucial step in the government's policy agenda to establish the infrastructure and regulatory framework for digital assets.

To comply with legal regulations and ensure transparency in business, enterprises need to implement several important measures. First, businesses must open corporate bank accounts

and provide consumers with accounts in their real names at the same financial institution. This enhances transparency and makes it easier to track transactions.

Secondly, businesses need to implement enhanced anti-money laundering (AML) and know-your-customer (KYC) processes based on risk assessments, including customer due diligence and reporting of suspicious transactions. This requires a technical solution that allows the sharing of customers' personal data with counterparty trading parties in accordance with FATF Regulation R.16.

In addition, companies need to obtain Information Security Management System (ISMS) certification from the Korea Internet Security Agency (KISA) to ensure their information systems meet high security standards.

Finally, businesses must provide detailed information to financial intelligence agencies, including company name, representative's name, business location, contact information, and bank account details. These measures aim to ensure safety, transparency, and legal compliance in business operations.

Egypt

Egypt is one of the countries that bans the use of cryptocurrencies. From Egypt's perspective, cryptocurrencies are considered Haram (News24.com, 2018) , meaning they are prohibited under Islamic law. This ban was issued after a warning from the Egyptian central bank in January 2018 about the risks associated with using cryptocurrencies. Dar al-Ifta, the main Islamic legislative body, issued a religious decree to reinforce this ban. According to the regulations, only currencies issued by the Egyptian central bank are legally recognized and used in payment transactions.

The ban on cryptocurrencies stems primarily from concerns about the potential risks associated with their use. Dar al-Iftar, an authority in religious and legal matters, pointed out that cryptocurrencies could pose a serious threat to national security and the stability of the financial system (Maanda, 2019) . The reason is that the decentralized and anonymous nature of cryptocurrencies facilitates their exploitation by criminal organizations, terrorists, or individuals with malicious intentions to conduct illegal transactions, launder money, or finance dangerous activities. These risks not only affect social order but also threaten the transparency and security of the global financial system. Therefore, banning cryptocurrencies is seen as a necessary measure to prevent potential threats and protect national interests.

Conclusion

Cryptocurrencies, with their rapid development in the digital age, have brought many opportunities for innovation and transformed the way traditional financial transactions are conducted. However, the emergence of cryptocurrencies also poses significant global legal challenges, requiring cooperation and regulation from countries and international organizations. One of the biggest challenges is the lack of a unified legal framework, leading to fragmentation in the approach to regulating cryptocurrencies among countries. While some countries like Japan and Switzerland have adopted progressive regulations to promote innovation, others have been cautious or even completely banned cryptocurrencies due to concerns about financial security risks, money laundering, and terrorist financing.

Addressing these challenges requires close collaboration between governments, financial institutions, and the technology community. Building a flexible legal framework that balances innovation and risk management is crucial for the sustainable development of cryptocurrencies in the future. Only when legal challenges are resolved can cryptocurrencies become an effective and secure financial tool in the digital age.

References

An, N. (2022). *Japan: Amending laws to regulate cryptocurrencies* . People's Representatives Online Newspaper. https://daibieunhandan.vn/nhat-ban-sua-doi-phap-luat-de-quan-ly-tien-ma-hoa-10291524.html

Crypto Council For Innovation. (2023). *Policy Brief: Japan's FSA Crypto Asset and Stablecoin Framework* . Crypto Council For Innovation. https://cryptoforinnovation.org/policy-brief-summary-of-japanese-fsa-crypto-asset-and-stablecoins-framework/

European Central Bank. (2012). *Virtual currency schemes* . https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Financial Services Commission. (2024). *New Enforcement Decree on the Protection of Virtual Asset Users Approved by the Government* . Korea.Net. https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=82534&type=N&insttCode=A260302

FreeMan Law. (nd). *South Korea and Cryptocurrency* . FreeMan Law. Retrieved https://freemanlaw.com/cryptocurrency/south-korea/

K. Goldman, Z., Maruyama, E., Rosenberg, E., Saravalle, E., & Strauss, J.S.-. (nd). *Terrorist use of virtual currencies: Containing the potential threat* . Center for a New American Security. Retrieved January 30, 2025, from https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies

Maanda, M.H. (2019). *Legal implications of virtual currencies* [Master Thesis]. University of Pretoria.

Moodley, M.S. (2008). *Money Laundering and Countermeasures: A Comparative Security Analysis of Selected Case Studies with Specific Reference to South Africa* [Master Thesis]. University of Pretoria.

Na'el Al-Tawil, T. (2022). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control* .

News24.com. (2018). *Egypt's mufti says bitcoin forbidden in Islam* . News24.Com. https://www.news24.com/News24/egypts-mufti-says-bitcoin-forbidden-in-islam-20180104

United Nations Security Council Resolution 1566.

Nguyen, H. (2018). *South Korea inspects 6 banks regarding the provision of virtual currency services to customers* . Banking Times. https://thoibaonganhang.vn/han-quoc-kiem-tra-6-ngan-hang-ve-viec-cung-cap-dich-vu-tien-ao-cho-khach-hang-71786.html

Normark, M., & Ranstorp, M. (2015). *Understanding terrorist finance: Modus operand and national CTF-regimes* . Swedish Defense University.

Office on Drugs and Crime (UNODC). (2014). *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies* . https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf

South African Reserve Bank (SARB). (2014). *Position Paper on Virtual Currencies* .

Thi Nhu Y, N. (2017). *Bitcoin—Current situation in some countries around the world and management in Vietnam* [Master's thesis]. Ho Chi Minh City University of Economics.

United Nation. (nd). *Money laundering through cryptocurrencies* . Retrieved https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

Viljoen, J. (2016). *Lessons from history: Tax evasion* [Master Thesis].

Yan, S.Y. (2024). Cryptocurrency and Tax Evasion: Unraveling the Digital Knot for Global Governance. *Proceedings of the 2024 2nd International Conference on Management Innovation and Economic Development (MIED 2024)* .