Cryptocurrency and Tax Evasion: Unraveling the Digital Knot for Global Governance

Suet Yi Yan

University of Leeds, Woodhouse Lane, Leeds, LS2 9JT, UK
1714010826@stu.hrbust.edu.cn

Abstract. In the digital age, the advent of cryptocurrencies such as Bitcoin and Ethereum was not just anticipated but has rapidly become a mainstay, heralding a paradigm shift in the financial ecosystem. However, their ascent has challenges for tax regulation and enforcement. This paper delves into the research background by highlighting the intrinsic properties of cryptocurrencies—namely, their anonymity, decentralization, and the absence of centralized reporting mechanisms—that complicate tax governance on an international scale. It articulates the thematic focus on the jurisdictional complexities and the pursuit of regulatory consensus through meticulously examining existing legal frameworks and illustrative case studies of cryptocurrency-related tax evasion. Methodologically, the study adopts a qualitative analytical approach to dissect the specific challenges digital currencies introduce to tax governance. It meticulously investigates the strategies leveraged to exploit these unique features for tax evasion and critically evaluates the capacity of existing legal frameworks, including the Fifth Anti-Money Laundering Directive and the Financial Action Task Force's Travel Rule, to surmount these hurdles. The key findings illuminate the dichotomy presented by digital currencies. While they forge innovative financial pathways, they concurrently pave the way for novel forms of tax evasion and money laundering, exacerbating the complexity due to a disjointed international regulatory landscape. Conclusively, this research advocates for implementing incentive-based reporting mechanisms and embracing cutting-edge technological solutions to bolster transparency and compliance. It emphasizes the overarching conclusion that international collaboration is paramount in crafting a standardized and harmonized global governance framework for digital currencies. The perpetually evolving nature of digital currencies demands unwavering vigilance, innovative thought, and cooperative engagement from all stakeholders involved, highlighting the importance of adaptability and unity in addressing the challenges and opportunities they present.

Keywords: Cryptocurrency, Tax Evasion, International Regulation.

1 Introduction

In recent years, the emergence of multiple tax haven leaks, starting with the Offshore Leaks in June 2013 and culminating with the Panama Papers in 2016, has significantly heightened public awareness and concern regarding tax evasion, avoidance, and fraud

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024)*, Advances in Economics, Business and Management Research 300,
https://doi.org/10.2991/978-94-6463-542-3_45

[1]. The revelation of the Panama Papers alone catalyzed a global awakening, prompting governments worldwide to reclaim an astonishing sum of over $1.36 billion in back taxes. A mere glimpse into the global scale of tax evasion, avoidance, and fraud, as illustrated by the Panama Papers, warrants such a staggering figure. These revelations have undoubtedly cast a spotlight on tax evasion, avoidance, and fraud, posing substantial threats to the integrity of both national and global financial systems during this period. While these three terms are often confused, they have different meanings from a legal and financial perspective. The U.S. Supreme Court has endorsed tax avoidance as an attempt to legally minimize tax obligations, recognizing the lawful right to reduce or avoid taxes using methods permitted by law [2]. Tax evasion, on the other hand, involves intentionally violating tax laws, potentially resulting in jail time, since it involves intentional disregard for legal obligations, where a mistake in understanding tax laws or belief in one's tax position cannot justify such behavior [2]. In tax fraud, information is intentionally falsified to avoid accurate tax assessments, for example, underreporting income or overstating deductions [3].

At the same time, digital currencies such as Bitcoin and Ethereum demonstrate another aspect of the global financial landscape that is rapidly evolving. Digital or virtual currencies, based on blockchain technology and secured by cryptography, have revolutionized financial transactions, and they have also created unique challenges for tax regulation and enforcement [4]. International communities were already dealing with tax evasion and avoidance with a lot of challenges before the rise of cryptocurrencies, but now digital currencies are complicating the situation further [5]. The international tax governance framework, a complex amalgam of bilateral and multilateral agreements, national laws, and guidelines from international organizations like the OECD and G20, is increasingly under pressure to adapt to the rise of digital currencies.

This paper aims to analyze the challenges digital currencies present to international tax governance, focusing on issues like anonymity and decentralization, jurisdictional complications, and the lack of regulatory consensus. Taking into account the dynamic and evolving nature of both digital currencies and international tax regulation, this paper will examine possible legal response strategies. The study is intended to contribute to the ongoing discussion about how to effectively govern and tax digital currency transactions globally by examining case studies and current regulatory measures. Firstly, the paper will provide an overview of digital currencies and their current regulatory measures, followed by an analysis of cases that highlights instances of tax evasion using cryptocurrencies. It will then discuss the specific challenges these currencies present to international tax governance and conclude with potential solutions of incentives for reporting and tracing methods, emphasizing the importance of international cooperation.

2 Characteristics and Challenges of Digital Currencies

2.1 Digital Currencies and Their Characteristics

Digital currencies, led by the likes of Bitcoin, are reshaping the financial world, pivoting away from centralization towards a distributed model that enhances transaction

transparency and user privacy. They operate on a blockchain network - a globally distributed ledger akin to a communal notebook, transparent to all but without a central owner. This ledger records all transactions made with digital currencies, ensuring they are verifiable by any participant yet not controlled by any single entity. The trust in this system is established not by a central institution but by a consensus among all users. Here, every participant, or node, plays a part in validating transactions and maintaining the ledger.

The governance of digital currencies reflects a decentralized philosophy. Bitcoin, for example, thrives on a peer-to-peer network, underpinned by blockchain to ensure secure transactions and controlled creation of new units [6]. This setup resembles Decentralized Autonomous Organizations (DAOs), as cryptocurrencies function as decentralized digital currencies using blockchain to secure transactions and control the creation of new units [7]. It is governed by programmed rules or smart contracts, which execute automatically, and decisions within a DAO are often made through community voting [8]. In this DAO setting, an algorithmic rule sets the money supply, and the integrity of the network replaces the need to trust the integrity of human participants. DAOs and consensus mechanisms like PoW eliminate the need for centralized control, allowing community-driven decisions and algorithmic rules to guide operations. Security is inherently strong due to the cryptographic links between blocks in the blockchain, making tampering virtually impossible [8]. However, user security largely depends on safeguarding private keys, as the loss or theft of a private key puts assets at risk. The blockchain's design offers an irreversible transaction process, a degree of anonymous nature, and eliminates the "middleman".

2.2 How Digital Currencies Become Tools for Tax Evasion

Cryptocurrencies such as Bitcoin, Ethereum, and Monero, characterized by their decentralized, encrypted nature, challenge traditional regulatory and enforcement mechanisms designed to maintain the integrity of financial systems. Their features, including pseudonymity and the absence of a central reporting authority, create sophisticated and difficult-to-trace avenues for tax evasion and money laundering.

Pseudonymity is one of the most prominent features of cryptocurrencies [9]. Unlike traditional bank accounts requiring customer identification, cryptocurrencies allow users to transact under pseudonyms represented by alphanumeric addresses the public key and the private key. The public key serves as the blockchain address visible to anyone and is used to generate one or more Bitcoin addresses. The private key is a secret piece of data that proves the right to spend bitcoins from a specific wallet through a cryptographic signature. As a result, individuals seeking to evade taxes can easily transfer large sums of money without leaving a clear trail. For instance, a person could sell a valuable asset for cryptocurrency and transfer the digital currency to an offshore wallet without the transaction being directly tied to their identity, effectively shielding it from taxation. The system allows individuals to transact without revealing their true identities, making it challenging for tax authorities to trace asset ownership or transfers directly to individuals and enabling taxpayers to obscure the ownership and transfer of substantial wealth outside regulatory oversight. Consequently, individuals can evade

taxes on capital gains, income, or inheritance without easily being traced by fiscal authorities. This level of anonymity makes it challenging for tax authorities to link specific transactions to identifiable individuals or entities [9].

A decentralized nature means transactions occur directly between users without an intermediary, like a bank or government. Consequently, there is no centralized point of monitoring or control where tax authorities could traditionally expect to gather data for taxation purposes. In many jurisdictions, the responsibility for reporting crypto-related gains indeed falls on the individual taxpayer, creating opportunities for deliberate omission or falsification of taxable events in the crypto space. For example, in the U.S., the Internal Revenue Service (IRS)categorizes cryptocurrencies as property, subjecting transactions to capital gains tax, with individuals responsible for reporting [10]. The United Kingdom's Her Majesty's Revenue and Customs (HMRC) [11], and the Australian Taxation Office (ATO) similarly mandate self-reporting capital gains from crypto assets on tax returns [12]. In Canada, the Canada Revenue Agency (CRA) treats crypto as a commodity, requiring taxpayers to report income or gains from transactions as business or capital gains [13]. In the context of tax evasion, the self-reporting system inherently allows individuals to omit or falsify information about their transactions and holdings deliberately. The complexity of tracking transactions across multiple wallets and exchanges, combined with the pseudonymous nature of blockchain transactions, exacerbates the challenge for tax authorities in verifying the accuracy of reported information, leading to potential underreporting and evasion of taxes [9]. The absence of a central reporting authority in the cryptocurrency ecosystem means no automatically generated reports for tax authorities to review, suspicious activity reports from institutions, and no straightforward way to enforce tax compliance on cryptocurrency transactions. As a result, individuals and entities can conduct transactions worth millions of dollars without automatic notification to regulatory bodies, providing an attractive mechanism for concealing taxable income or assets.

Moreover, tax-loss harvesting exemplifies a sophisticated strategy for minimizing taxable income through cryptocurrencies. The "wash sale" rule, a regulation in securities markets, disallows tax deductions for losses on the sale of a security if a substantially identical security is purchased within 30 days before or after the sale [14]. The rule aims to prevent taxpayers from claiming tax benefits on artificial losses. However, most cryptocurrencies are not classified as securities by regulatory authorities, the Securities and Exchange Commission (SEC), and are not subject to this rule [14]. This absence allows investors to sell cryptocurrencies at a loss and repurchase them immediately, leveraging these transactions for tax benefits without violating wash sale regulations. Investors can sell their digital assets at a loss to offset capital gains in other areas of their portfolio and repurchase them almost instantaneously, preserving their market position. The absence of the "wash sale" rule, which prevents the claim of a tax deduction for a security sold in a wash sale in the context of cryptocurrency transactions, accentuates the appeal of digital currencies for aggressive tax planning.

2.3 How Digital Currencies Become Tools for Money Laundering

Cryptocurrencies can also be utilized in money laundering through intricate steps that exploit their inherent characteristics. Cryptocurrencies can be leveraged in the money laundering process, detailing the placement, layering, and integration stages.

The initial step in money laundering using cryptocurrencies involves the placement of illicit funds into the digital financial system. Criminals initiate this process by converting their "dirty" money into cryptocurrencies through various means [9], such as purchasing them on cryptocurrency exchanges, using peer-to-peer platforms, or through Initial Coin Offerings (ICOs). An ICO is a fundraising method that new cryptocurrency projects use to sell their underlying crypto tokens in exchange for bitcoin, ether, or other established cryptocurrencies. It is similar to an Initial Public Offering (IPO) for stocks, where investors buy company shares. The anonymous or pseudonymous nature of many cryptocurrency transactions makes it difficult to trace the source of funds [15]. Additionally, mixers or tumblers are services that improve the anonymity of cryptocurrency transactions. They mix the digital assets of multiple users before redistributing them, making it harder to trace the source of the funds.

Once illicit funds have been converted into cryptocurrency, the layering phase begins. This stage involves conducting complex transactions across different cryptocurrencies and blockchain platforms to distance the funds from their illegal origins [9]. Criminals may employ tactics such as chain hopping, which involves moving assets across different blockchain platforms or cryptocurrencies to complicate the transaction trail and obscure the origin of funds [15].

Another method is to use decentralized finance (DeFi) platforms for swapping assets through liquidity pools, which are collections of funds locked in a smart contract. This method does not require user identification, further anonymizing the transaction history. DeFi refers to financial services that operate on a blockchain [9], allowing people to lend, borrow, trade, and earn interest on their cryptocurrency without the need for traditional financial intermediaries like banks. These transactions exploit the crypto ecosystem's decentralized and often lightly regulated nature, making it exceedingly difficult for authorities to follow the money trail.

The final stage involves integrating the laundered funds into the legitimate economy as "clean" money [9]. This can be accomplished by purchasing valuable assets with cryptocurrencies, such as real estate, luxury goods, or NFTs (Non-Fungible Tokens), that can later be sold for fiat currency. Another method involves using cryptocurrency debit cards, which convert crypto assets into local currencies at point-of-sale, allowing criminals to spend their money freely. Additionally, investing in legitimate businesses or ICOs as a silent partner or through shell companies can provide a facade of legitimacy to the illicit funds [9]. Once integrated, the money is distanced enough from its source to be used without raising suspicion.

Using cryptocurrencies in money laundering exemplifies criminals' sophisticated methods to exploit the digital currency space. The inherent features of cryptocurrencies, such as their global accessibility, pseudo-anonymity, and the rapidity and permanence of transactions, create significant challenges for regulatory and enforcement agencies aiming to curb such illicit financial flows.

3 Current Legal Responses to Tax Evasion via Digital Currencies

3.1 The International Legal Framework's Response to the Challenge of Digital Currency Tax Evasion

The Fifth Anti-Money Laundering Directive. In the European Union, crypto assets and cryptocurrencies are designated as Qualified Financial Instruments (QFIs) [9]. Regional regulations necessitate that cryptocurrency exchanges dealing with QFIs are required to comply with EU regulations, including AML Directives (AMLD). Notably, the Fifth Anti-Money Laundering Directive (5AMLD) extended AML legislation to include cryptocurrency-fiat currency exchanges in 2020, mandating these businesses to perform thorough customer due diligence, register with local authorities, and adhere to standard reporting requirements [16].

The directive bolstered the financial system's defenses by heightening corporate and trust ownership transparency, augmenting financial intelligence access, mitigating risks associated with the anonymity of digital currencies and prepaid devices, and encouraging improved AML supervision and coordination with the European Central Bank. Specifically, 5AMLD mandated that virtual currency exchange services and custodian wallet providers come under AML/CFT regulations, marking the first instance where businesses operating with cryptocurrencies were required to implement regulatory compliance measures [17].

The directive's focus on Customer Due Diligence (CDD) required verifying personal information from credible sources to counteract the anonymity of digital currency transactions. This verification includes collecting names, photo identifications, addresses, and other identifying data [18]. For entities, CDD extends to uncovering the beneficial ownership, which is crucial for piercing corporate veils often used in money laundering or tax evasion. By understanding the control structures of companies, the real controlling parties are exposed, hindering the misuse of digital currencies for illicit activities [18].

Financial Action Task Force. The Financial Action Task Force (FATF) recommended crypto firms follow the Travel Rule to curb the increasing abuse of crypto platforms for money laundering in 2019. One of the key FATF Recommendations is the Travel Rule, formally known as Recommendation No. 16, which was initially targeted at wire transfers but expanded to include Virtual Asset Service Providers (VASPs) in response to the evolving nature of financial transactions, including the rise of digital currencies [19].

The Travel Rule requires financial institutions and VASPs to collect and share personal information on the parties of transactions that exceed a certain threshold, which is currently set at US$/€1,000 [19]. This information includes but is not limited to names, account numbers, physical addresses, unique ID numbers, customer identification numbers, or the date and place of birth of the individuals, beneficiary name and

account number or virtual wallet number involved in the transactions [19]. Furthermore, the FATF creates a more transparent financial environment by mandating personal data collection and sharing among financial institutions and VASPs. This transparency not only aids in the direct prevention of financial crimes but also serves as a deterrent to individuals and entities looking to exploit the digital currency space for illicit purposes.

3.2 The Social Reality of Tax Evasion Through Digital Currencies

The cases of John McAfee and Ethan Thomas Trainor shed light on the social reality of tax evasion through digital currencies, illustrating the complexities and challenges arising in the cryptocurrency age.

John McAfee, a notable figure in the tech industry, faced charges for failing to file tax returns on millions earned from various ventures, including cryptocurrencies, for four years. The Securities and Exchange Commission also brought civil charges against McAfee, alleging that he made over $23 million by promoting cryptocurrency offerings without disclosing he was paid. McAfee's alleged evasion strategies included using nominees to hide income in cryptocurrency exchange accounts, revealing a sophisticated understanding of digital currencies to evade tax obligations. This method of concealing income and assets is not unique to McAfee but reflects a broader challenge of the allure of cryptocurrencies for those seeking to obscure wealth from tax authorities, challenging the traditional financial oversight and taxation mechanisms.

Ethan Thomas Trainor's case further demonstrates the darker side of cryptocurrency transactions, linking tax evasion to illegal activities on the dark web. Trainor admitted to earning over $1 million in cryptocurrency through dark web transactions and attempted to conceal this income using "mixers," services that anonymize cryptocurrency transactions. His activities demonstrate how the inherent features of digital currencies, designed to ensure privacy and security, can also be exploited for tax evasion and illegal trade.

Both cases exemplify the broader social implications of digital currencies in enabling new forms of tax evasion. While digital currencies offer innovative opportunities for privacy and financial autonomy, they also create avenues for tax evasion and illegal activities that undermine the social contract and fiscal responsibilities citizens owe to their governments.

3.3 Limitations of the Current International Law in Governing Tax Evasion through Digital Currencies

Legislative Challenges. The current international law faces significant challenges in regulating tax evasion through digital currencies, partly due to the fragmentation of regulations. In the United States, federal agencies differ in their approach to cryptocurrencies: the SEC views them as securities, the CFTC as commodities, and the FinCEN under money services business regulations. This regulatory mosaic hinders the establishment of unified tax laws for digital currencies [9]. The situation is similar in the United Arab Emirates (UAE) and the European Union (EU); the lack of a cohesive

regulatory framework results in a patchwork of regulations across its various emirates and member states. Globally, countries exhibit a wide range of regulatory stances, from El Salvador's acceptance of Bitcoin as legal tender to the prohibitive measures seen in China and India, further complicating the establishment of a cohesive regulatory strategy [9].

Jurisdictional issues compound these challenges. The transnational nature of cryptocurrency transactions makes determining the jurisdiction for tax purposes complex, allowing individuals to exploit regional regulatory disparities. The EU's 5AMLD sought to mitigate this by increasing transparency and facilitating information exchange, yet several member states have been slow to implement it, underscoring the gap between legislative proposals and practical enforcement.

Additionally, tax havens present significant obstacles to international regulatory efforts due to their characteristic reluctance to exchange taxpayer information, a preference for minimal financial disclosure, and often low taxation on foreign income and assets, coupled with permissive corporate governance. Notably, some jurisdictions identified as tax havens, including Ireland, Luxembourg, and the Netherlands, have been lagging in the implementation of the 5AMLD. This hesitance extends to engaging with global measures designed to enhance financial transparency, such as the FATF's Travel Rule and OECD's initiatives for information exchange and addressing BEPS. Such reluctance by tax havens poses a substantial hurdle to curtailing tax evasion, particularly within the digital currency sphere, where the traceability of transactions is a critical component of financial oversight.

Judicial Challenges. The judicial system encounters significant challenges when confronting the anonymity of cryptocurrencies and technologies such as the Tor browser and 'mixers'. These tools obscure user identities and actions, complicating the tracing of illicit activities and their perpetrators [20]. Although the blockchain can reveal questionable transactions, the anonymity afforded by these technologies makes it difficult to connect activities to specific individuals for legal action.

This obscurity presents a notable dilemma in legal contexts where associating anonymous online actions with actual identities is essential for prosecution. Despite global initiatives like Know Your Customer (KYC) guidelines, CDD, and the Travel Rule, designed to counter such issues, new services that enhance privacy complicate enforcement efforts. These services can effectively thwart attempts to track transactions back to their originators.

Hence, the current international legal framework's inadequacies in dealing with tax evasion via digital currencies are highlighted. The complex, anonymized nature of digital currencies, combined with sophisticated privacy-enhancing technologies, undermines traditional legal and investigative methods. Consequently, the international legal system struggles to keep pace with the rapid evolution of digital currencies, underlining the need for innovative legal, technological, and collaborative approaches to address these challenges effectively and curb tax evasion and related illicit activities through digital currencies.

4 Future Strategies for Managing Tax Evasion Involving Digital Currencies

4.1 Incentives for Reporting

Drawing inspiration from the Panama Papers, which exposed intricate international tax evasion schemes via offshore companies and accounts, implementing incentive reporting emerges as a pivotal strategy in combating tax evasion facilitated through cryptocurrencies. The Panama Papers revealed many individuals and entities utilizing offshore accounts and corporate structures to minimize or evade tax liabilities. Originating from Mossack Fonseca, a Panamanian law firm, these revelations underscored the facilitative role of certain legal and accounting firms in offering "turnkey" tax avoidance solutions.

For Individuals. Applying the lessons learned from the Panama Papers to cryptocurrency tax evasion underscores the importance of intermediaries, such as law firms and financial advisors, who play pivotal roles in tax evasion schemes. In cryptocurrency, this role could be mirrored by exchanges, wallet providers, and other digital asset gatekeepers. Hence, incentive reporting tailored for the crypto sector should focus on these "gatekeepers," offering incentives for reporting suspicious activities and thereby unveiling potential tax evasion practices.

Firstly, monetary rewards for whistleblowers, predicated on traditional whistleblower programs, could be a powerful motivator for disclosing information. Secondly, pre-emptive measures may encourage self-reporting and deter evasion by providing incentives or reducing penalties for voluntary self-reporting of undeclared cryptocurrency transactions. Thirdly, encouraging incentive reporting to include entities that enable cryptocurrency-based tax evasion, whether intentionally or unintentionally, acknowledges the possibility of organisational complicity. Fourthly, protecting and ensuring anonymity for whistleblowers, drawing from the Panama Papers, where anonymous sources were crucial, remains imperative. Offering stringent confidentiality and legal protections for informants, including firm employees privy to sensitive information, is essential.

For Countries. The effectiveness of countermeasures against tax evasion significantly depends on establishing robust international frameworks and genuine cooperation among all jurisdictions, including those often labelled as tax havens. Thus, achieving international consensus and harmonizing regulatory measures across countries present formidable challenges, necessitating a long-term commitment and concerted effort.

Efforts by international regulatory bodies such as the OECD, FATF, and EU to propose and advocate for cohesive regulations to combat tax evasion on a global scale are indispensable. Nevertheless, they must be augmented by strategies that directly incentivize participation and cooperation among countries. In this vein, incorporating incentive reporting mechanisms within bilateral agreements and the strategic utilization of Multilateral Instruments (MLI) emerge as promising approaches. These mechanisms

are designed to create tangible benefits and motivations for countries, encouraging their active participation in international efforts against tax evasion.

One viable strategy involves the establishment of agreements that facilitate the sharing of recovered assets or fines between countries collaborating on cross-border tax evasion investigations. Another crucial aspect of fostering international cooperation is the provision of technical assistance, training, and technology transfers to developing countries by wealthier nations or international bodies. This support, made contingent on the recipient countries' commitment to adhere to international cooperation and transparency standards, would not only empower these nations to more effectively monitor and tax cryptocurrency transactions but also integrate them more fully into the global effort against tax evasion.

Lastly, in integrating incentive reporting mechanisms with existing international reporting standards, particularly those related to KYC and CDD, an opportunity exists to create a more cohesive and effective global regulatory framework. This harmonization ensures that new measures complement and reinforce existing practices, facilitating a more integrated approach to combating tax evasion. By aligning incentive reporting with established regulatory standards, countries can leverage both national and international tools in a concerted effort to address the challenges posed by tax evasion in the digital age.

4.2 Leveraging Technological Means

The root of tax evasion schemes through cryptocurrencies is the inherent nature of peer-to-peer (P2P) systems and the absence of third-party reporting mechanisms, making it difficult for authorities to monitor or track financial flows [6]. Despite the complexities introduced by Tor and Mixer services in tracing these transactions, they inadvertently open a small crack in the door for law enforcement agencies.

One of the methods is to use ExoneraTor, which maintains a database of IP addresses that are or have been part of the Tor network and provides information on the usage of Tor relays [20]. When law enforcement agencies investigate illicit online activities, identifying an individual solely based on an IP address can be unreliable. The unreliability arises predominantly in environments where IP addresses are shared amongst multiple users, such as public libraries, cafes, and open wireless networks. Thus, these IP addresses are not definitive evidence linking a specific person to criminal activities.

ExoneraTor allows investigators to cross-reference IP addresses encountered during their investigations against a publicly accessible database of Tor exit relays [20]. While ExoneraTor does not unveil the originating IP address, it signals to investigators that the suspect IP address was part of the Tor network. In simpler terms, ExoneraTor is like a tool that tells authorities if someone used the Tor service, but it still does not tell investigators who they are. Hence, this sort of information, not directly incriminatory, is invaluable in constructing a circumstantial framework around the suspect's efforts to maintain anonymity, suggesting a potential motivation and a piece of the puzzle to conceal illicit activities.

Additionally, the effectiveness of Tor in protecting a user's identity is contingent upon strict adherence to secure online practices [20]. However, users often inadvertently compromise their anonymity through browser plugins, interacting with Google Captcha, utilizing Flash or PDFs, enabling JavaScript, allowing cookies, or transmitting information in clear text over HTTP [20]. Specifically, content or plugins requiring Java or Flash can independently connect to the internet without routing their traffic through the Tor network. Consequently, these actions can result in data leakage that bypasses the protective layers of Tor, rendering the user vulnerable to identification.

For mixers services, through advanced blockchain analysis techniques and pattern recognition. Authorities can detect patterns in mixing, such as repetitive transaction sizes or timing, similar to identifying Tor use with ExoneraTor. These strategies, while not directly revealing the identity of individuals, significantly contribute to a broader investigation framework, offering crucial insights into attempts to maintain anonymity and possibly conceal illicit activities. Just as lapses in secure online practices can expose Tor users, similar behaviour patterns or transactional characteristics can potentially expose users to mixing services.

Ultimately, both Tor and mixer services share a common vulnerability: the human element. Despite the sophisticated technologies designed to protect anonymity, it is often user behaviour, detectable through meticulous analysis, that opens a pathway for law enforcement to follow, slowly chipping away at the anonymity that criminals rely on to shield their illicit transactions from scrutiny.

5 Conclusion

In conclusion, the inherent traits of cryptocurrencies, particularly anonymity and decentralization, present significant challenges to traditional tax enforcement frameworks. The effectiveness of current international strategies is compromised by fragmented regulations and the emergence of services that further enhance transaction anonymity. Consequently, incentive-based reporting mechanisms and the adoption of advanced technological solutions emerge as viable strategies for increasing transparency and ensuring compliance. These approaches necessitate a blend of regulatory innovation and extensive global collaboration. Looking ahead, despite these proposed methods, achieving standardization and harmonization in the global governance of digital currencies remains a critical goal for the international community. Given the dynamic and continuously evolving nature of digital currency, constant vigilance, innovative thinking, and cooperation among all stakeholders are essential.

Reference

1. Schmal, F., Schulte Sasse, K., & Watrin, C.: Trouble in Paradise? Disclosure After Tax Haven Leaks. Journal of Accounting, Auditing & Finance 38(3), 706–727 (2023).
2. Abney, G., & Monnin, P.: Tax avoidance vs. tax evasion. Tax Executive 70(6), 54–58 (2018).

3. https://plus.lexis.com/api/permalink/9bd0c8d3-a1fe-4505-9977-a4219d96c8f6/?context=1001073
4. Härdle, W. K., Harvey, C. R., & Reule, R. C. G.: Understanding Cryptocurrencies. Journal of Financial Econometrics 18(2), 181–208 (2020).
5. Baer, K., Mooij, R. A., Hebous, S., & Keen, M.: Taxing Cryptocurrencies. IMF Working Paper No. 2023/144. International Monetary Fund, Washington, D.C. (2023).
6. Dyntu, V., & Dykyi, O.: CRYPTOCURRENCY in the SYSTEM of MONEY LAUNDERING. Baltic Journal of Economic Studies 4(5), 75 (2019).
7. Härdle, W. K., Harvey, C. R., & Reule, R. C. G.: Understanding Cryptocurrencies. Journal of Financial Econometrics 18(2), 181–208 (2020).
8. Tredinnick, L.: Cryptocurrencies and the Blockchain. Business Information Review 36(1), 39–44 (2019).
9. Al-Tawil, T. N.: Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches. Journal of Money Laundering Control, (2022).
10. Notice 2014-21. IRS, https://www.irs.gov/pub/irs-drop/n-14-21.pdf, last accessed 2024/3/29.
11. HM Revenue & Customs: Cryptoassets: Tax for Individuals. GOV.UK, https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals, last accessed 2024/3/29.
12. Tax Treatment of Crypto-Currencies in Australia - Specifically Bitcoin. Ato.gov.au, https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/, last accessed 2024/3/29.
13. Canada Revenue Agency: Guide for Cryptocurrency Users and Tax Professionals. Canada.ca, https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html, last accessed 2024/3/29.
14. Avi-Yonah, R.: Comment on Cong et al., 'Tax Loss Harvesting with Cryptocurrencies.' Journal of Accounting and Economics 76(2-3), 101612–12 (2023).
15. Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M.: The Use of Cryptocurrencies in the Money Laundering Process. Journal of Money Laundering Control 22(2), 210–216 (2019).
16. "A Guide to the 5th Money Laundering Directive." LexisNexis Risk Solutions | Transform Your Risk Decision Making, https://risk.lexisnexis.co.uk/insights-resources/infographic/5th-money-laundering-directive, last accessed 2024/4/6.
17. Girasa, R.: International Regulation. Palgrave Studies in Financial Services Technology, 313–377 (2022).
18. "Customer Due Diligence." Www.lexisnexis.com, https://www.lexisnexis.com/en-gb/glossary/customer-due-diligence, last accessed 2024/4/7.
19. "TARGETED UPDATE on IMPLEMENTATION of the FATF STANDARDS on VIRTUAL ASSETS and VIRTUAL ASSET SERVICE PROVIDERS." https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf, last accessed 2024/4/7.
20. Irwin, A. S. M., & Turner, A. B.: Illicit Bitcoin Transactions: Challenges in Getting to the Who, What, When and Where. Journal of Money Laundering Control 21(3), 297–313 (2018).