INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CODE IS NOT A SHIELD: EXTRADITING DECENTRALISED FINANCE PROTOCOL DEVELOPERS FOR DOWNSTREAM CRIMINAL ACTIVITY- A COMPARATIVE ANALYSIS OF LIABILITY, ATTRIBUTION AND JURISDICTIONAL CHALLENGES

AUTHORED BY - VIDHI SINGH
Institution Name- Institute of Law, Nirma University
Fourth Year BA.LLB (Hons) Student

ABSTRACT:

The rapid and exponential expansion of Decentralised Finance (DeFi) protocols has created novel challenges for international extradition law. Traditional legal frameworks struggle to identify individuals accountable and establish a jurisdictional nexus when sovereign and autonomous smart contracts facilitate the evils of money laundering, terrorist financing and sanctions evasion across borders. This research article focuses on the aspects of situations when developers of DeFi protocols should be subjected to extradition for the crimes committed by the users of their blockchain code. This paper addresses a critical gap at the junction of transnational criminal law and technological innovation.

This study evaluates the method of conceptualisation of criminal liability for code developers and the application of foundational extradition principles, such as double criminality, being adopted across different jurisdictions of the US, UK, EU and Singapore. This research employs doctrinal analysis, case study methodology and comparative jurisprudence to scrutinise recent prosecutions, specifically focusing on the Tornado Cash Case, to determine patterns contributing to liability along with procedural challenges. The facet of divergences in balancing innovation protection with criminal liability is also analysed, assessing the imperative issues such as the degree of developer knowledge and control needed to establish criminal liability, if post-deployment immutability of smart contracts negates ongoing responsibility, the degree to determine double criminality when DeFi-centred offence may exist in requesting states but not in the executing states, etc.

ISSN: 2582-6433

The study acts as conceptual groundwork by broadening attribution theory to cover diffuse, decentralised systems and by suggesting frameworks for establishing the territorial nexus in borderless digital crimes. On the ground, it offers a judicial guidance for prosecutors deciding on the feasibility of extradition, defence counsel spotting the viable challenges, and judges dealing with novel technological issues. The research ends with a call for local and international legal reforms — a reduction of friction in bilateral treaties and domestic laws, a move towards international harmonization that still keeps the innovation incentives intact but ensures that those who deliberately facilitate transnational crimes are held accountable. The establishment of clear legal frameworks for developer liability in the case of DeFi ecosystems graduating is as critical to the technological innovation sector as it is to international criminal justice.

The study acts as conceptual groundwork by broadening attribution theory to cover diffuse, decentralised systems and by suggesting frameworks for establishing the territorial nexus in borderless digital crimes. On the ground, it offers judicial guidance for prosecutors deciding on the feasibility of extradition, defence counsel spotting the viable challenges, and judges dealing with novel technological issues. The research ends with a call for local and international legal reforms — a reduction of friction in bilateral treaties and domestic laws, a move towards international harmonisation that still keeps the innovation incentives intact but ensures that those who deliberately facilitate transnational crimes are held accountable. The establishment of clear legal frameworks for developer liability in the case of DeFi ecosystem graduation is as critical to the technological innovation sector as it is to international criminal justice.

Keywords: *Decentralised Finance, DeFi, Extradition, Smart Contracts, Cryptocurrency, Double Criminality, Jurisdictional Nexus, Transnational Crime, Blockchain Technology, Attribution Theory*

I. INTRODUCTION

The introduction of such advanced technology into the financial sector is like the birth of digital currency itself.[1]They are run by the use of smart contracts on blockchains mainly Ethereum-DeFi protocols that allow people to transfer value, build credit relations, and do complex

[1] PHILIPP HACKER, STEVE WERCHICK & MATTHIAS HOLZWEBER, REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 45 (2019).

ISSN: 2582-6433

financial transactions without the helpers. [2]However, this high level of technical know-how has not only been a boon but instead, has created an equal number of problems for regulatory bodies and disciplined law agencies across the globe. The emergence of decentralized finance has been closely related to the cases of illicit use documented. Criminals have used it for money laundering by swimming in liquidity pools, financing terrorism through token transfers, and evading sanctions by decentralized exchanges.[3] This poses a fundamental conundrum: How should the extradition law- a framework built for tangible crimes, identifiable individuals and territorial states- be applied to a borderless system, intangible code and development that is distributed?[4]The answer to this dilemma is not self- evident because unlike the traditional crimes, which are traceable, these computer codes can serve both lawful and unlawful purposes at the same time. Traditional extradition mechanisms are based on several key principles: double criminality, personal jurisdiction, individual culpability and exhaustion of domestic remedies. Each of these principles when used on DeFi developers thus becomes debatable.

Without clear lawfully frameworks, it is difficult to see how DeFi could mature into a legitimate and regulated financial sector. On the other hand, it is possible that legal uncertainty could constantly destabilize the ecosystem.[5]The issue lies in striking a balance which has scope for innovation and mechanism of holding individuals accountable who deliberately facilitate transnational crime.

II. TECHNICAL AND LEGAL OVERVIEW

A. Principles in the Law Of Extradition

Extradition includes the convergence between sovereignty and transnational justice.[6] The traditional extradition system, as outlined in multilateral treaties such as the European Convention on Extradition, enables states to request the surrender of a person suspected of a crime for trial.[7] In turn, there has been a dynamism in the process of extradition, shifting from

[2] See JERRY KAN & ANDREW MARTIN, DISTRIBUTED LEDGER TECHNOLOGY AND FINANCIAL CRIME 12-18 (2020).
[3] FIN. ACTIPN TAST FORCE (FATF), *GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS* 4-6 (2019).
[4] Helen Anderson, Dual-Use Technology and the Moral Status of Neutrality, 9 CRIT. REV. INT'L SOC. & POL. PHIL. 410 (2006).
[5] Marek Dabrowski, Regulatory Approaches to Cryptocurrency and Blockchain Technology, CEPS POL'Y BRIEF No. 121 (2018).
[6] KATE STOUT, *THE HISTORY AND DEVELOPMENT OF INTERNATIONAL EXTRADITION LAW* 45 (2d ed. 2018).
[7] DAVID J. BEDERMAN, *INTERNATIONAL LAW FRAMEWORKS 123* (4th ed. 2014).

ISSN: 2582-6433

merely diplomatic negotiations to internationally agreed-upon rules that also encompass human rights and procedural requirements. Major gaze has been towards the efficient legal system and procedural flow of a country, if poor, extradition becomes doubtful even when essential aspects of double criminality are fulfilled. Today, the system of extradition entails a balance of the two concepts: on the one hand, a state's sovereignty and, on the other hand, the requirements of transnational justice and accountability for the gravest crimes.

The double criminality principle essentially means that the behaviour which makes up the crime with which a person is charged should be a crime in both the country that gives the extradition request and the country that is going to execute it.[8] It has several purposes: it bars politically motivated prosecutions, thus political vetos being used as a substitute for justice; it provides fair notice of what conduct is considered criminal; and it honours the idea that punishment presupposes previous legal condemnation in the relevant jurisdictions.[9] On the other hand, the double criminality principle is based on the assumption that there is synchronised legal development in different jurisdictions, which is an assumption that is becoming increasingly challenged in the technology sector, where innovation is far ahead of legislation. Most countries have criminalised money laundering explicitly; however, only a few have explicitly dealt with the issue of liability for the developers of technology that can be used for money laundering.

The degree of criminality necessary for extradition differs from one jurisdiction to another. In some jurisdictions, the statutory elements must match exactly; however, in other jurisdictions, it is sufficient that the conduct in the essential elements is considered a crime under both legal systems.[10]This difference has resulted in a large number of judicial decisions on how deeply courts have to examine the facts in order to decide whether the double criminality principle is fulfilled. On the other hand, the majority of jurisdictions set a limit of the minimum severity: extradition is only applicable to crimes of a certain level of seriousness, and usually, it is minor offences that are excluded.[11]The logic is that extradition is an extraordinary use of state power which can potentially infringe human rights; therefore, it must be proportionate to the gravity of the alleged conduct.

In traditional criminal law, responsibility for an offence is attributed according to several well, known doctrines: principal liability (the perpetrator of the crime), accessorial liability (assist

[8] 18 U.S.C. § 3184 (2020); see also Gus Van Horn, Double Criminality in United States Extradition Law, 47 COLUM. J. TRANSNAT'L L. 306 (2009).
[9] Van Horn, supra note 19, at 310.
[10] Middlebrook & Hughes, supra note 2, at 675.
[11] See MODEL PENAL CODE § 1.04 (3d ed. 2021).

ISSN: 2582-6433

and encourage), conspiracy, and vicarious liability.[12]These doctrines are based on the assumption that there are direct human actors performing physical or verbal acts. For principal liability, it is necessary that the defendant knowingly committed the forbidden action. Accessorial liability entails that the defendant was knowledgeable of the principal's crime and intended to facilitate it.[13]Conspiracy entails that there is an agreement to a criminal objective and an overt act that is done to further the conspiracy. When these legal principles are applied to software developers, they become quite different. A developer may have written a code years before it was used for committing a crime, is not in direct control of the deployment decision, and may have legitimately expected non, criminal uses of their creation.[14]The time, cause, and intention links between development and unlawful application are so weakened that a serious challenge is raised as to whether the conventional liability doctrines properly reflect the responsibility of the developer.

B. Smart Contract- Based DeFi Protocols

Smart contracts are digital agreements that can self-execute. They are put on blockchains, and whenever certain conditions are met, they automatically carry out the terms of the contract.[15] So instead of a centralised intermediary being needed to execute the agreements, smart contracts take the contractual logic and embed it in software, thus parties can trust the code execution rather than having to trust the institution.

DeFi protocols are essentially a set of interconnected smart contracts that allow different kinds of financial transactions: automated market makers (AMMs) provide a way for tokens to be exchanged at prices decided by mathematical algorithms that take into account supply and demand; lending protocols allow borrowing against collateral and with automatic liquidation when the value of collateral falls, through the automation of these processes; liquidity pools gather the capital of many providers and distribute the returns accordingly and automatically based on the amount of trading fees.[16] This structure makes it possible to do highly sophisticated financial operations without anyone having to centralise control, thus making it possible for the financial transactions to be done peer, to, peer on a scale which has never been seen before.

[12] United States v. Fountain, 777 F.2d 287, 290 (5th Cir. 1986).
[13] 18 U.S.C. § 2(a) (2020).
[14] See Anderson, supra note 9, at 415-418.
[15] DE FILIPPI & WRIGHT, supra note 1, at 28.
[16] See Tal Z. Zarsky, Incompatible: The GDPR in the Context of the Internet of Things, 47 *ST. MARY'S L.J.* 297 (2016).

ISSN: 2582-6433

Once published on public blockchains, smart contracts, by and large, become immutable; that is, developers or any other party cannot modify or remove them.[17] This aspect of immutability has a number of significant roles: it gives users the confidence that the protocol will operate as intended, and it prevents the developers from unilaterally changing the protocol for their own benefit and to the detriment of the users. Users entrust large amounts of assets to DeFi protocols; immutability gives them the certainty that the code will not be altered after the fact to steal their assets or change the terms of their contracts. For instance, a user supplying liquidity to a liquidity pool has to be given assure that the formula used to calculate their share of the protocol fees will not be changed after the fact to the effect of lessening their compensation. Immutability is what makes such modifications technically impossible, and thus it provides this assurance.

A broader philosophical problem is under discussion that responsibility usually depends on having control, and without control, the onus of responsibility becomes ambiguous, therefore just because a system is immutable it does not in turn mean that someone can be held accountable for what it does. Modern criminal law usually holds that responsibility is dependent on the right to have control or influence over the behaviour at issue; thus, the basis of moral responsibility is the freedom to have acted differently.[18] If developers are not allowed to change the code after its release, they will be without the means of controlling the post-deployment behaviour, thus it will be doubtful whether it is correct, both from the point of view of philosophy and of morality, to hold them responsible for it.

Tornado Cash is perhaps the clearest illustration of such complications.[19]

The protocol acts like a mixer: users send cryptocurrency to a smart contract; the contract mathematically combines users' deposits; users then withdraw the same amounts from different addresses. The mathematically designed system makes it impossible to link depositors with withdrawals, even through a chain analysis method, thanks to a very sophisticated cryptographic method called zero-knowledge proofs.[20]

The protocol does not have any custodial features; the developers never have users' funds in their hands. Users, however, possess private keys that allow them to withdraw exactly their deposited amount.[21] On the one hand, the code itself does not demonstrate any intention to

[17] JERRY KAN & ANDREW MARTIN, supra note 5, at 25.
[18] Id.
[19] See Allison, supra note 3.
[20] See Nishith Desai, Emerging Issues in Data Protection and Cryptocurrency Regulation, 3 I*NT'L J. DATA PROT.* 202, 205 (2019).
[21] See id.

ISSN: 2582-6433

facilitate crime; on the other, it is not even capable of preventing legitimate use by its very nature. Depositors maintain complete ownership of their funds as well as the decision to withdraw at any time.

Defi protocols are a good example of distributed organisational governance frameworks. Leading-edge protocols have decentralised autonomous organisations (DAOs), where governance of the protocol is through distributed token holders rather than a few individuals.[22] Members of token holders make decisions through a voting process. Changes to the protocol, new feature launches, and a share of the protocol's income are all the results of decentralised voting. In such scenarios, it becomes very difficult to point out who is responsible: who runs the protocol when governance is scattered among thousands of token holders, most of whom are passive investors rather than active decision, makers?[23] Conventional criminal law has difficulties in determining who is liable if the decision-making power is truly distributed and not concentrated in the hands of a few individuals or a board.

CROSS-BORDER JURISDICTIONAL EVALUATION

A. United States – Stance On Developer Liability

The extradition law of the US is based on its Constitution, federal laws and extradition treaties. The Extradition Act of 1868 provides the basic legal framework, and the extradition treaties set the terms in an international forum.[24] Under their Constitution, via the Treaty Clause and Commerce Clause, Congress is solely authorised to regulate and formulate extradition law.[25] The US system highly focuses on dual criminality.[26] US courts have created a refined set of jurisprudence which allows one to look at the statutory elements instead of the statutory labels, thus they can decide whether double criminality is fulfilled or not. The prosecution theory put forward in the Tornado Cash case involves an extremely broad understanding of criminal liability in the US for software development, which will be discussed further.[27]

US courts have on several occasions recognised limits on liability for technology providers, such as in the case of is the Sony Corp. v. Universal City Studios, Inc.

[22] See HACKER, WERCHICK & HOLZWEBER, supra note 4, at 50.
[23] See Desai, supra note 35, at 210-212.
[24] U.S. CONST. art. IV, § 2, cl. 2; see also Extradition Act of 1868, 18 U.S.C. §§ 3181-3195 (2020).
[25] U.S. CONST. art. II, § 2, cl. 2 (Treaty Clause); id. art. I, § 8, cl. 3 (Commerce Clause).
[26] See United States v. Alcantara, 396 F.3d 224, 230 (2d Cir. 2005).
[27] See U.S. Dep't of Justice, Indictment, *United States v. Alexey Pertsev* (filed Aug. 2022).

ISSN: 2582-6433

B. United Kingdom Framework And Jurisprudential Caution

The UK has its own statutory framework (the Extradition Act 2003) implementing the European Convention and pre, 2020 European Union frameworks, as well as post-Brexit bilateral arrangements.[28] UK extradition law is also based on the requirement of double criminality and, in addition, it incorporates abuse of process protections.[29]

Traditionally, UK courts have been more cautious than US courts in extending liability doctrines to software development, as a matter of law, which reflects UK courts' general jurisprudential commitments to proportionality and protection of legitimate activity.[30]The Extradition Act 2003 places a requirement on the UK that extradition be proportionate to the seriousness of the charge. This gives UK courts the power to refuse extradition on grounds of disproportion even when the requirement of double criminality has been met.[31]

C. European Union - EAW System

EU member states function under an EAW (Extradition and the European Arrest Warrant) system.[32] This framework greatly reduces the restrictions on extradition by liberalising it compared to the old state, by, state negotiation model, thus creating quick procedures for extradition.[33]

EU anti-money laundering directives (in particular, the Fifth and Sixth Anti-Money Laundering Directives) set requirements for financial institutions and, even more and more, for entities that facilitate financial transactions.[34] These directives imply standards of knowledge: the institutions have to identify and report suspicious transactions.[35] The member states of the EU diverge significantly in the ways they deal with developer liability. German courts, relying on very strong free speech and freedom of expression doctrines protected not only under the German Constitution but also under the European Convention on Human Rights, have been quite hesitant to extend criminal liability to those providing neutral tools. [36]

The General Data Protection Regulation (GDPR) and Digital Services Act mark the shift of the

[28] Extradition Act, 2003, c. 41 (U.K.).
[29] Id. § 21.
[30] See generally R. v. Blackledge, [2005] EWHC 2888 (Admin.) (U.K.).
[31] Extradition Act, 2003, c. 41, § 21A (U.K.).
[32] See Extradition Act, 2003, c. 41, § 21A (U.K.).
[33] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures Between Member States, 2002 O.J. (L 190) 1.
[34] See UK-EU Trade and Cooperation Agreement, 2020 O.J. (L 444) 14.
[35] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, 2015 O.J. (L 141) 73.
[36] See German Federal Constitutional Court, NJW 2007, 1039.

ISSN: 2582-6433

EU towards regulatory and not criminal, only approaches to technology governance.[37]

D. Singapore's Proactive Regulatory Model

Singapore follows a regulatory model and not extradition-centric. The Monetary Authority of Singapore (MAS) has mapped out clear regulatory routes.[38] The Payment Services Act 2019, along with the related guidance set out direct regulatory requirements.[39]

Companies licensed under the Payment Services Act have to put in place full AML/KYC programs similar to those of conventional financial institutions. The regulatory method brings the benefits of establishing well-defined compliance requirements, offering developers the necessary guidance for lawfully conducting their business, and allowing the regulator to be agile in dealing with emerging threats.

Singapore's methodology seems to be that the act of providing services to Singapore users makes the service providers subject to Singapore's regulatory authority.[40] This principle is in line with extraterritorial regulatory assertions that are generally used in contemporary financial regulation, however, it questions the viability of its application to fully decentralised protocols that do not have any centralised service provider. In case a decentralised protocol is entirely run by smart contracts and token, holder voting, and there is no legal entity, no office, and no persons with regulatory authority, can Singapore still regulate the protocol or hold developers responsible for regulatory breaches?[41]

III. THE TORNADO CASH CASE STUDY

On August 8, 2022, Tornado Cash was added to the list of tools which were used for eluding sanctions by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), making it illegal.[42] This act stirred a controversial debate with the claim that the OFAC had no authority to designate software and hence could not be sanctioned under US law.[43] Following this the co-founder of Tornado Cash, Alexey Pertsev, was arrested and presented with an extradition warrant. His arrest was controversial as the protocol was legal in the Netherlands, and Pertsev was a leading developer in privacy-enhancing technologies. Pertsev's arrest was a clear illustration of how far the wings of the US prosecutors can go, as it has global implications

[37] See Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 1BvR 856/06 (Ger.).
[38] Monetary Authority of Singapore, Guidance on the Payment Services Act (2019).
[39] Payment Services Act, No. 62 of 2019 (Sing.).
[40] Monetary Authority of Singapore, supra note 78, at 15.
[41] See Allison, supra note 3.
[42] U.S. Dep't of the Treasury, supra note 8.
[43] See Allison, supra note 3.

ISSN: 2582-6433

for developers in countries which do not have extradition treaties with the US and also for developers whose actions are lawful at home. The charges were based on the claim that Pertsev deliberately joined a conspiracy to use Tornado Cash as a money laundering tool while being fully aware that the protocol would be used for criminal purposes.

Legal Issues:

First, if a developer knows that users may employ a protocol for criminal purposes, does that knowledge establish liability for all the criminal use facilitated through the protocol?[44] This question relates to how far conspiracy liability can be extended and what degree of foreseeability is required to establish liability. Second, can merely continuing to operate i.e., passively maintaining already deployed code, be considered an ongoing conspiracy?[45] Third, how much consideration should the courts give to the legitimate uses of a protocol?[46] Tornado Cash has allowed those in sanctioned regions to retain their financial privacy and has also been used by individuals to protect themselves against doxing and harassment.

The case furthermore sheds light on the matter of double criminality. The use of Tornado Cash by itself is not necessarily considered a crime in all locations. When Pertsev was arrested, the Netherlands had not made it illegal to operate a mixing protocol before the OFAC designation. According to Dutch criminal law, it is the user's act (laundering money) that is criminalised, not the supply of the means to that act. The shared custody of the protocol (co-sharing of the administrative functions among several developers) is another complication for the question of jurisdiction: which state's law applies when the acts are spread over several territories? If the developers had different job roles in different locations, which jurisdiction's extradition law would be applicable? If the protocol operation is spread out over several jurisdictions, how can any one of them claim exclusive authority to prosecute?

Firstly, the case shows that tech companies should not take for granted that being a mere provider of technology will protect them from being held liable if prosecutors and judges adopt a broad interpretation of facilitation of crime. Secondly, the case shows how US extraterritorial enforcement can influence developers worldwide and can even dissuade the creation of privacy-enhancing technologies in countries where such development is legal.

[44] See Anderson, supra note 9, at 418.
[45] See Pinkerton v. United States, 328 U.S. 640 (1946).
[46] See Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

ISSN: 2582-6433

IV. ATTRIBUTION THEORY AND DISTRIBUTED SYSTEMS

Conventional attribution theory in criminal law is based on separate and distinguishable actors whose actions lead to separate and distinguishable harms.[47] For example, if a person manufactures a weapon knowing that the weapon will be used to commit a murder, then liability comes from that knowledge and intent to facilitate the specific crime. This framework has been enough for physical crimes with identifiable victims and clear causal chains for hundreds of years.

DeFi protocols, on the other hand, pose a completely different problem when it comes to attribution.[48] The development of these protocols is usually a shared effort by many token holders. Various developers add code, govern protocols and deploy decisions at different times and are distributed rather than being individualistic.[49] Moreover, causation is also fragmented: the user's criminal conduct, not the protocol, is the direct cause of the harm; the protocol's creation is a more distant and less direct cause. A developer who coded a piece of software several years ago without knowing the specific applications is significantly different from a person who is actively facilitating criminal transactions. Extending attribution theory to include distributed systems entails major changes to the theory. One of the changes is that the theory should clearly identify primary actors as the ones whose conduct directly causes the harm and secondary actors as those whose earlier conduct through their behaviour has created the conditions enabling the harm. Second, we must develop causation frameworks that recognize weakened causal chains.

Between the deployment of the code and the year of its criminal use, several years may pass. Causation, however, does not weaken entirely; the protocol would not be used for laundering without the developer's code, but it is weakened.

Thirdly, on the question of whether knowledge standards ought to differ based on time and control factors, we need to give it a thought as well.[50] Attribution theory in the present day is increasingly acknowledging that the extent to which one is held responsible should be in proportion to one's control and involvement in the harmful act and it can be extended to those

[47] Mark F. Grady, Duty of Care and the Demand for Tort Reform, 30 *VAL. U. L. REV*. 465 (1996).
[48] See Ben-Shahar & Porat, supra note 15, at 1110.
[49] See DE FILIPPI & WRIGHT, supra note 1, at 45.
[50] See FRANKFURT, supra note 32, at 835.

ISSN: 2582-6433

who join the conspiracy but not those who are completely unaware of its existence.

These theoretical refinements indicate that DeFi developer liability should not simply be based on accessorial liability doctrines but necessities, intricately developed, a framework attending to: temporal gap, availability of technical measures, knowledge, nature of attribution being direct and whether the tool in question has lawful uses.

V. DOUBLE CRIMINALITY IN DeFi CONTEXTS

Double criminality raises the issue of which specific standards are used in the enforcement of the same offence in different jurisdictions. There are, firstly, differences in the definition, coverage and severity of money laundering crimes in various legal systems. The US approach is defined very broadly, making all financial transactions involving proceeds of a crime covered. The European Union has issued directives which set the minimum standard for anti-money laundering compliance across member states. Other jurisdictions keep their standards low and focus on the aspect of intentional concealment of proceeds.

Tornado Cash developers may get prosecuted in the US under money laundering laws, but they have no similar liability in the Netherlands, where the protocol was created.[51]

As countries clarify their laws on DeFi protocol liability, the alignment of double criminality standards is becoming a key issue.[52] If country X considers it a crime to develop protocols that might be used to launder money, but country Y doesn't, then the extradition between these countries is legally difficult unless both agree explicitly on the liability standards. The lack of harmonisation leads the liability standards to be conflicting and the enforcement to be arbitrary. Even for the same actions, developers may be held liable criminally in some countries but be completely exempt in others. This situation brings about, on the one hand, incentives for regulatory arbitrage and, on the other hand, migration to jurisdictions which are more developer, friendly.

[51] See Wetboek van Strafrecht [Dutch Criminal Code] art. 9.(Neth.).
[52] See JERRY KAN & ANDREW MARTIN, supra note 5, at 40.

ISSN: 2582-6433

VI. POST-DEPLOYMENT CONTROL AND SMART CONTRACT IMMUTABILITY

A significant characteristic of numerous DeFi protocols is their immutability: the code of the smart contract, once it is deployed, cannot be altered or deleted by developers at their own discretion.[53] Such immutability plays a key role, it gives the users trust in the protocol functioning correctly and stops the developers from changing the protocols arbitrarily in an unfair way to users. Users may lock up their funds worth millions in DeFi protocols; therefore, the assurance that the protocols will run as deployed is vital for their willingness to join. If there were no immutability, the users would always be under the threat of the developers changing the protocols in a way detrimental to them. Still, immutability does make liability analysis less straightforward. Philosopher Harry Frankfurt maintained that moral responsibility entails being able to do otherwise.[54] If the developer is not allowed to change the code after deployment, then they do not have the power to control post, which in turn raises the question of whether responsibility for such behaviour is in line with philosophy and morality.

Nonetheless, this concept doesn't completely protect developers from being held liable. A refined framework breaks down the developer's liability into three distinct stages: (1) liability for deciding to deploy the system initially, a decision that developers have full control over; (2) liability for changes in the system after deployment, a situation in which developers might be lacking in control; and (3) liability for the direct involvement in facilitation of particular criminal acts, which developers cannot do after the system deployment.[55] According to this framework, the developer's liability for the use of the system in crimes after the deployment doesn't derive from the post-deployment conduct (which the developers can't control) but from their initial decision to deploy with the knowledge of the probable criminal usage a system that is beyond their control and capability to modify. This is the liability for the deployment decision, not for the subsequent criminal use. This method moderates the developers' responsibility for conscious decisions to deploy against the fact that developers cannot control post-deployment conduct.

[53] See JERRY KAN & ANDREW MARTIN, supra note 5, at 40.
[54] See FRANKFURT, supra note 32, at 835.
[55] See id. § 2.02.

ISSN: 2582-6433

VII. STANDARDS OF INTENT AND KNOWLEDGE

There are four categories of liability under tradition criminal law namely: strict liability, negligence, recklessness and specific intent .[56] But where on this spectrum should DeFi developer liability be?

If strict liability is the standard, then developers will be exposed to prosecution even if they had no ill, intent when developing a technology that can be or might be used for crime. Negligence standards will hold liable developers who could have foreseen their technology being used for crime but didnt prevent it. Recklessness standards will catch developers who knowingly disregarded the risks. Specific intent standards will make the prosecuting party prove that the defendant planned to commit the crime through the help of the developer.

The prosecutorial theory behind the successful Tornado Cash case appears to be an figuring out of the knowledge standard: Pertsev allegedly knew that his protocol could be used for money laundering and he intended to provide a tool for that purpose.[57]The prosecutor's need to establish these two elements: developer's actual knowledge that users will commit crime through the use of the protocol;[58]intent to commit that criminal act. Such elements are extremely difficult to meet and mainly the direct evidence or very strong circumstantial evidence of the doer's actual state of mind would fulfill the standards. However, knowledge and intent in the context of decentralised systems present difficult issues.

Firstly, a developer is aware that a plethora of illegal activities are undertaken every day in almost all jurisdictions, but is such an awareness of criminals enough to establish knowledge of the likely use of one's specific creation by criminals? Similarly, intent becomes ambiguous: a developer may intend to develop a privacy, protecting tool without intending to facilitate crime by the tool. The developer's goal may be to promote financial privacy as a public good, rather than to allow money laundering. In order to conclude a developer is aware of or intends to facilitate criminal use, it is necessary to carefully differentiate between knowledge that crime might take place and intent to help the crime from the mere fact that one provides a privacy, enhancing technology.

[56] See MODEL PENAL CODE § 2.02 (AM. L. INST. 2021).
[57] See U.S. Dep't of Justice, supra note 42.
[58] Id.

ISSN: 2582-6433

One reaction involves a focus on the developer's intent: if the developer's main objective is to create a tool that enables Financial privacy legally, then being aware that the same tool can be used for crime is not enough to make the developer guilty.[59]

This method, giving more weight to the legitimate purpose, stems from US technology law and DMCA case law, which differentiate between the tools that are primarily intended for legitimate uses and the ones that are specifically designed to be used for circumventing protections.

According to this line of argument, the developer's purpose is the deciding factor. Courts would assess whether the developer's leading intention was to make a privacy, enhancing protocol or to facilitate money laundering.

One alternative method uses a negligence or recklessness standard: developers should be blamed if they ought to have foreseen a criminal use or consciously ignored the risk of such use.[60] This criterion is less strict, it does not require proof of specific intent or actual knowledge of particular crimes, only reasonable foresight of probable criminal misuse. This method greatly increases liability as most developers might foresee that any technology could be misused. Nevertheless, it gives prosecutors more flexibility in proving liability without the need for proof of specific intent.

Which standard jurisdictions adopt will largely determine the extent of developer liability.[61]Strict intent requirements allow greater protection for legitimate innovation; negligence standards, on the other hand, significantly extend liability. International harmonisation should be based on intent, based on standards, which protect innovation while ensuring that developers with eyes wide open are held responsible. A reasonable standard should ideally include: knowledge that the protocol can be used for money laundering, intent to facilitate the same or conscious disregard of a sufficient risk that the protocol could be used for illegal financial transactions.

[59] See Ben-Shahar & Porat, supra note 15.
[60] See id.
[61] See Dabrowski, supra note 14.

ISSN: 2582-6433

VIII. ESTABLISHING TERRITORIAL NEXUS IN BORDERLESS DIGITAL CRIMES

Traditional extradition law is about who owns the land where the crime happened; so, generally, a state's power to regulate is limited to the territory where the conduct first occurred.[62] However, DeFi protocols are functioning worldwide through public blockchains, which are reachable and thus localizable from each and every place, but simultaneously are, in the very same way, in all and no place at the same time (considering that blockchain data are replicated several times over geographically dispersed nodes). Therefore, the question arises as to which state has the right to prosecute a developer who provides code that enables illegal activities (depending on the specific cases) that may be happening in several different jurisdictions at the same time?[63]

There are several ways to establish sufficient nexus to justify extradition: A first way, the passive personality principle, may allow for jurisdiction when the victims are the citizens of the prosecuting state.[64]A second way, the protective principle may allow for jurisdiction when the crime hits the state's financial system. A third way, the universality principle, may allow for jurisdiction due to the nature of the crime.[65] Money laundering is gradually being considered to be a universally condemned crime, which thus gives a justification for a wide jurisdiction. A fourth way, the effects doctrine, may allow for jurisdiction when a state experiences the effects of the crime within its territory.

Each principle, however, when applied to distributed systems, has its drawbacks.[66] The passive personality principle entails finding the victims, but money laundering victimizes entire financial systems rather than specific individuals. The protective principle entails showing that the state's interests have been harmed, which is difficult when a protocol is being misused on a global scale. The universality principle gives the possibility to different jurisdictions at the same time to request extradition for the same conduct. Thus, several states may concurrently claim jurisdiction based on universality which can lead to duplicate prosecutions and inconsistent sentences.

[62] See Van Horn, supra note 19.
[63] See Anderson, supra note 9.
[64] See BEDERMAN, supra note 18.
[65] See M. CHERIF BASSIOUNI, INTERNATIONAL CRIMINAL LAW 234 (3d ed. 2008).
[66] See JOEL P. TRACHTMAN, THE STRUCTURE OF INTERNATIONAL LAW 78 (2013).

ISSN: 2582-6433

A preferable approach that is more satisfying to the parties involved determines a nexus by a significant connection between the developer's activities and the state of the prosecutor.[67]The developer's actions that may have brought the state into crime could be, for instance: (1) the developer deliberately targeting the users of the state;[68] (2) the developer having a considerable presence or contacts in the state;[69] (3) a great part of protocol abuse being done in state's territory;[70](4) the crime having a major effect on the state's financial system.[71]These standards maintain legitimate jurisdiction, and at the same time, they avoid the problems of forum, shopping and multiple prosecutions. Besides, they encourage international cooperation rather than unilateral enforcement action. This method compels prosecutors to prove that the extradition is in line with the legitimate interests of the requesting state and not simply that of a prosecutorial opportunist.

On the other hand, extradition treaties could stipulate that in the case of software-based crimes, extradition is only possible when the accused has been involved in the targeted conduct directed at the state's citizens or institutions.[72] This would stop extradition being solely based on the worldwide availability of the software, but would, however, allow extradition if the developer targets a state's financial system or its citizens specifically.

IX. BALANCING INNOVATION, PROTECTION AND CRIMINAL ACCOUNTABILITY

A fundamental contradiction runs through the evaluation of developer liability in the DeFi context:

On the one hand, society benefits from innovation, including financial technology innovation, but on the other, it needs to be protected from the criminal misuse of technology. Overextension of developer liability could deprive us of future innovations. At the same time, if developers are granted liability exemptions, they may enable criminal activities without any repercussions. Determining the right balance therefore entails great delicacy in reconciling these different values. One can learn from the history of technology law that an overreaction to the liability of the victim could seriously delay the delivery of the technology.

[67] See JOEL P. TRACHTMAN, THE STRUCTURE OF INTERNATIONAL LAW 78 (2013).
[68] See Dabrowski, supra note 14.
[69] See id.
[70] See id.
[71] See id.
[72] See Middlebrook & Hughes, supra note 2.

ISSN: 2582-6433

The European Union has similarly tried to solve such tensions in the area of telecoms and internet law. The eCommerce Directive and the case law that followed draw a line between hosting providers (who are basically neutral and thus deserve the most protection) and content providers (who are at the same time editors and thus less protected). This distinction allows tech companies to provide the necessary infrastructure while at the same time keep incentives for content supervision. Those service providers who merely host user content without changing it in any way are given immunity for such content; on the contrary, platforms that intervene or control the content have to bear greater responsibility.

When the distinction is applied to DeFi, it becomes a problem.[73]On the one hand, DeFi developers are not purely passive, on the other, they are not purely active either. They write code (active conduct) and then publish it (decision with consequences), but they do not exercise any control thereafter (passive role).[74]The traditional intermediary doctrines are not fit to describe this middle ground. Thus, new doctrinal frameworks need to accommodate the peculiarities of open, source software development and decentralised protocol governance.

A more refined view acknowledges that certain protocols are built with major legitimate purposes in mindand some mainly for illicit ones.[75] A money mixing service that helps both legitimate users protecting their privacy and criminals laundering money is a very different entity from one that was purposely designed to steal funds or to enable Ponzi schemes.

This differentiation allows for regulation that is in line with the protocol's real design and intent. Protocols that have significant legitimate purposes can be treated differently from those that are designed solely for crime.

Real elements that need to be considered in weighing this balance are: whether the industry acknowledges the protocol to be a legitimate tool in several use cases;[76] the presence of technical controls capable of limiting the illicit uses;[77] whether developers comply with the requests for the information from regulatory authorities; the extent of criminal use versus

[73] See HACKER, WERCHICK & HOLZWEBER, supra note 4.
[74] See id.
[75] See Anderson, supra note 9.
[76] See Desai, supra note 35.
[77] See FATF, supra note 6.

ISSN: 2582-6433

legitimate use; developer actions aimed at stopping known criminal use.[78] These elements allow determining if the protocol is genuinely intended for legitimate services or whether it only presents a legitimate purpose while being essentially a crime tool. A protocol with strong legitimate uses should be treated differently in terms of liability exposure compared to a protocol where criminal use is predominant.

This method allows for the accountability of developers who intentionally aid crime; at the same time, developers of protocols with significant legitimate purposes are protected from developers' liability.[79] Besides that, it provides developers with the motivation to adopt technical features to prevent foreseeable criminal misuse, e.g., sanctions screening, without the need to completely remove criminal potential that, from the technical standpoint, may be impossible. Developers who take reasonable precautions and respond to requests for information should be accorded more protection than those who disregard problems related to criminal misuse.

X. RECOMMENDATIONS

A. Global Harmonisation-

The development of international standards for DeFi developer liability should be an effort of multilateral cooperation.[80] The Financial Action Task Force (FATF) has taken the first steps in handling cryptocurrency issues,[81] and similar groups may be able to coordinate the development of agreed standards for developer liability.[82] International harmonisation would give developers clear guidance on what is allowed in different jurisdictions. A lack of international harmonisation results in regulatory arbitrage incentives, where developers move to jurisdictions that offer greater legal certainty and less liability exposure. Areas to focus on harmonisation include: mentioning the standard of intent needed for developer liability, universal standards for assessment of double criminality, post-deployment control effects on liability, and methods for the determination of territorial jurisdiction. It is permissible for different jurisdictions to have different approaches to dealing with their affairs as long as these differences reflect diverse values instead of creating arbitrary enforcement disparities.

[78] See id.
[79] See Ben-Shahar & Porat, supra note 15.
[80] See FATF, supra note 6.
[81] See id.
[82] See id.

ISSN: 2582-6433

B. Domestic Legislative Reconfiguration

Discussions on developer liability should be made more accessible through explicit statutory frameworks in each jurisdiction rather than through prosecutorial interpretation of the existing statutes.[83]The frameworks should set out: specific behaviour qualifying for liability[84]; necessary mental state and intent[85]; defences available to the developers (e.g., good faith in legitimate purpose, compliance with the known law, etc.)[86]; creation of safe harbours for developers who are executing legitimate technical controls to avoid the foreseeable misuse.[87]

Legislation should make a distinction between various types of DeFi protocols based on their design characteristics and recognised legitimate use cases, [88]thereby granting more protection to those protocols whose main purposes are for legitimate uses. Statutory frameworks would be aware of the fact that not all protocols are equally likely to be misused in crimes.

C. Development Of Regulatory Framework

Instead of criminal liability only, jurisdictions should lay down coherent regulatory frameworks that address DeFi protocols.[89] Such regulatory frameworks should set out: under what circumstances DeFi protocols become regulated financial services;[90] the compliance duties of protocol developers (KYC, AML, transaction monitoring);[91] and administrative sanctions for non-compliance, as an alternative to criminal prosecution.[92]

A regulatory approach works well and serves to give developers a lot more clarity and certainty in respect of their compliance obligations. Regulatory frameworks might set up a system of escalating requirements that are based on the design features of the protocol and the risks that have been identified.[93]

D. Extradition Treaty Reform

Extradition treaties need to be updated to cover technology, related problems, for example: clear standards for determining the territorial connection to a crime in cases of borderless digital crimes; advice on the double criminality test when the same conduct is criminal in one state

[83] See Middlebrook & Hughes, supra note 2.
[84] Id.
[85] Id.
[86] See MODEL PENAL CODE § 2.02 (3d ed. 2021).
[87] See FATF, supra note 6.
[88] See Desai, supra note 35.
[89] See Dabrowski, supra note 14.
[90] See Payment Services Act, No. 62 of 2019 (Sing.).
[91] See Monetary Authority of Singapore, supra note 78.
[92] See id.

ISSN: 2582-6433

but not in another; methods for dealing with successive requests for extradition from different states; the use of international assistance in the investigation of distributed, development protocols. Most of the modern extradition treaties that were made in the twentieth century do not properly deal with digital crime, which is, by its very nature, a crime that is done without regard to any territorial limitations. The language of the updated treaty would take into account the technological aspects without thereby compromising the protection of human rights.

XI. CONCLUSION

The fast growth of decentralised finance has led to new extradition laws and developer liability issues. Existing legal systems are based on certain assumptions, single, identifiable actors with control, physical actions causing clear harms, criminality across different jurisdictions happening at the same time, that are difficult to apply to distributed systems and immutable code. The prosecution against Tornado Cash shows that courts are slowly starting to engage with these problems by using very broad theories of prosecution, which may, however, not survive judicial review.

Nevertheless, these problems should not be used as an argument against legal liability. On the contrary, they require that we develop more sophisticated frameworks that are able to capture the features of distributed systems. It is not necessary for responsibility to be based on control if it can be based on the decision to use systems that one cannot control, with the knowledge that such systems will probably be used for criminal purposes. Attribution doesn't need to be perfect if it mirrors realistic causal chains. Jurisdiction does not have to be purely territorial if it is a tool that reflects a significant connection between the defendant and the prosecuting state.

The Tornado Cash case is just the beginning of a lengthy court battle that will define the developer liability in the DeFi era. The case is both ominous and promising. The positives are that developers can be held responsible if they knowingly facilitate crimes through decentralised systems. The downsides are that over, criminalisation can stifle genuine innovation and developers can find themselves in legal trouble if they develop tools with a significant legitimate use. Here, the legal decision will largely determine the path of DeFi development and how willing developers around the world are to innovate in fin, tech.

Since blockchain is poised to play an increasingly important role in the world financial landscape, the legal frameworks around developer liability will determine not just the future of

ISSN: 2582-6433

the crypto sector but the overall pace of tech innovation. Code cannot serve as a shield for developers against accountability if they knowingly facilitate transnational crime.

At the same time, developers shouldn't be treated as criminals by legal frameworks just because they create tools that can be misused. In fact, the main task of the law in the near future is to wisely and prudently balance the response between the two extremes while paying close attention to the special features of decentralised systems. It is only through continuous cooperation among the legislators, judges, prosecutors, technologists, and policymakers that legal frameworks can be developed which both protect innovation and guarantee accountability.