THE CASE FOR ON-CHAIN PRIVACY AND COMPLIANCE

Shlomit Azgad-Tromer, Joey Garcia, Eran Tromer*

ABSTRACT

Recent trends in financial-regulation compliance of blockchain-based assets ("crypto"), including by the European Union and the U.S. Treasury, reflect regulators' belief that policy frameworks and regulatory regimes designed for financial intermediaries can be effectively implemented to police the decentralized, software-mediated cryptocurrency markets. Furthermore, a principal tool relied upon to manage the risk of illicit financial transactions in these markets is blockchain analytics, which depend on blockchains' transaction ledgers being transparent.

This paper argues that while these two core premises—intermediary regulation and blockchain transparency—play an essential role in mitigating illicit financial risk in the current environment, exclusive reliance on them raises critical questions that must be addressed as cryptocurrency markets enter mainstream adoption.

In traditional financial services, the tension between privacy and compliance is addressed by trusted intermediaries, who maintain private information silos that (when operating as intended) protect customers' privacy by default. In addition, financial privacy rights enjoy statutory and regulatory protections within these financial intermediaries, giving rise to operational controls restricting access to personal financial information (albeit imperfectly, as reflected in persistent cybersecurity incidents). In light of this default-privacy, compelled disclosures to regulatory agencies and law enforcement support efforts to combat sanctions evasion, terrorist financing, money laundering, and other illicit financial activity.

However, in decentralized finance, such trusted intermediaries do not always exist. The vision of decentralized finance is based on peer-to-peer mechanisms that allows users to transact without the involvement of banks or other financial institutions. Intermediary regulation thus does not address the need to regulate blockchain-based finance: it leans on assumptions rooted in the traditional financial world.

Moreover, in contrast to this default privacy and compelled transparency of traditional financial services, cryptocurrency markets

operating on most public blockchains are transparent by default. Historically, this transparency stems from a technical consideration: it allows the blockchain consensus rules (e.g., preservation of monetary invariants) to be easily verified. Subsequently, this public transaction data has been utilized for additional purposes, including detection of illicit activity via blockchain analytics. However, this default-transparency raises heightened risks to consumers. Transparency and immutability allows anyone with an internet connection to see the full transaction history and net holdings of any wallet holder. Absent the type of privacy protections—both practical and legal—that exist in the traditional financial system, it is not surprising that even legitimate users would employ privacy-preserving technologies like mixers to obfuscate their identity and hide their transaction history from prying eyes, without any intent or desire to engage in illegal activity. Indeed, just as law-abiding citizens and corporations strive to protect their privacy in other contexts, the use of privacy-preserving tools in cryptocurrency context may be considered a cybersecurity best practice. Moreover, imposing the same customer identification requirements (designed to overcome the default-privacy of traditional financial services) in cryptocurrency context raises heightened risks in this environment, because of its diversified nature and the ability to correlate this data with on-chain data.

Financial confidentiality and protection of personal information is necessary for widespread adoption of blockchain-based payments for personal and commercial uses. Thus, the reliance on blockchain analytics as a tool for compliance reflects a fundamental tension at the heart of cryptocurrency markets as they currently function: between the needs of consumer privacy and cybersecurity, on the one hand, and the public interest in preventing illicit financial activity, on the other.

The key question raised by this dynamic is whether it is possible to create privacy-enhancing technologies that protect legitimate customer privacy while simultaneously providing regulators and law enforcement a way of combating illicit financial risks. We believe that the answer is yes. The paper argues that advances in cryptography and blockchain technology have the potential to overcome the false binary choice between privacy and compliance, through blockchain-native solutions that permit on-chain compliance that is programmable and tailored to jurisdictional needs and enforced by consensus rules. We discuss the contours of this blockchain-native, on-chain compliance and its potential to strike a healthy balance between privacy and compliance in the crypto ecosystem.

1. INTRODUCTION

In October 2022, a bankruptcy filing by Celsius, a digital asset lending platform, revealed the names and transaction history of nearly half a million depositors. The Celsius case illustrates a risk that arises from the transparency and traceability of the blockchain. The privacy standard in most public blockchains is based on pseudonymity, which can be easily pierced to track user activity and balance. As a result, data leaks of names and wallet addresses can cause privacy harms to blockchain users, since anybody with an internet connection can easily match the on-chain activity and wallet addresses of named Celsius users disclosed in the filing with the dates and amounts of every transaction on their wallet, exposing wallet owners to the risk of theft or extortion.

As a practical matter, such data leakages can also occur simply by transacting with another party who knows your identity. Consider for example using crypto in your payroll, where employees can see the employer's account balance and the paycheck of their team members; exposing trading methodologies to your competitors, or simply exposing the local coffee shop to visible information on how much you make and where you shopped yesterday.

To mitigate this risk, digital asset holders employ additional privacy enhancing technologies to protect confidentiality of their financial information. The problem is that current techniques to manage illicit finance risk on blockchains rely on transparency and traceability in order to assess user identity. As a result, the same tools used to protect legitimate privacy interests on public blockchains can also frustrate government investigations into malicious activity.

But privacy in blockchain is fraught with legal risk. In August 2022, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned the virtual currency mixer Tornado Cash in accordance with Executive Order 13694, claiming it has been used to launder more than $7 billion worth of virtual currency since its creation in 2019.[1] Specifically, OFAC alleged that Tornado Cash had been used for illicit transactions by facilitating anonymous transactions and obfuscating their origin, destination, and counterparties, "with no attempt to determine their origin" of the transaction. "While the purported purpose is to increase privacy," the US Treasury wrote in its press announcement, "mixers like Tornado Cash are

---

* Shlomit Azgad-Tromer is Chief Executive & Chief Legal Officer, Sealance Corp.
Joey Garcia is Director and Head of Legal and Regulatory Affairs, Xapo Bank; Consultant to the United Nations.
Eran Tromer is Associate Research Scientist, Columbia University; Chief Technology Officer, Sealance Corp.
The authors thank Jai Ramaswamy for fruitful and insightful discussions.
[1] U.S. Department of the Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

commonly used by illicit actors to launder funds, especially those stolen during significant heists…Tornado receives a variety of transactions and mixes them together before transmitting them to their individual recipients."[2] With a similar rationale, the European Parliament approved in April 2023 a landmark piece of legislation for crypto markets titled "Markets in Crypto-Assets" ("MiCA"),[3] scheduled for final legislative approvals by July 2023. In Article 68, MiCA requires trading platforms for crypto-assets to prevent the trading of crypto-assets which have inbuilt anonymisation function, "unless the holders of the crypto-assets and their transaction history can be identified by the crypto-asset service providers that are authorized for the operation of a trading platform for crypto-assets or by competent authorities."[4]

The positioning of anonymity and privacy as tools for illicit finance without acknowledging their importance for preserving privacy and enhancing consumer protection on transparent blockchain should be cause for significant concern. In this essay, we argue that the apparent clash between privacy and compliance can and should be overcome using technological advances that harness the power of the blockchain to enforce compliance in a manner that will sustain financial confidentiality and privacy for consumers and users, while providing law enforcement and regulators the tools required to enforce compliance, view suspicious information and prevent illicit activity with selective disclosure designated to specific authorized agents. These emerging technologies could serve to strike a better balance between national security, crime prevention and the fight against illicit finance, on the one hand, and the right to privacy, on the other, by harnessing blockchain technology.

The essay identifies two fundamental premises of financial regulators in designing regulation for crypto markets and argues that—although useful—they face limitations as crypto markets, and the associated decentralized network services ("Web3"), mature.

First, financial regulators rely on the gatekeeping role of financial intermediaries, and as a result appear to insist on mandating that these intermediaries continue to exist in decentralized financial networks. This approach threatens to expand the definition of financial intermediaries—with associated regulatory responsibilities and liabilities—to parties that

---

[2] *Id.*

[3] LEGISLATIVE OBSERVATORY (EUROPEAN PARLIAMENT), DIGITAL FINANCE: MARKETS IN CRYPTO-ASSETS (MICA), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/0265(COD).

[4] *See* Gary Weinstein, *Blockchain Privacy is at Risk in the EU*, COINDESK (Feb. 9, 2023) https://www.coindesk.com/consensus-magazine/2023/02/09/blockchain-privacy-is-at-risk-in-the-eu.

have neither the required information nor the ability to carry out the required regulatory responsibilities, resulting in a *de facto* prohibition on decentralized blockchain networks.

Second, financial regulators rely on the weakness of blockchain transaction privacy, as utilized by blockchain analytics and associated heuristics, as a key tool for compliance. This reliance leads to a suspicion that privacy-preserving technologies serve as means to facilitate illicit financial activity. Recent examples of these trends include the actions against Tornado Cash, but also the Virtual Asset Guidance published in October 2021 by the Financial Action Task Force, several stablecoin and digital asset bills being considered by the U.S. Congress, and most recently MiCA's aforementioned Article 68. Additional jurisdictions are likewise considering how to bring digital assets within the regulatory perimeter that applies to financial services, and often default to these same two approaches: financial intermediation and blockchain transparency.

The essay posits both these assumptions are not adequate for the permissionless and decentralized ecosystem of Web3. Privacy is a fundamental constitutional value, and should not be presumed illegitimate simply because current compliance methodologies rely on transparency and heuristic based surveillance. Likewise, the search for financial intermediaries as agents of legal enforcement in a disintermediated financial system (which replaces intermediaries with direct communication and programmatically-enforced consensus rules), is misguided and doomed to fail.

This essay further discusses how, because of these assumptions, current regulatory frameworks lack the ability to address permissionless environments that characterize the emergence of Web3. It describes the ability of emerging technologies to address the risks correctly identified by relevant authorities and policy makers by adopting the same consensus principles that underlie blockchain technology to programmatically enforce compliance obligations on-chain. The essay concludes by discussing the merits of such programmable on-chain compliance as a rule-based, blockchain-native approach to crypto compliance as well as its potential limitations.

2. HOW CRYPTO COMPLIANCE WORKS TODAY

Illicit-finance regulatory compliance in the crypto space is, at present, an attempt to replicate the anti-money laundering regulation of traditional finance. The first anti-money laundering regime to arise was developed in the US and is referred to as the Bank Secretary Act ("BSA"), a series of U.S. statutes and regulations that emerged in the 1970s, have evolved over the intervening years, and were most recently revised through the U.S. PATRIOT Act. Legislated for a financial system managed by

intermediaries, the BSA's initial purpose was to ensure that banks would collect information about their customers (and their customers' counterparties and transactions) that would provide law enforcement with information designed to provide intelligence for prevention of crime. The BSA establishes reporting and record-keeping requirements for regulated banks and Money Service Businesses (MSBs), including the filing of suspicious activity reports (SARs) with FinCen, a bureau within the United States Treasury Department that serves as the U.S. financial intelligence unit and principal AML regulator. A core tenet of the tenet of the record keeping and reporting requirements of the BSA is the obligation for money service businesses to have a Customer Identification Program and for banks and other financial intermediaries, in addition, to conduct Customer Due Diligence (CDD), colloquially referred to as "KYC" or "know your customer" rules. This regime relies on the existence of so-called "gatekeepers" responsible for confirming and validating the identity of participants, as well as detecting and preventing illicit financial activity. The BSA's implementing regulations require a custodial relationship with customers to be covered as a money service business with BSA obligations. The BSA also contains carve-outs for software providers. As of the date of this publication, FinCEN has not taken the position that unhosted wallets or non-custodial smart contracts are money service businesses. In its recent Illicit Finance Risk Assessment on Decentralized Finance, the Treasury Department did caution that "[i]n cases in which a DeFi service falls outside the scope of the BSA, this can result in gaps in suspicious activity reporting, and limit authorities' collection of and access to information critical to supporting financial investigations."

In the following, we identify why the two approaches to regulating Web3 with respect to illicit finance—the search for intermediaries in a decentralized environment, and the assumption of continued blockchain traceability and transparency—are flawed and warrant a new approach.

2.1 The Search for Intermediaries

Current financial regulations addressing illicit financial activity target financial intermediaries responsible for performing critical aggregation and settlement functions on behalf of customers. Since these financial intermediaries maintain their transaction records on private, internal ledgers, modern financial regulations have placed obligations on them to ensure customer protection, and for purposes of this paper act as gatekeepers to detect and prevent illicit financial activity. To comply with these regulatory obligations, financial institutions implement regulatory requirements through policies, internal compliance controls and monitoring processes. Recognizing that Web3 disintermediates the provision of financial services, current regulatory approaches have begun to stretch the definitions of

financial intermediaries beyond their traditional scope. However, as we discuss further below, such approaches will generally operate as a de facto prohibition on these technologies since the alternative intermediaries identified typically do not possess the information to comply with relevant obligations or are ill-suited to regulatory compliance because they are functionally very different from traditional financial intermediaries.

A. FATF's definition of a VASP

A recent example of such efforts is the revisions to the Virtual Asset Guidance published in October 2021 by the Financial Action Task Force ("FATF"), a global standard-setting body for Anti Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations.[5] The October 2021 updated Guidance followed the original FATF Interpretative Note to Recommendation 15 (INR. 15) on New Technologies published in June 2019, which was widely recognized and acknowledged as a significant step in the development of standards in the blockchain-based "virtual assets" space. These updates were also welcomed by the United Nations Security Council in Resolution 2462 of March 2019,[6] which called on Member States to assess and address the risks associated with virtual assets, and encouraged Member States to apply risk-based anti-money laundering and counter terrorist financing regulations to Virtual Asset Service Providers ("VASPs") and to identify effective systems to conduct risk-based monitoring or supervision of VASPs.

The Guidance was designed to ensure that countries apply the same (or higher) standards of AML/CFT to VASP-related activity as those applied to regulated financial services institutions operating in the traditional financial world. The approach taken by FATF mimics the models of compliance in traditional finance, expanding the definition of intermediary entities upon which to impose regulatory responsibilities in a decentralized world.

The Guidance defines a VASP[7] as "any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. Exchange between virtual assets and fiat currencies; ii. Exchange between one or more forms of virtual assets; iii. Transfer of virtual assets; Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v.

---

[5] THE FINANCIAL ACTION TASK FORCE (FATF), UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, (Oct. 28, 2021), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

[6] S.C. Res. 2462, (Mar. 28, 2019), https://www.un.org/securitycouncil/content/sres24622019.

[7] FINANCIAL ACTION TASK FORCE, *supra* note 5.

Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset." VASPs are subject to various AML and countering the financing of terrorism obligations including licensing and registration, implementation of effective systems for monitoring or supervision by their jurisdictions,[8] including a duty "to implement an effective control framework to ensure that they can comply with their targeted financial sanction obligations."[9]

It then goes on to encourage bringing within the regulatory perimeter of AML/CFT regimes "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized.[10] Furthermore, even if a DeFi protocol has no such party at *present*, the FATF guidance looks *back in time* to whether there may be "at least some party involved at some stage of the product's development and launch that constitutes a VASP," by previously "automating a process that has been designed to provide covered services."[11]

The Guidance had been amended from a proposed draft Guidance issued by FATF for consultation in March 2021,[12] whose expanded definition included any person who "facilitated" an activity—and which would have been wide enough to arguably capture any developer or person involved in any aspect of an activity in the virtual assets space, even if they did not directly "conducted" the activities activity. The use of the word "facilitation" was met with broad opposition from the industry, and resulted in the final language eventually issued. While an improvement on the original proposed language, the draft Guidance explicitly explained that "the expansiveness of these definitions represents a conscious choice by FATF [which] envisions very few VA arrangements will form and operate without a VASP involved at some stage. Where customers can access a financial service, it stands to reason that some party has provided that financial service."[13]

Under the FATF Guidance, owners/operators of DeFi protocols are treated as financial intermediaries and "should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to manage and mitigate these risks in an ongoing and

---

[8] *Id*., Recommendation 15.
[9] *Id*., Paragraph 194.
[10] *Id*., Paragraph 67.
[11] *Id*., Paragraph 91.
[12] FINANCIAL ACTION TASK FORCE(FATF), DRAFT UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VASPS, (Mar. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.
[13] *Id*., Paragraph 76.

forward-looking manner. In cases where a person can purchase governance tokens of a VASP, the VASP should retain the responsibility for satisfying AML/CFT obligations.[14] When no intermediary is identified using this already expansive standard, the FATF recommends that "countries may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement." In other words, where no intermediary exists regulators should require the creation of VASP—a recommendation which would essentially prohibit decentralized protocols altogether.

B. Global Regulatory Trends

While the general approach of expanding the definition of intermediaries is a recurring method in the global efforts to regulate the crypto space, it is important to recognize that the field is still nascent. Most jurisdictions are still in the process of defining their regulatory approach, and there is an opportunity to change course. As of July 2021,[15] of 128 jurisdictions which provided responses to the assessment on a self-assessment basis, only 58 reported that they had necessary legislation to implement R15/INR/15, with 35 reporting that their regime was operational.[16] Only a minority of jurisdictions had conducted examinations, and even fewer were reported to have imposed any enforcement actions. 32 jurisdictions reported that they had not yet decided what approach to take for VASPs and therefore do not have an AML/CFT regime in place and have not commenced a legislative/regulatory process. Similarly of the 52 jurisdictions which reported that they had established regulatory regimes permitting VASPs, 31 had established only registration regimes and only 17 licensing regimes. Given that jurisdictions have yet to coalesce around an approach regulating decentralized protocols globally, there is an opportunity to apply Web3 native principles that might achieve on-chain regulation without effectively prohibiting decentralized protocols and the efficiencies that arise from them. The novel approach of on-chain compliance described below is yet to be applied in practice. One of the contributions of this essay is to help provide jurisdictions with a wider array of options for achieving regulatory goals, consistent with both the fundamental societal value of privacy, and of compliance.

---

[14] *Id*., Paragraph 68, footnote 7.
[15] FINANCIAL ACTION TASK FORCE(FATF), SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (July 2021),https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (discussing the state of implementation by the public sector through the global network of the FATF).
[16] *Id*., at 6.

(i) On Intermediary Roles

Some jurisdictions have followed the 2021 FATF Guidance and transposed the wording and definition of a VASP as determined by FATF in the exact word format, while others have sought to interpret, extend or even narrow the scope of the definition. For example, a 2022 discussion paper published by the Financial Services Regulatory Authority of Abu Dhabi Global Markets,[17] suggests defining "DeFi controller"(s) as those who can "update the software underlying the protocol" with suggested control tests including "the share of code underlying the protocol contributed by a person" or "the amount of control over the DeFi protocol's administration keys" and proposes requiring the licensing of DeFi controllers to hold them accountable for regulatory obligations equivalent to traditional financial intermediaries, including mandatory KYC and AML requirements, as well as investor disclosure and other investor protection measures.

In the EU, under MiCA , DeFi is generally out of scope, largely on the basis that further legislative packages designed to deal with DeFi will be considered further down the road.[18] However, the definition of "Crypto Asset Service Provider" or CASP, includes the "operation of a trading platform" which is defined as managing a trading platform within which multiple third party buying and selling interests for crypto assets can "interact in a manner that results in a contract.[19]" Similarly, the "reception and transmission of orders" for crypto-assets is also a defined CASP activity and includes a definition to "subscribe for one or more crypto asset and the transmission of that order to a third party for execution." How will each regulator of each Member State of the European Union interpret this or to what extent will the designer or developer of a protocol or decentralized operation be brought within the scope of interpretation of that national authority? It is possible that certain authorities will deem this to cover a completely decentralized and permissionless operation. As authorities continue to evolve their regulatory approaches as to who, if anyone, can be defined as a controller or influencer of that arrangement, different outcomes

[17] FINANCIAL SERVICES REGULATORY AUTHORITY OF ABU DHABI GLOBAL MARKETS, DISCUSSION PAPER NO. 1 OF 2022: POLICY CONSIDERATIONS FOR DECENTRALISED FINANCE (Apr. 13, 2022), https://www.adgm.com/discussion-paper.

[18] Patrick Hansen, *ECB President Lagarde Yesterday in Front of the EU Parliament,* TWITTER (June 21, 2022, 9:30 AM), https://twitter.com/paddi_hansen/status/1539284632608329729?t=DPbBwiMhrYuaWlaDNd3P7g&s=19.

[19] EUROPEAN PARLIAMENT, PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON MARKETS IN CRYPTO-ASSETS, AND AMENDING DIRECTIVE (EU) 2019/1937 - ARTICLE 3(11) (Sept. 24, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

can be established. Although the context of a "controller" will also continue to develop, at present there would be no requirements that applied to any arrangement, technology infrastructure, software or otherwise where there was no responsible person or entity identified as the intermediary.

In Nicaragua, the Regulation of Financial Technology Payment Service Providers (Resolution CD-BCN-XLIV-1-20 approved on September 23, 2020) defines "Financial Technology Payment Service Providers" as: "Legal entities authorized by the BCN, engaged in providing payment services with digital wallets, mobile points of sale, electronic money, virtual currencies, electronic trading and exchange of currencies and/or funds transfers. [20] The activities subject to registration there related to the management of virtual platforms on which virtual assets are traded and to provide such virtual assets (suppliers). [21] The new law (No. 561) in Nicaragua relates to the "General Business Law of Banks, Non-Banking Financial Institutions and Financial Groups" and this brings VASP-related activity within the scope of Nicaragua's Financial Analysis Unit. It is within this process that the business, entity or intermediary is required to register themselves with the Financial Analysis Unit and on that basis, there is no mechanism for any business to comply with requirements to safeguard and combat illicit activity outside of there being a registered entity.

In Vietnam, there is as yet no legal definition of a crypto currency or virtual asset, although the Ministry of Finance of Vietnam has publicly announced the tasking of agencies to prepare the appropriate legal framework for the space. This has been on the basis that the legal gap reflects "mistrust and confusion" as there is no "control" over the ecosystem.[22] The focus for local authorities historically has been to consider regulation in the context of cryptocurrencies being categorized as securities, and as such, to clearly identify the responsible intermediary being the issuer or operator of the relevant platform. While authorities will continue to build responsive legislation that takes into account the high variability in the market, it is clearly the focus to identify the responsible intermediary in a way that complies with FATF Recommendations. However, given the significant volume of activity in Vietnam in the DeFi context, and the fact that the legislation is in a development phase, it is also an interesting case

---

[20] NATIONAL ASSEMBLY OF THE REPUBLIC OF NICARAGUA, REGULATION OF FINANCIAL TECHNOLOGY PROVIDERS OF PAYMENT SERVICES (Sept. 28, 2020), http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/f37b8e176b7e5484062585ec0060f787.

[21] *Id.*

[22] Lisa Prodent, *Vietnam Tasks Government Agencies to Prepare Legal Framework for Cryptocurrencies, Virtual Assets,* VIETNAM-BRIEFING (Apr. 11, 2022), https://www.vietnam-briefing.com/news/vietnam-tasks-government-agencies-prepare-legal-framework-cryptocurrencies-virtual-assets.html.

for the authorities to understand the mechanisms that exist to address the relevant risks without necessarily identifying an institution or intermediary.

In the Philippines, the Bangko Sentral ng Pilipinas (BSP) issued circular 944 in 2017 establishing itself as arguably the first to formally regulate digital currency services, by capturing digital currency exchanges as remittance and transfer companies.[23] They have since issued Circular 1108 in January 2021[24] and changed the scope of virtual assets regulation within the Philippines. The definition of a Virtual Asset Service Provider is now aligned with the FATF VASP definition but excludes the 5th limb of the FATF definition being the "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset." This is because such activity and any activity relating to an Initial Coin Offering (ICO) falls under the regulatory purview of the Securities and Exchange Commission in the Philippines.[25] However, the wording of Circular 1108 goes slightly beyond the FATF definition in other contexts by defining a VASP as "any entity that offers services or engages in activities that provide facility" for the transfer or exchange of a virtual asset, suggesting a blanket definition of the intermediary providing a "facility" for an exchange of a virtual asset. The intention does quite clearly appear to be one of identifying the operator of the platform as the provider of the facility and subject of regulatory liability.

In Thailand, the Digital Asset Management Act BE 2561 was enacted in May 2018 and the Securities and Exchange Commission (SEC Thailand) was granted authority to regulate the space under separate categories: a Digital Asset Exchange, Digital Asset Broker, Digital Asset Dealer, ICO portal, and a Digital Asset Investment Advisory categorisation.[26] In all cases there is a clearly defined intermediary required to go through a licensing process with the authorities there. In an effort to expand definitions and establish intermediaries, the definition of a "digital asset business" in Thailand also includes a digital asset exchange as a "center or a network" established for the purposes of trading or exchanging digital assets.[27]

---

[23] BANGKO SENTRAL NG PILIPINAS MONETARY BOARD , GUIDELINES FOR VIRTUAL CURRENCY (VC) EXCHANGES (Jan. 19, 2017), https://www.bsp.gov.ph/Regulations/Issuances/2017/c944.pdf.

[24] BANGKO SENTRAL NG PILIPINAS MONETARY BOARD , GUIDELINES FOR VIRTUAL ASSET SERVICE PROVIDERS (VASP) (Jan. 21, 2021), https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf.

[25] BANGKO SENTRAL NG PILIPINAS, FREQUENTLY ASKED QUESTIONS (FAQS) ON THE GUIDELINES FOR VIRTUAL ASSET SERVICE PROVIDERS (Jan. 26, 2021), https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/FAQs_VASP.pdf.

[26] THE SECURITIES AND EXCHANGE COMMISSION, THAILAND, DIGITAL ASSETS (2019), https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx.

[27] THE SECURITIES AND EXCHANGE COMMISSION, THAILAND, SUMMARY OF THE EMERGENCY DECREE ON DIGITAL ASSET BUSINESS B.E. 2561 (May 2018),

Restrictions are also in place in Thailand and the Thai SEC approved new rules in June 2021 to prohibit regulated digital asset exchanges from providing services in relation to utility tokens and certain categories of cryptocurrencies.[28] This included meme tokens, fan tokens, non-fungible tokens ("NFT") and digital tokens issued by digital asset exchanges or related persons. This restriction was introduced largely on the basis that these instruments involve significant risk and are designed for speculative purposes creating significant market risk. While these may be considered to be restrictive tests in terms of the assets permitted to be listed, the breadth and width of the interpretation of a "center or network" established for the trading of virtual assets has not yet been publicly tested.

In Indonesia, the Minister of Trade Regulation No. 99 of 2018 formally permitted the trading of cryptoassets in Indonesia as futures contracts, and brought such activity within the scope of the Commodity Futures Trading Supervisory Authority ("Bappebti").[29] By doing this, the authorities are automatically bringing any such activity within existing law and regulation, and on that basis, identifying the intermediary that is to be regulated and responsible for the operation of the platform. The Bappebti Regulation No5 of 2019 provided a regulatory framework for the operation of the physical crypto asset futures market. This essentially means that the trading activity may be regulated but virtual assets and their application or use as a payment instrument are prohibited in the jurisdiction. Generally speaking, the activities falling within the scope of regulation are defined as Cryptoasset Exchanges, Cryptoasset Clearing Agencies, Cryptoasset Traders, Cryptoasset Clients, and Cryptoasset Storage Providers, all subject to separate requirements under local law.

In the UK, the registration requirements for VASP related activity is captured by the activity defined under Regulation 14A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).[30] In summary the UK regulation captured cryptoasset exchange providers (both fiat to crypto and crypto to crypto) and

---

https://www.sec.or.th/TH/Documents/DigitalAsset/enactment_digital_2561_summary_en.pdf .

[28] SEC News, *SEC Board approves rules governing digital asset exchanges regarding service provision related to utility tokens and certain types of cryptocurrencies* (June 12, 2021), https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=8994.

[29] MINISTER OF TRADE OF THE REPUBLIC INDONESIA, REGULATION OF THE MINISTER OF TRADE OF THE REPUBLIC OF INDONESIA NUMBER 99 OF 2018 CONCERNING GENERAL POLICY ON ORGANIZING THE CRYPTO ASSET TERM TRADE (June 25, 2019), http://jdih.kemendag.go.id/peraturan/download/1744/3.

[30] THE MONEY LAUNDERING, TERRORIST FINANCING AND TRANSFER OF FUNDS (INFORMATION ON THE PAYER) REGULATIONS 2017: UK STATUTORY INSTRUMENTS, 2017 NO. 692, PART 2, CHAPTER 1, REGULATION 14A (2017), https://www.legislation.gov.uk/uksi/2017/692/regulation/14A.

custodian wallet providers. Services described as "exchanging, or arranging or making arrangements with a view of the exchange of, one crypto asset for another" are caught within the definition of a Cryptoasset exchange provider. Similarly, "operating a machine which utilizes automated processes to exchange crypto assets for money or money for crypto assets" is also defined and captured as a regulated service. Again, while there are questions of interpretation around these terms, and while neither may have been written to specifically aim at a specific market, the trend to expand definitions of regulated entities in search of financial intermediaries in crypto is apparent.

(ii) On unhosted wallets

Over the past several years, regulators and policy makers have expressed concern about the heightened risk of illicit financial activity posed by so-called unhosted wallets and DeFi protocols. Recall that in the vision of decentralized finance, centralized custody is not necessary. Instead of entrusting funds to the hands of intermediaries, crypto owners often opt to hold their assets directly in "unhosted wallets," controlled by a cryptographic key that is held directly by the owner. Thus, the owner of an unhosted wallet self-custodies their own assets and maintains full and unilateral control over these, much like physical cash. The absence of intermediaries in the decentralized, peer to peer (P2P) environment of Web3 poses a challenge to the current intermediary-based regulatory regimes. Hence, unhosted wallets concern financial regulators, particularly when they interact with regulated entities.

Policy makers worldwide have developed various approaches to addressing the challenge posed by unhosted wallet transactions. One prominent example was embodied in the United States Treasury's attempt to impose financial monitoring requirements that facilitate transactions with unhosted wallets in December 2020. Pursuant to the proposed rule, banks and money service businesses would have had to collect identifying information and file a report with FinCEN for transactions involving unhosted wallets, not only for their own customers but also for their customer's counterparties.[31] While this particular proposal faced strong opposition, with more than 7,000 letters submitted in objection,[32] other

[31] U.S. Department of the Treasury, *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions* (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216.

[32] Miles Kruppa & Hannah Murphy, *Crypto Industry Fears Impact of Proposed Treasury Rule,* FINANCIAL TIMES (Jan. 11, 2021), https://www.ft.com/content/97ec59d6-bc68-4ffc-853e-0de561b82c1e.

jurisdictions are continuously looking for regulatory means to bring unhosted wallets into the regulatory perimeter through the intermediaries they transact with.

Another example of regulatory resistance to unhosted wallets concerns the application of the so-called "Travel Rule" to the crypto industry. This rule requires all financial intermediaries to a transaction to pass along information identifying the originator and beneficiary along with every payment transaction, and as such require information relating to the identity of a sender and a recipient of a transfer of a crypto asset to be captured, regardless of the destination address being an unhosted wallet address. Similar positions have been taken in Singapore[33] and Switzerland.[34]

In bringing unhosted wallets within the perimeter of the travel rule, regulators again bring the requirement for European Crypto-assets Service Providers ("CASPs," which are similar to "VASPs" under the FATF standards) to collect information on the unhosted wallet, and in addition, apply a risk-based approach to determine any further measures.[35] In essence, prior to the transaction being executed, the CASP or business would be required to identify and assess the AML/CFT risk presented by the unhosted wallet and apply relevant risk mitigation measures which will be defined by the European Banking Authority in the near future. While CASPs and payment service providers are required to ensure that the information on the payer and the payee or originator and beneficiary are not missing or incomplete, there must also be an effective risk based procedure for determining whether to execute or reject a transfer that lacks the required beneficiary information.

This can lead to multiple issues with respect to unhosted wallets. The first is how to accurately validate the owner of an unhosted wallet, which can simply be physically passed on to another person (in case of a hardware wallet) or have another person sharing its secret key, and not be linked to any person or entity at any point. Second, if the unhosted wallet is a counterparty of the CASP's customer who has no relationship with the

---

[33] MONETARY AUTHORITY OF SINGAPORE, PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – HOLDERS OF PAYMENT SERVICE LICENCE (DIGITAL PAYMENT TOKEN SERVICE) (Dec. 5, 2019), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/PSN02-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--Digital-Payment-Toke.pdf.

[34] FINMA applied the Anti-Money Laundering Act to VASPs and clarified it as part of the latest update to the FINMA-AMLO legislation (Article 10).

[35] EUROPEAN PARLIAMENT, REPORT ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON INFORMATION ACCOMPANYING TRANSFERS OF FUNDS AND CERTAIN CRYPTO-ASSETS (RECAST) (June 4, 2022), https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.html.

CASP, they will be asked to turn over sensitive personal information to a party with whom they have no contractual relationship and have no reason to trust with such sensitive information. This raises enormous cybersecurity and privacy concerns. The challenge is how to define rules and sensible policies around transactions that may or may not be permitted, or to create secure data sensitive networks that allow transactions to occur in a secure environment without the requirement for multiple jurisdictions and authorities to interpret and implement risk mitigation measures which are defined by the European Banking Authority.

The approach in the UK, which was published in response to the consultation around the Money Laundering and Terrorist Financing (Amendment) (No2) Regulations 2022,[36] proposes a different approach in respect of transactions with unhosted wallets in light of the feedback received. Here the authorities note that "[i]nstead of requiring the collection of beneficiary and originator information for all unhosted wallet transfers, crypto asset businesses will only be expected to collect this information for transactions identified as posing an elevated risk of illicit finance."[37] The factors to determine the risk will be set out in legislation but the UK Government has taken the view that unhosted wallet transactions should not be automatically viewed as high risk. However, they are not completely exempt from the Travel Rule requirements on the basis that an outright exclusion could incentivise criminals to use them to evade controls.[38]

2.2 Blockchain Analytics

Because most of the blockchain ledgers today are pseudonymous, the principal tools currently used by compliance professionals, regulators and law enforcement are blockchain analytic services that use heuristic, best-effort matching of public transaction information with private information. These heuristic techniques critically rely on the transparency of the blockchain and use big-data techniques to identify and inspect it into data that can fuel compliance and risk management.

Several trends pose challenges to the sustainability of these tools. First and foremost, as blockchain ledgers grow more private, blockchain analytics would be rendered less of a powerful tool for compliance. Many of the important use cases for blockchain, including payments, central bank digital

---

[36] HM TREASURY, AMENDMENTS TO THE MONEY LAUNDERING, TERRORIST FINANCING AND TRANSFER OF FUNDS (INFORMATION ON THE PAYER) REGULATIONS 2017 STATUTORY INSTRUMENT 2022(JUNE 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083351/MLRs_SI_2022_-_Consultation_Response_final.pdf.
[37] *Id*., Section 6.21.
[38] *Id.*

currencies, and tokenization of traditional financial products, require privacy: a transparent payment platform, which reveals all transactions and balances would impose grave risks for individual privacy, commercial confidentiality and national security. Moreover, the long term efficiency of blockchain analytics is questionable. As FinCEN recently observed,[39] existing blockchain analytics approaches "can be rendered less effective by a number of factors, including the scale of a blockchain network, the extent of peer-to-peer activity [...], the use of anonymizing technologies to obscure transaction information, and a lack of information." The FATF has similarly acknowledged[40] the "challenges and limitations inherent in this kind of research with blockchain analytics, in terms of coverage, timeliness, accuracy and reliability."

If blockchain analytics is used by compliance staff, financial regulators, and law enforcement as the primary tool for crypto compliance, and given the reliance of blockchain analytics on the transparency and traceability of transactions on the blockchain, then the same privacy-preserving technologies (e.g., anonymous cryptocurrencies) that serve to protect privacy and enhance cybersecurity on the blockchain technology will enhance the risk of illicit activity on blockchains. Indeed, the Financial Action Task Force (FATF) considers transactions involving privacy preserving cryptocurrencies and anonymity enhanced cryptocurrencies as a indicators of "red flags" suggesting potential risks of money laundering.[41] FinCEN, in an interpretive guidance, similarly considers "anonymity-enhanced" transactions as often "structured to conceal information otherwise generally available through the native distributed public ledger; or… specifically engineered to prevent their tracing through distributed public ledgers.[42]

The recent enforcement action against Tornado Cash serves as a great example of these tensions. Tornado Cash is a protocol providing privacy to crypto users by means of mixing. Simply put, Tornado Cash mingles assets of different users together in a way that obfuscates their origin. Users could

---

[39] U.S. DEPARTMENT OF THE TREASURY, REQUIREMENTS FOR CERTAIN TRANSACTIONS INVOLVING CONVERTIBLE VIRTUAL CURRENCY OR DIGITAL ASSETS (Dec. 23, 2020), https://public-inspection.federalregister.gov/2020-28437.pdf.

[40] FINANCIAL ACTION TASK FORCE (FATF), UPDATED GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

[41] FINANCIAL ACTION TASK FORCE(FATF), *VIRTUAL ASSETS RED FLAG OF MONEY LAUNDERING AND TERRORIST FINANCING* (Sept. 2022), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

[42] U.S. TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

use Tornado Cash to enhance their legitimate financial privacy and confidentiality. But at the same time—as the action brought by OFAC enumerated—it was used by rogue state actors and cybercriminal organizations in furtherance of their illicit financial activity. Circumstantially, the use of mixers such as Tornado Cash could be attributed to a desire to clean "dirty" assets due to the difficulty of identifying illicit financial activity through mixers using typical blockchain analytic techniques. However, as we show below, emerging technologies could serve to provide law enforcement with the requisite selective disclosure, while at the same time provide privacy and financial confidentiality to crypto users, striking a better balance between law enforcement and AML needs on the one hand, and consumer privacy on the other.

3. WHY IS CURRENT REGULATION INEFFICIENT AND UNSUSTAINABLE

We believe that expanding the definition of financial intermediaries to parties ill-suited to implementing regulatory obligations while at the same time doubling down on blockchain transparency creates grave cybersecurity risks from both state actors and criminal organizations, undermines consumer protection, and threatens national security as blockchain technology gains broader adoption. Furthermore, these approaches conflict with the rights to financial confidentiality and privacy, and jeopardize the innovation taking place in Web3.

3.1 Consumer Protection and Information Security Risks

Forcing an intermediary-based approach on distributed computing systems—which is what the decentralized crypto eco-system, or Web3 represents is flawed in two ways. First, it presumes the existence of reliable entities that can collect the information, report it to law enforcement and keep it safe from cyber attacks. However, this is a problematic presumption, since in the decentralized settings many of the intermediaries (especially as captured by the aforementioned expansive definitions) are themselves ad hoc players who may be nefarious, and even if well-meaning, are incapable of protecting sensitive personal and commercial information. In particular, the collection and retention of personal information (e.g. names and physical address) of members of the public should not be carried by entities that are not well equipped to protect it, and lack the training, the resources and the culture of compliance to do so in a safe way. Imposing record-keeping requirements on such parties substantially increases the risk of data theft and concomitant harm to law-abiding citizens.

When blockchain-based assets are used for payments, for example through the use of stablecoins, current crypto regulation would lead to

enormous cybersecurity vulnerabilities. Expanding the definition of intermediaries, if taken to the extreme, could for example impose AML obligations on merchants to collect the personal information of all customers who make payments using an unhosted wallet, in order to relay this information to the MSBs and banks that serve these merchants. Blockchain-based asset holders would thus be effectively required to disclose their home address to merchants they transact with. This is not merely odious from the perspective of financial confidentiality; it is downright dangerous as an invitation to extortion or home invasion, if the merchant is rogue or had its systems compromised by a cyber attack. This risk is aggravated by criminals' ability to observe wallets' balances on public blockchains, to identify "juicy" targets. (Recall that blockchain analytics and its transparency-based heuristics rely on such information being broadcast on public blockchains.) In a future world where cryptocurrencies are a major payment currency, for example as the use of stablecoins expand and governments adopt CBDCs, the transparency of every transaction is not merely an individual risk for a data breach: It is a national security risk, threatening to expose national financial data to the prying eyes of enemies. Indeed, the prudent regulatory path would be to embed privacy preserving technologies rather than default transaction transparency into stablecoins and CBDCs to preserve financial confidentiality much as traditional banks do, but to also embed within these digital assets on-chain compliance mechanisms through the use of smart contracts in a Web3 environment.

The search for intermediaries, and imposition of AML obligations on small entities in the decentralized ecosystem, may also conflict with the Regulatory Flexibility Act. These small entities rarely have the capabilities required to collect and safely store highly-sensitive information. Often, creators and developers of smart contracts operate from small "garage" settings, and the overencompassing intermediary-based approach would impose on them an obligation to acquire new expertise, computer software, computer hardware, and/or services, at high costs. Furthermore, such small entities may face additional liability and/or insurance costs, due to federal and state regulations governing the storage and breach-response of personally identifying information.

Payment of cryptocurrency to a third party, such as a merchant, does not necessarily require users to disclose the physical address. However many uses of cryptocurrency for payments would require payees to share this highly sensitive information with a broader array of services, ranging from MSBs to merchant terminals and other data providers. Increasing the number of obligations for identification and the number of services that hold this valuable data, would greatly increase the probability of a data breach that harms customers.

This harm is not theoretical. In recent years, dozens of cryptocurrency exchanges and businesses have been subject to data breaches that exposed

sensitive customer information, including customer home addresses and cryptocurrency balances.

The potential for consumer harm is especially grievous when considering a data breach or misuse that exposes the physical address of a self-hosted wallet's owner and connects it to the balance in that wallet (which is readily visible once you know the wallet address, in many blockchains; recall, the pseudonymous nature of the blockchain is the key to its transparency and lack of financial confidentiality). Furthermore, even minor data leaks can cause disproportionate privacy harm to customers, since even a small amount of wallet identifying data can often be combined with public ledger data in order to recover a user's entire transaction history. Such a breach can expose the wallet owner to the risk of online or even physical extortion attempts. Indeed, cryptocurrency wallet owners have been subject to both threatened and actual attacks.

Interestingly, some of the plaintiffs challenging the U.S. Treasury Department's sanctions of the Tornado Cash smart contracts and asking the Court to remove them from the U.S. sanctions list, raise these risks.[43] One of the plaintiffs is an early crypto adopter with a large online presence and a public ENS name linked to his Twitter profile; he thus used Tornado Cash to protect his personal security while transacting. Another plaintiff operates an Ethereum staking business, and started using Tornado Cash after a stranger inquired about his Ethereum staking earnings.

There also exists ample precedent for such concerns in the domain of traditional credit and debit card payments. A large number of criminal data breaches have targeted companies, including large ones (e.g., Equifax, TJ Maxx and Home Depot) who have significant IT capability. The intermediary-based approach would make attacks even more lucrative (due to the additional personal information and the linkability to asset holding balances), and thus increase mitigation and recovery costs.

Overall, expanding the definition of financial intermediaries beyond financial institutions, to other parties in the crypto ecosystem increases the amount of confidential and personal data that will need to be collected, without any corresponding attention to ameliorating the attendant information security risks this will pose across the cryptocurrency ecosystem and beyond. Furthermore, it risks exposure of commercial activity to untrusted third parties, with potential economic and national-security implications.

3.2 Harm to innovation

[43] Nikhilesh De, *Crypto Engineers, Investors Sue US Treasury Over Tornado Cash Sanctions,* COINDESK (Sept. 8, 2022, 12:14 PM), https://www.coindesk.com/policy/2022/09/08/crypto-engineers-investors-sue-us-treasury-over-tornado-cash-sanctions.

The approach of expanding the definition of intermediaries is also fundamentally incompatible with existing and emerging technologies for virtual assets conveyed on distributed ledgers. Many such technologies rely on autonomous and decentralized mechanisms, such as smart contracts (i.e., distributed computer programs) that are deployed across many computers that operate the ledger. Such smart contracts do not have legal names or physical addresses, and thus users of regulated financial institutions would be unable to interact with these technologies in the situations covered by the proposed statutes and regulations. This raises the possibility of hamstringing the growing technology area of decentralized finance and its integration with traditional finance.

There is an additional risk of fragmentation of the crypto ecosystem, when the global regulatory landscape is inconsistent and allows for arbitrage. Adopting regulation which seeks to enforce intermediaries on a decentralized system, would position the jurisdictions that impose and enforce such rules as hostile to creation and adoption of advanced distributed ledger technology, and encourage innovators to develop and base their projects in other jurisdictions. We have already seen this chilling effect play out in other regulatory contexts, such as securities regulations, which have led many innovative virtual asset projects (e.g., Facebook's Libra/Diem Foundation) to incorporate and operate outside the US. Overburdening Web3 innovators with regulation could induce the exodus of talent and the ceding of innovation lead. It would also hamstring the long-term ability of the US to regulate parties who build distributed-ledger technology.

3.3 Ineffective Methodologies to Regulate a Decentralized Space

Many innovations in blockchain technology, aiming to improve efficiency and scalability, do so by omitting information from public view. This includes cryptographic techniques such as zero-knowledge roll-ups, Bitcoin's new Taproot protocol, Lightning Network, and various other Layer 2 solutions. All of these are privacy-enhancing trends that would undermine the transparency of the blockchain and render blockchain analytics less effective. Moreover, as the arc of the crypto ecosystem leans more towards decentralization, complex smart contracts, replacing some financial intermediaries with algorithms, are increasingly being deployed to support decentralized finance. These often operate in complex ways that commingle funds. Today's heuristic analysis, lacking application-specific information, often resorts to blanket "de-risking" of DeFi services.

Indeed, as FinCEN acknowledged, blockchain analytics approaches "can be rendered less effective by a number of factors, including the scale of a blockchain network, the extent of peer-to-peer activity [...], the use of

anonymizing technologies to obscure transaction information, and a lack of information."[44] The FATF has similarly acknowledged the "challenges and limitations inherent in this kind of research with blockchain analytics, in terms of coverage, timeliness, accuracy and reliability."[45]

Further, as the arc of crypto innovation leads to further decentralization, the search for intermediaries is not likely to be effective in its stated goal of keeping records and filing reports that have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in intelligence or counterintelligence matters to protect against international terrorism. True, law-abiding customers of banks and MSBs may be induced to provide detailed counterparty information (if their counterparties deign to share personal details such as physical address, despite the aforementioned risks). However, nefarious parties, such as those engaged in crime, tax evasion or terrorism, would circumvent such requirements by relaying their transactions with third parties through their own unhosted wallet.

The enforcement actions against Tornado Cash are illustrative of the methodological difficulty in regulating protocols using current tools. Unlike traditional subjects of sanction enforcement, Tornado Cash is a protocol, not an entity or an individual. It is a decentralized, permissionless code; a smart contract running on blockchain. Enforcement actions against protocols are unprecedented, and some could argue, violate hard core constitutional principles, such as the first amendment.[46] Significantly, decentralized protocols offer a technological innovation that allows code to be developed and enforced without a centralized focal point of control. Unlike previous enforcement actions against mixers, such as OFAC's action against Blender.io,[47] that indeed involved an underlying centralized service, it is not clear whether Tornado Cash has an intermediary entity standing behind the

---

[44] U.S. TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, REQUIREMENTS FOR CERTAIN TRANSACTIONS INVOLVING CONVERTIBLE VIRTUAL CURRENCY OR DIGITAL ASSETS (Dec. 23, 2020), https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.

[45] FINANCIAL ACTION TASK FORCE (FATF), UPDATED GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

[46] Jerry Brito & Peter Van Valkenburgh, *Analysis: What is and What is Not a Sanctionable Entity in the Tornado Cash Case* (Aug. 15, 2022), https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case.

[47] Robert Stevens, *Bitcoin Mixers: How Do They Work and Why Are They Used?,* COINDESK (Aug. 22, 2022, 12:11 PM), https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used;

Ellen L. Aldin et al., *OFAC Imposes First-Ever Sanctions Against Virtual Currency Mixer,* MAYER BROWN (May 6, 2022), https://www.mayerbrown.com/en/perspectives-events/publications/2022/05/ofac-imposes-first-ever-sanctions-against-virtual-currency-mixer.

decentralized curtain and actively involved in concealing assets and providing services to support illicit finance. It is not clear at this point whether there are any individuals or entities behind Tornado Cash that could justify the intermediary-based approach taken by OFAC in this case.

In April 2023, The US Department of the Treasury published an assessment of Illicit Finance Risks of Decentralized Finance.[48] The assessment does not impose any mandatory obligations; rather, it suggests a normative framework, and ends with open questions by extending an invitation to industry dialogue. Overall, the report finds that DeFi services which do not comply with existing AML/CFT regulations are posing the most significant illicit finance risk in the virtual asset domain. The assessment finds that illicit actors, including ransomware cybercriminals, thieves, scammers, and Democratic People's Republic of Korea (DPRK) cyber actors, are using DeFi services in the process of transferring and laundering their illicit proceeds. The assessment also proposes a functional test for DeFi Regulation, stating that a DeFi service that functions as a financial institution, will be required to comply with BSA obligations, including AML/CFT obligations, regardless of whether the service is centralized or decentralized. A DeFi service's claim that it is or plans to be "fully decentralized" does not impact its status as a financial institution under the BSA, nor any of its other financial regulation obligations.

3.4 Rights to Privacy

The protection of privacy is related to the functions of privacy in our social lives: the promotion of liberty, autonomy, selfhood, and human relations, and for furthering the existence of a free society.[49] Statutory privacy rights are therefore common in the western world, to protect and limit the ability to collect data on the individual against her will. In the US, state legislation protects privacy as a right. The 2020 California Consumer Privacy Act (CCPA) defines a right to limit the use and disclosure of sensitive personal information. The Virginia Consumer Data Protection Act (VCDPA) provides rights to information, access, correction, deletion, data portability, and opt out (2021).[50] Also enacted in 2021, the Colorado Privacy Act provides a similar set of rights.[51] Federally, The Right to Financial Privacy Act of 1978 (the RFRA) protects the confidentiality of personal

[48] For the full text of the assessment, see https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.
[49] Ruth Gabizon, *Privacy and the Limits of Law,* 89 YALE L. J. 421 (Jan. 1980), https://ssrn.com/abstract=2060957.
[50] VIRGINIA CONSUMER DATA PROTECTION ACT, VA. CODE ANN. §§ 59.1-575 to 59.1-585.
[51] COLO. REV. STAT. §§ 6-1-1301 to 6-1-1313 (2021) (effective July 1, 2023).

financial records, and requires that federal government agencies provide individuals with a notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to a federal government agency, often for law enforcement purposes.[52] In the EU, the General Data Protection Regulation (GDPR), provides a Right to Restriction in Article 18, where Article 18 of the GDPR enables an individual to demand that organizations stop processing their data, accompanied with the right to object in Article 21, where individuals have a right to object to the processing of their personal data.[53]

Naturally, the right to privacy conflicts with law enforcement's need to know about crimes and terrorism before they happen; for crime prevention and national safety as well as for investigation ex post. For example, when police attempts to learn of plans for a terrorist action, potential terrorist may raise a privacy claim concerning this information. A terrorist may opt to use privacy tools to conceal and obfuscate their actions. To differentiate between legitimate and illegitimate types of motivations for privacy, a balance between privacy and law enforcement is required, because, as Gabizon says, "the need to have solitude and anonymity is related not only to the wish to conceal some kinds of information, but also to needs such as relaxation, concentration, and freedom from inhibition."[54]

In traditional finance, the balance between the right to privacy and financial confidentiality vs. law enforcement's needs is achieved via financial intermediary. In both Europe and the U.S., laws define a civil right to privacy and financial confidentiality, that limits the ability of the financial intermediary to use the data for commercial or other purposes, but carves out exceptions for sharing legally-required information with law enforcement agencies, so that compliance reports cannot be considered a breach of that privacy right.

In decentralized finance and crypto markets, however, in the absence of effective intermediaries, law enforcement leans on the traceability and transparency of the blockchain as a condition of legality, rendering the right to privacy and financial confidentiality in this space obsolete.

Against this backdrop, it is important to emphasize that tools for privacy, such as Tornado Cash, can be used for legitimate privacy protection, rather than for obfuscating the visibility of law enforcement. As Coinbase CEO and co-founder Brian Armstrong notes, "If you receive your salary in crypto, for example, you might not want the world to know how much money you make, or how you choose to spend it."[55] Individuals

---

[52] 12 U.S.C. §§ 3401-342.
[53] Regulation (EU) 2016/679 (General Data Protection Regulation).
[54] *Id.*
[55] Brian Armstrong, *Defending Privacy in Crypto,* COINBASE (Sept. 8, 2022), https://blog.coinbase.com/defending-privacy-in-crypto-e09db33dece8.

reported to use Tornado Cash could use it to anonymously donate money to Ukraine;[56] to protect personal security while transacting; to conceal asset balance in their wallet and protect their finances.[57] Abandoning privacy all together because of methodological constraints in law enforcement seems to overturn the legal foundations. If we knew crime prevention came at the cost of constant surveillance, "we might feel the need to rethink criminal law," as Gabizon says. But it so happens that the methodological constraints for law enforcement are based on false premises: emerging technologies for on-chain compliance become a critical tool set for the future regulator of financial markets, and enable decentralized and privacy-preserving enforcement of compliance, without intermediaries, and with no reliance on blockchain analytics and no need in traceable trade on-chain. In the next section, we will describe some of these emerging technologies.

3.5 Stablecoins and the risk for bank runs and financial stability

In March 2023, the Federal Reserve published its denial decision of Custodia's membership application, as well as its application for a master account.[58] The decision goes quite a way beyond this in an 86-page release, with the Fed detailing the "fundamental concerns" with Custodia's approach, many of which had related to its intent to issue stablecoins affiliated with the bank, and the nature of stablecoins issuance and trading. In particular, the Federal Reserve dives deeply on why the transparency of public blockchains imposes risks and how it correlates and supports potential runs .

On most public blockchains, the public is able to see tokens moving from one wallet to another, including as they are issued and redeemed. The Fed emphasizes that the public would know when Custodia's stablecoins are being redeemed in high or higher-than-usual quantities. This redemption transaction visibility could potentially increase the likelihood of a run on Custodia's stablecoins, other deposit liabilities, or custodied assets (which could affect its fee revenue). While Custodia has said it will manage liquidity risks by keeping all the dollars backing stablecoins in a master account at the Federal Reserve if such an account is granted, history has shown that runs on any bank or financial intermediary have led to panic and contagion that spread to other banks and financial intermediaries. The Fed emphasizes why transaction privacy is critical and desirable from a regulatory perspective.

4. ON-CHAIN COMPLIANCE AND HOW IT COULD ENSURE PRIVACY

[56] *Id.*
[57] *Id.*
[58] For the full text of the order, see https://www.federalreserve.gov/newsevents/pressreleases/files/orders20230324a1.pdf.

Emerging blockchain technologies allow enforcement of crypto compliance mechanisms using the power of blockchain's consensus rules. These consensus rules, which govern the operation of blockchains, are programmatic means that determine what transactions are deemed valid for the purpose of addition to the blockchain's append-only ledger (e.g., by miners or validators). Traditionally, these consensus rules, and the programmatic smart contracts they enable, have been used mainly for defining asset-transfer mechanisms and financial instruments. However, they can be used also for the purpose of compliance. Indeed, for every blockchain, decentralized protocol or virtual asset thereon, it is possible to create a compliant version that would code the compliance requirements into consensus rules and thereby enforce jurisdictional policies while preserving the asset's economic value and the protocols' technological capabilities.

Using blockchain technology for compliance could also provide for privacy-preserving enforcement, similar to the financial compliance enforcement in traditional finance, where only authorized parties have visibility to reports carrying information about actors' identity and funds' provenance. Personal identity and other data could be made selectively visible only to authorized law enforcement authorities, subject to clear policies, while protecting sensitive personal information from the prying eyes of data miners, business competitors, criminal actors and nation-state adversaries. This could be realized using advanced cryptographic techniques, such as zero-knowledge proofs and verifiable encryption.

Compliance policies, established by regulators and/or within organizations, could be programmed to enforce rules for which digital transactions may be allowed, and what information should be stored with each transaction. These rules could determine which transactions are compliant, what human approvals (if any) are needed, what reports should be generated, when, and who should have access to these reports.

Using such on-chain compliance, pools of assets can be created such that each and every transaction is guaranteed (by the consensus rules and cryptography) to be compliant with the specified policies, and to carry the associated identity credentials that demonstrates compliance. That guarantee could be maintained regardless of whether the transaction was conducted through custodial or self-hosted wallets. Assets would enter the compliant pool by an identification process at a regulated entity, which the policy may require to verify identity or source of funds. The underlying assets could also be extracted from the pool, again subject to policy mandates such as reporting. As long as assets are subject to the programmable policy, the pool of assets as a whole can be cryptographically trusted as compliant.

4.1 Financial Confidentiality and Privacy

Crucially, on-chain compliance would be enforced without compromising the financial privacy and security of cryptocurrency users. While identity information may be recorded on the blockchain ledger, it could be cryptographically protected and not publicly visible. Instead, sensitive personal information (direct or derived) would be visible only to authorized parties, subject to the predetermined policy. On-chain compliance does not rely on centralized silos or privileged "panopticons."

The policy could prescribe who are the parties, within a jurisdiction, who have special privileges (e.g., visibility of information, or authority to issue alert lists and sanction lists), and what conditions are placed on exercising these privileges. It could also define any constraints and reporting requirements on fund movements across jurisdictional policies. Crucially, on-chain compliance could robustly protect confidential identifying information and never expose information or reveal it to third parties, except as dictated by the policy. Similar to traditional finance, on-chain compliance robustly protects privacy and financial confidentiality, with visibility available only for those authorized under law and policy. On-chain compliance opens windows of selective visibility, when the default is robust privacy protection. Data, and deductions from it, are revealed only to authorized parties. Integrity of the data, and of mandated actions such as reports, is cryptographically ensured—without reliance on centralized, high-risk repositories of sensitive information. Rather than requiring a repository of sensitive data, on-chain compliance could allow regulators to see and focus on the information they need.

In traditional finance, the transaction details are visible only to the counterparties (and their intermediaries), and to law enforcement, while private to the general public. Intermediaries are in charge of protecting the information security and privacy of their customers' financial data, and enforcing compliance. In blockchain today, transactions are visible (in pseudonymous form) to the general public, and partially to law enforcement as well (depending on the source of the transaction). On-chain compliance brings crypto to par level with traditional finance, by opening windows of visibility for law enforcement and to the counterparties, while robustly enforcing privacy and financial confidentiality for all others.

4.2 Programmable Policies

Consensus rules could be configured to facilitate precise specification of what policies to enforce on transactions. Regulators and law enforcement can ensure that these policies satisfactorily reflect the laws, rules and regulations in their jurisdiction. Once a policy is deployed and activated, its fulfillment is robustly ensured "on autopilot" by cryptographic mechanisms. Policy rules may dictate what information about the parties should be recorded or disclosed, and to whom. They may also restrict transactions, or

freeze funds, e.g., for compliance with sanctions or securities regulations. Multiple policies can coexist for the same sealed asset, e.g., corresponding to different jurisdictions.

Regulators and law enforcement can define the policies within their jurisdictions, and ensure that these policies satisfactorily reflect the laws, rules and regulations in their jurisdiction. Execution of a policy is then robustly ensured by cryptographic mechanisms, which integrate with the blockchain consensus rules.

Examples of policies that could be enforced using on-chain compliance include rules over parties' identity (e.g., nationality) without publishing confidential user identity information; embed encrypted KYC/CDD/EDD data with granular access control, and ensure the correctness of the data; monitor transactions and streamline mandated reports, including Suspicious Activity Report annotations to transactions that can be seen only by designated regulators; block transactions with sanctioned identities/attributes, or stolen funds; report aggregate financial activity statistics; convey travel rule information for transactions between virtual asset service providers; and extra verification or reporting when moving funds to/from wallets that are subject to other jurisdictional policies.

The policy can prescribe who are the parties, within a jurisdiction, who have special privileges (e.g., visibility of information, or authority to issue alert lists and sanction lists), and what conditions are placed on exercising these privileges. It also defines any constraints and reporting requirements on fund movements across jurisdictional policies.

On-chain compliance can accommodate nuanced risk-based policies that reason about multiple risk indicators. Transaction blocking and alerting can weigh myriad criteria including identity attributes, the source of identity attestations, amount thresholds, past transaction history, activity patterns, and alert/block lists. These policies can reflect the regulatory mandates, augmented with the VASP own risk policies and tolerance, and can use data feeds such as customer records and existing chain analytics.

The flexibility of consensus rules can ensure that policies may coexist for the same assets, each issued for a different jurisdiction. Policies can be designed to harmonize common elements (e.g., following FATF guidelines), thereby streamlining investigative cooperation and ensuring data availability and integrity. Moreover, on-chain compliance can accommodate nuanced risk-based policies that reason about multiple risk indicators. Transaction blocking and alerting can weigh myriad criteria including identity attributes, the source of identity attestations, amount thresholds, past transaction history, activity patterns, and alert/block lists. These policies can reflect the regulatory mandates, augmented with the VASP own risk policies and tolerance, and can use data feeds such as customer records and existing chain analytics.

4.3 Blockchain-Native Approach: Regulating DeFi

Instead of enforcing principles of traditional financial regulation on a decentralized financial system, on-chain compliance allows regulators to harness the power of the blockchain to enable stronger blockchain-based enforcement that is compatible with Web3 infrastructure. One prominent example of the need for an on-chain, blockchain-native approach to compliance is DeFi. DeFi protocols can be distinguished from traditional market infrastructures in several ways. First, typically assets in DeFi are held directly by users in ”unhosted” wallets or through smart contract-based escrow rather than by a centralized service provider or custodian in an account on the asset owners' behalf. Second, settlement and execution are conducted by software (smart contracts) rather than financial intermediaries. Rather than relying on a centralized service provider, operator, or organization that ultimately exercises discretion, DeFi protocols are governed by open-source code. DeFi is a decentralized financial arena, with no intermediaries. Users may create intermediary or proxy contracts that redirect calls and transactions to a modified contract as a way of updating an earlier contract but they are always self sovereign and hold their assets directly without a custodian.

In the absence of an entity that can serve as an intermediary, on-chain compliance could regulate and enforce compliance in DeFi as a natural, programmable upgrade to the smart contract. For example, on-chain compliance can be compatible with unhosted (self-custodied) wallets, without entrusting any third party with control or custody of the funds. Once unhosted users are identified and verified by a legitimate KYC provider, programmable on-chain compliance can monitor the trade and automatically issue reports off the blockchain, without any intermediary intervening in the process. Even for the most sophisticated compliance reports such as SARs, red flag tests can be coded into an on-chain policy and provide jurisdictional compliance.

Indeed, in its assessment of decentralized finance published in April 2023,[59] the U.S Treasury acknowledges the promise of cryptographic Zero-Knowledge proofs integrated as compliance mechanisms into smart contract code. The report promises that the Treasury is working to improve the overall effectiveness of the AML/CFT regulatory framework and sanctions compliance programs in the virtual asset space and will engage with the private sector to support responsible innovation in the DeFi space. The assessment recommends that the U.S. government should engage with developers, including through tech sprints and potentially with research and

[59] U.S. DEPARTMENT OF THE TREASURY, *supra* note 48.

development grants, to promote innovation that seeks to mitigate the illicit finance risks of DeFi services. Policymakers and regulators should also seek and assess necessary changes in regulation or guidance to support these developments.

4.4 Modernizing AML Rules

On-chain compliance is an opportunity to modernize AML rules utilizing consensus rules running on a blockchain. Instead of struggling to harmonize KYC practices, or exposing the financial system to a central panopticon with the implications on cyber security compromised, on-chain crypto compliance provides an opportunity for financial institutions to rely on other institutions' attestations and use them for risk management without moving information or exposing it to the user. Sanctions can be enforced on-chain and updated in real time, to prevent any transaction from going through absent compliance. And reports can be administered automatically off chain, saving important time and providing law enforcement with better chances to prevent crime from happening. Saving the redundancy of duplicate KYC checks in every entry would reduce the compliance burden from the financial industry, improve customer and user experience, and allow compatibility of the AML infrastructure with the future of stablecoin and CBDC payments, with robust enforcement that does not rely on intermediaries.

There is thus a national opportunity to develop a decentralized financial utility that would modernize anti money laundering rules and provide for a modernized financial utility, that would be decentralized and resilient of security attacks and does not involve mass accumulation or transfer of personal information, as only cryptographic attestations would be shared along the ecosystem, rather than private information.

4.5 Rules versus Standards for Crypto Compliance

On-chain compliance represents a preference for rules over standards as a form of legal policy. We posit that rules should be preferred for financial regulation of Web3 environments: rules are forward-looking norms, setting a normative benchmark for behavior before it occurred and thus letting subjects the freedom to plan ahead their course of action given the rules of the game, while directing behavior in the socially desired pattern prescribed. Standards, on the other hand, are ex post norms that require normative application after each and every case to which the standard applies. Programmatic enforcement by rigid well-defined mechanical means can only support rules defined in great detail and in advance, rather than vague standards.

Consistent with the nature of financial regulation, certainty, uniformity and stability are core virtues we should apply, while flexibility and open-endedness would be less valuable. Consider, for example, the approach taken by the SEC recently regarding crypto regulation. In a speech given in September 2022, SEC Chairperson Gensler said "I've asked the SEC staff to work directly with entrepreneurs to get their tokens registered and regulated, where appropriate, as securities…Given the nature of crypto investments, I recognize that it may be appropriate to be flexible in applying existing disclosure requirements."[60]

The flexibility Gensler suggests as a merit is in fact a vice for Web3 environments, as it requires particular tailoring for each and every project. Flexibility is a feature of regulation by standards that require individualization and adaptation by the regulator. Rules, on the other hand, are uniform and certain and known to all parties ex-ante, so they can plan accordingly.

Typically, Web3 is based on open source, that allows users and developers to understand the contours of the arrangement before they leap in. The flexible standards in interpretation of SEC regulation that Gensler suggests intermediacy, as developers are required to step into the SEC and consult with the SEC before they code; an expectation that is completely obsolete given the culture of Web3. If rules were available and published, at least some of the developers would read and study them, and code accordingly. But requiring an appointment to be made with the SEC is not likely to effectively apply in the emerging global financial world of Web3; and enforcement action in hindsight is similarly harmful for economic progress and efficiency of legal policy at scale.

The debate between rules and standards is also a debate between general and particularized justice. Instead of solving one case at a time in a costly litigation process, rules set up a general framework that applies broadly. A rule based legal system allocates the discretion for the norm design to the rule maker, freeing users and developers from the expenditures involved in discretion of standard interpretation. This is particularly valuable in Web3, when uncertainty and lack of clarity hinder innovation and progress by casting doubts on the legitimacy of the investment. Consider the difference between a standard "drive safely" and a rule specifying specific speed limits. Our lives proceed more efficiently because by relying on posted speed limits we spend less time calculating how fast to drive. Moreover, they prevent discrimination and bias, by setting equal normative benchmarks for different parties, regardless of their background

[60] Gary Gensler, *Kennedy and Crypto* (Sept. 8, 2022), https://www.sec.gov/news/speech/gensler-sec-speaks-090822.

or their available resources. Rules could make Web3 regulation better, both from a fairness and from an efficiency perspective.

In fact, Web3 offers a promise for a fundamental shift in the methodology for rule making for the future of money. Emerging technologies now allow blockchains to enforce policies ex-ante by coding rules into the core payment infrastructure, providing normative boundaries for their use. On-chain compliance could set a normative benchmark for blockchain transactions, granting users and developers the freedom to plan ahead their course of action given the predetermined and clear rules of the game. Programming policies to the chain for automated enforcement can enhance ideas of self-reliance and nonintervention, consistent with the ethos of the emerging decentralized arena of Web3: by setting social norms in great detail and in advance, society creates a specific benchmark for adherence, and poses a choice for users whether to comply or bear the costs.

Instead of flexible standards that need to await interpretation by the courts, financial regulators could now use programmable policies to create a layer of legality upon which developers could create. That would achieve better predictability and better legal certainty as a whole, and would be a legal design much better fit for the needs and ethos of Web3, and allow for financial growth of this important cutting-edge sector of the economy.

5. CONCLUSION

The current tension between privacy and compliance represents an uneasy compromise in traditional financial services that will be tested as crypto markets evolve and achieve broader mainstream adoption. In this evolving ecosystem, it is clear that the current regulatory solutions, which rely upon financial intermediation and blockchain analytics premised on the immutable and transparent nature of the blockchain, will confront limitations; and that attempts to force the regulatory model on decentralized and peer-to-peer transactions will broadly sweep in innocent conduct and hamper innovation in this space. This paper has suggested an alternative solution that can harness the power of modern cryptography and blockchain programmability to overcome the seemingly binary choice between compliance and privacy. Regulators and law makers assessing approaches to govern this evolving space of financial activity should assess the possibilities of adopting these novel tools, to achieve higher efficiency for compliance on the one hand, and privacy and information security on the other.