Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs

By Joseph Burleson, Michele Korver, and Dan Boneh†

Introduction

Of all the utility that programmable blockchains offer – security, predictability, interoperability, and autonomous economies, among others – as of today, the most widely used blockchains do not offer privacy. This remains a key impediment to their widespread adoption. Although not all crypto tokens are solely – or even principally – financial instruments, and can be used for a variety of purposes within the growing web3 ecosystem, blockchain users do transact with each other on blockchains using digital assets. The current architectures of most existing blockchains rely on transaction transparency to promote trust, but this default transparency and lack of privacy increases the risk of consumer harm by permitting other blockchain users to view the transaction history and holdings of any wallet holder. The pseudonymity characteristic of blockchains is the principal protection against bad actors, but it is easily overcome. Modern blockchain analytics practices have shown that heuristic analysis of user interactions can be used to pierce this privacy, and anyone who transacts with a wallet holder can effectively see their entire financial profile. Consequently, although it provides a net benefit in tracing illicit financial activity, transaction transparency makes users of blockchain technologies particularly vulnerable to fraud, social engineering, and theft of assets by bad actors, as well as the inchoate harm caused by revealing sensitive financial data to third parties.

The transparent nature of public ledgers on blockchains stands in stark contrast to the default privacy of the traditional financial system, which arises from the recording of transactions on private ledgers maintained by financial intermediaries, supported by statutory rights to financial privacy and human controls on access to sensitive financial information. Indeed, regulations and guidance promulgated by the Department of the Treasury's (Treasury) Office of Foreign Assets Control (OFAC), responsible for the U.S. financial sanctions regime, and the Financial Crimes Enforcement Network (FinCEN), responsible for U.S. anti-money laundering regulations and supervision, along with their enabling statutes, have been designed to compel transparency to overcome the inherent opacity of the traditional financial system and the privacy it affords. The recordkeeping and reporting requirements arising from these statutes require financial intermediaries to maintain and disclose information to the government (as well as take other actions such as blocking access to assets) in order to support law enforcement investigations, stop terrorist financing, and advance national security policies, among other things. Importantly, these measures create *exceptions* to protected privacy rights and represent a balance – albeit an imperfect one – between privacy rights and compliance requirements.

None of these protections – neither the practical privacy protections afforded by the inherent opacity of private ledgers, nor the explicit legal recognition of rights to financial privacy – exists with respect to users on public blockchains. Moreover, attempts to import measures (such as customer identification and due diligence, colloquially known as "know your customer" or "KYC" requirements) risk undermining even the minimum levels of privacy afforded by pseudonymity, by creating "honeypots" of information that attract malicious attacks and insider threats. While compromise of such information causes consumer harm in the traditional financial system, it dangerously exacerbates the already heightened risk of theft, fraud, and even physical harm that exists as a result of full financial transparency.

While there are newer, more narrowly adopted layer-1 blockchains that primarily focus on privacy, for those blockchains that are not inherently private, users have to rely on a host of smart contract protocols and layer-2 blockchains that anonymize transaction data, many of which use zero-knowledge proofs, privacy-preserving cryptographic techniques, to achieve anonymity. These protocols and blockchains have commonly been derided as having solely nefarious purposes (including by being labeled "mixers"), and while it is irrefutable that a portion of their volume has ties to hacks and other illicit purposes,[1] there is undeniable value in advancing privacy-preserving technology for lawful purposes. In fact, such technologies could permit legitimate consumers to benefit from a level of financial privacy and consumer protection beyond what is enjoyed by consumers of traditional financial services. The same solutions that maximize privacy, however, may frustrate the government's ability to pursue investigations, combat illicit financial activity, or recover stolen assets in furtherance of law enforcement and national security goals. Does this mean that blockchain technology necessarily forces a choice between compliance to detect, prevent, and disrupt illicit financial activity, on the one hand, and privacy and consumer protection on the other hand?

This paper argues emphatically that the answer is no. Resolution of this tension using modern cryptographic techniques – unlike existing frameworks that rely on human controls – is not necessarily a zero-sum game. Reconciling the privacy needs of users and the informational and national security needs of regulators and law enforcement is both possible and necessary. This paper proposes potential use cases for zero-knowledge proofs in blockchain protocols that can achieve both sets of goals. First, we describe the basics of zero-knowledge proof technology, followed by an overview of relevant legal and regulatory regimes that may apply. Then, using Tornado Cash as an example, we lay out a number of high-level solutions that developers and policymakers might consider.

---

[1] *See Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume*, Chainalysis (July 14, 2022), https://blog.chainalysis.com/reports/cryptocurrency-mixers; *see also U.S. Treasury Sanctions Widely Used Crypto Mixer Tornado Cash*, TRM Labs (Aug. 8, 2022), https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash.

In writing this, the authors affirm the important premise, "regulate apps, not protocols."[2] In the United States, it's common practice for the application layer to perform sanctions screening using geo-fencing techniques and restricting user access through a variety of measures. While these restrictions are helpful, they are not fail-safe, and bad actors may nonetheless circumvent such controls. As a result, certain privacy-preserving technologies that may be susceptible to use by sanctioned parties have chosen to include restrictions at the protocol level to address national security concerns. The authors don't take the stance that all privacy-preserving technologies should make the same decision; developers should have the freedom to choose whether or not they want to adopt protocol-level restrictions to protect against use by illicit actors and potential regulatory liability. For those that choose to adopt protections, we simply offer up potential alternatives to consider which may make these solutions more effective, while also limiting the potential for them to be used for censorship.

Background

Achieving Privacy Using Zero-Knowledge Proofs

It is unlikely that blockchain technology will achieve mainstream adoption without ensuring privacy. For example, when it comes to financial infrastructure, potential users of blockchain-based payments systems may be highly reluctant to use these systems if their salaries or other sensitive financial information, including payments for services such as medical treatments, are publicly viewable. The same can be said for social networking services, decentralized lending protocols, philanthropic platforms, and any other use case where users value the privacy of their information.

The data corroborates that position. The 30-day moving average of cryptocurrency market value received by on-chain privacy-preserving services or protocols reached $52 million as of April 29, 2022, up nearly 200% over the preceding 12 months.[3] For context, many privacy-preserving protocols use algorithmic cryptography to facilitate one blockchain address depositing digital assets into a pool of similar fungible assets, followed by another blockchain address controlled by the same user withdrawing the same number and type of assets from that pool, effectively breaking the chain of custody and inhibiting the traceability of transactions. Certain of those protocols and some layer-2 blockchains use algorithms known as zero-knowledge proofs to anonymize transactions without exposing sensitive user information to the chain.

Zero-knowledge proofs enable private transactions on a public blockchain. At its core, a zero-knowledge proof is a way for one party, called a "prover," to convince another party, a "verifier," that a certain statement is true, while revealing nothing about the underlying data that makes the statement true. For example, the prover can prove knowledge of the solution to a Sudoku puzzle without revealing anything about the solution. More

[2] Miles Jennings, *Regulate web3 Apps, Not Protocols*, a16z Crypto (Sept. 29, 2022), https://a16zcrypto.com/web3-regulation-apps-not-protocols/.
[3] *See* Chainalysis, *supra* note 1.

interestingly, a person can prove they are old enough to buy alcohol or vote, without revealing the name and date of birth printed on their driver's license. (Technically, they would prove in zero knowledge that they have government-signed documents, and that their date of birth on these documents establish the requisite age of the person.) The proof convinces the verifier that this fact is true, without revealing any other information.[4]

One can build a variety of privacy mechanisms using zero knowledge tools. For instance, Alice can send funds to a service that keeps transaction details private, and the service gives Alice a receipt for her deposit. The service, as well as the public, learns that Alice sent funds. At a later time, when Alice wants to withdraw the funds from the service, she constructs a zero-knowledge proof that she has a valid receipt, and that she has not yet withdrawn the funds associated with that receipt. The proof reveals nothing about Alice's identity, but convinces the service that it is interacting with someone who is eligible to withdraw those funds. Here, the zero-knowledge proof is used to convince the service that the withdrawal claim is valid, while keeping the identity of the withdrawer private.

Critically, zero-knowledge proofs protect privacy by permitting selective disclosure of the information necessary to assess policy compliance, without exposing all of the underlying information. Zero-knowledge proofs can enable varying degrees of privacy, including complete privacy where no one can track a transaction, or privacy from everyone except for a few specific parties. While there are a number of lawful reasons why people may need strong privacy protection, these technologies can also be a magnet for bad actors. Just as overall usage of privacy-preserving protocols peaked in 2022, so did the relative proportion of value received from illicit sources, with illicit blockchain addresses accounting for approximately 23% of all funds sent to such protocols this year through Q2. Nearly all of that illicit activity originated from sanctioned entities or consisted of stolen funds.[5] Despite the privacy-preserving technology utilized by these protocols, blockchain analytics firms, like Chainalysis and TRM Labs, are sometimes able to track illicit funds flowing through these protocols where they do not have sufficient volumes to mask the activity, or where the volumes they do have are not sufficiently diverse.[6] Further, even when illicit actors exploit privacy-protecting technology, they still face challenges taking their assets off-chain, as fiat on-ramps and off-ramps are in most instances considered financial institutions in major financial centers and other jurisdictions across the globe, and thus subject to AML/CFT requirements.[7] However,

[4] The way a prover accomplishes this is by first encoding the statement to be proved as a series of polynomials (the sum of a series of algebraic terms) that are identically zero if and only if the statement is true. This encoding – often called the "arithmetization" of the statement – is the magical step that makes zero-knowledge proofs possible. The prover then convinces the verifier that the polynomials are indeed identically zero.

[5] *See* Chainalysis, *supra* note 1.

[6] *See North Korea's Lazarus Group moves funds through Tornado Cash*, TRM Labs (Apr. 28, 2022), https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash.

[7] "AML" is anti-money laundering, and "CFT" is countering the financing of terrorism. *See* Fin. Crimes Enf't Network, *History of Anti-Money Laundering Laws*, https://www.fincen.gov/history-anti-money-laundering-laws.

implementation and enforcement of these requirements globally is uneven at best, and non-existent in some jurisdictions, offering a favorable climate for illicit actors to exchange digital assets for fiat currency. As a result, although privacy-preserving protocols are critical to keeping legitimate user information private, they do create vulnerabilities within blockchain ecosystems for illicit actors to exploit. Compliance with international legal and regulatory regimes is complex, to be sure, but a standardized and regulatory-compliant implementation of zero-knowledge proofs in decentralized blockchain protocols can address some key vulnerabilities while at the same time benefitting web3 participants.

Applicable Regulatory Regimes

Understanding how zero-knowledge proofs can overcome the apparent binary choice between compliance and privacy requires an appreciation of the particular jurisdictional regulatory requirements that relate to combating illicit financial activity. In the U.S., regulations most likely to affect privacy-preserving protocols can be categorized into two primary legal regimes: (A) under the series of federal statutes and regulations commonly known as the Bank Secrecy Act (BSA) – (i) Customer identification program and customer due diligence requirements (commonly referred to as "Know Your Customer" or "KYC" standards) and (ii) transaction monitoring as well as other recordkeeping and reporting requirements;[8] and (B) under Presidential wartime and national emergency powers – U.S. sanctions programs.[9] Web3 market participants must address the legal requirements of both regimes in order to minimize any risk of enforcement for non-compliance and to mitigate against the illicit use of protocols and platforms. Further, any failure to comply may result in severe consequences, including civil penalties and criminal prosecution.[10]

The BSA requires certain financial institutions and other related entities to comply with a number of monitoring, recordkeeping, and reporting obligations. The purpose of these obligations is to assist FinCEN, OFAC, and law enforcement agencies with the identification, prevention, and prosecution of money laundering, terrorist financing, and fraud activity, as well as the identification and blocking of assets in the U.S. financial system belonging to sanctioned parties pursuant to national security and foreign policy goals. Full compliance under the BSA and sanctions regimes create a clear and

[8] 31 U.S.C. § 5311 *et seq.*

[9] *See* U.S. Dep't of the Treasury, *Office of Foreign Assets Control (OFAC) – Sanctions Program and Information*, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information .

[10] For example, in 2021, the alleged operator of Bitcoin Fog, a mixing service, was arrested and charged with money laundering, operating an unlicensed money transmitting business, and money transmission without a license in the District of Columbia. *See* Press Release, U.S. Dep't of Justice, Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer" (Apr. 28, 2021), https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

auditable paper trail of illicit activity for regulators and law enforcement to follow and is critical to their successful enforcement.[11]

BSA-covered or obliged entities include traditional financial institutions such as banks, as well as money services businesses (MSBs) such as currency dealers, exchangers, and money transmitters, among others.[12] FinCEN has further clarified that individuals and entities which issue, administer, or exchange Convertible Virtual Currency (CVC), or value that substitutes for currency, are considered MSBs as well, and therefore subject to all of the applicable compliance obligations under the BSA.[13] Depending on the facts and circumstances of a mixing service's operation or business model, a mixer could be deemed an MSB and subject to the registration and compliance requirements of the BSA. This is because certain mixing services can enable value that substitutes for currency to move from wallets within the platform to wallets outside of the platform.[14] In contrast, privacy-preserving decentralized blockchains likely do not involve money transmission. As FinCEN explicitly states in its most recent guidance, issued in 2019, non-custodial, self-executing code or software alone, even if performing mixing functions, will not at present trigger BSA obligations:

> *An anonymizing software provider is not a money transmitter. FinCEN regulations exempt from the definition of money transmitter those persons providing "the delivery, communication, or network access services used by a money transmitter to support money transmission services." [31 CFR § 1010.100(ff)(5)(ii)]. This is because suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission.*[15]

The application of sanctions compliance requirements is a bit less clear. The sanctions regimes administered by OFAC apply to all U.S. persons, both individuals and entities, wherever they reside, and require them to identify, block, and segregate transactions involving property of sanctioned parties. Although OFAC has stated that sanctions regimes do not apply to the publication of software and privacy-preserving technologies *per se*,[16] the failure to implement measures to prevent sanctioned parties from abusing

---

[11] 31 U.S.C. § 5311.

[12] *Definitions Relating to, and Registration of, Money Services Businesses*, 64 Fed. Reg. 45438 (Aug. 1999), https://www.govinfo.gov/content/pkg/FR-1999-08-20/pdf/FR-1999-08-20.pdf.

[13] Fin. Crimes Enf't Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[14] Money transmission involves the transmission of funds, CVC, or value that substitutes for currency to another location or person by any means. *See* Fin. Crimes Enf't Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[15] *Id.* at 20, 23-24.

[16] Frequently Asked Questions, U.S. Dep't of the Treasury's Off. of Foreign Assets Control ("OFAC"), No. 1076, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1076 ("While engaging in any transaction with Tornado Cash or its blocked property or interests in property is prohibited for U.S. persons,

these technologies – as discussed in further detail below – risks responses from OFAC that could undermine such technologies' viability, such as recently was the case with Tornado Cash.[17]

KYC Standards and Transaction Monitoring

Those individuals or entities whose business models are classified as MSBs must fulfill certain information collection and transaction monitoring requirements in order to meet their obligations under the BSA. MSBs are required to obtain KYC information from persons that use their services to conduct transactions, in order to verify the identity of such persons.[18] At a minimum, MSBs must obtain a user's name, address, and tax identification number as part of the KYC process.[19]

Post-onboarding, MSBs must also monitor transactions conducted through their platforms and report any suspicious activity that might signal illegal conduct by filing Suspicious Activity Reports (SARs). The BSA requires MSBs to file a SAR within 30 days if they know of or suspect that a transaction on their platform may involve illegal activity, provided that such transaction involves the transfer of at least $2,000 in the aggregate. In order to incentivize timely filing, the proper filing of a SAR with respect to a transaction will shield the MSB from all civil liability related to that transaction.[20]

While the BSA also imposes other recordkeeping and reporting requirements on MSBs such as the filing of Currency Transaction Reports (CTR) , this requirement currently does not apply to digital assets and is not immediately relevant for present purposes.[21]

Sanctions

FinCEN has full authority to administer the BSA, promulgate rules thereunder, and bring enforcement actions against those in violation of the BSA, but OFAC has a much broader jurisdictional mandate. Most economic sanctions come from authority delegated to the President in the International Emergency Economic Powers Act (IEEPA) and the National

---

interacting with open-source code itself, in a way that does not involve a prohibited transaction with Tornado Cash, is not prohibited. For example, U.S. persons would not be prohibited by U.S. sanctions regulations from copying the open-source code and making it available online for others to view…").

[17] Press Release, U.S. Dep't of the Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[18] Alexandra D. Comolli & Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DOJ J. FED. L. & PRAC. 3 (2021).

[19] 31 CFR § 1010.410.

[20] 31 CFR § 1022.320(a)(1); 31 U.S.C. § 5318(g)(3).

[21] CTRs require reporting of cash or coin transactions over $10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to over $10,000 in a single day. They do not apply to digital assets currently, although there is a pending rule that could expand CTR-like requirements to CVC transactions meeting certain criteria. *See* 31 CFR § 1010.311; *see also* Fin. Crimes Enf't Network, Notice to Customers: A CTR Reference Guide, https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf.

Emergencies Act (NEA).[22] Thus, sanctions are a wartime and national security-related power enacted via Executive Order. OFAC oversees all financial transactions in the U.S. and may sanction any individual, entity, or country that poses a threat to national security. As a result, if an OFAC-designated person or entity has an interest in any transaction processed through or property held by any U.S. person or entity, including but not limited to BSA-obliged entities such as MSBs and banks, the U.S. person or entity would be required to (i) block (freeze) the prohibited transaction, and any accounts or property related to the specified person, and/or (ii) place any funds received in connection with such transaction into a segregated, blocked account, and (iii) file certain reports with OFAC. In either case, no U.S. person or entity may process such transaction and/or release such funds until OFAC removes the individual or entity in question from the sanctions list, the applicable sanctions program is rescinded, or OFAC explicitly authorizes the release of withheld funds through the granting of a license.[23]

For sanctions relating to cryptocurrency transactions, the authority generally comes from EO 13694 which focused on "significant malicious cyber-enabled activities."[24] Individuals who violate economic sanctions may face civil or criminal penalties.[25] It should be noted that the administrative, or civil, liability standard for sanctions violations is strict liability, meaning that one can be held liable for sending or receiving a transaction or failing to block property associated with a sanctioned person, entity, or country, even if there was no intention to do so.[26] This effectively imposes a due diligence requirement to inquire as to the source of funds when engaging in financial or business activities. Criminal liability, on the other hand, requires a showing of willfulness – that the person violating sanctions meant to do so. Criminal prosecutions for sanctions violations are brought by the Department of Justice under IEEPA or money laundering statutes codified in Title 18 of the U.S. Code.[27] The important takeaway, however, regarding sanctions liability and OFAC compliance requirements is that these obligations apply to *all* persons and entities in the U.S. or doing business in the U.S. and are not tied to whether or not the person or entity is BSA covered.

Optimizing Privacy Protocols to Mitigate Illicit Finance Risk

The potential for privacy enhancements afforded by zero-knowledge proofs stands in tension with the aforementioned regulatory framework. The technology's ability to shield

---

[22] *See* 50 U.S.C. § 1702(a); Nina M. Hart, *Enforcement of Economic Sanctions: An Overview*, Congressional Research Service Reports (Mar. 18, 2022), https://crsreports.congress.gov/product/pdf/IF/IF12063.
[23] Fed. Fin. Institutions Examination Council, *Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual* (2021), https://bsaaml.ffiec.gov/manual/OfficeOfForeignAssetsControl/01.
[24] *See* OFAC Cyber-Related Sanctions Frequently Asked Questions, Nos. 444, 445, and 447, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546. Sanctions involving cryptocurrency may also come from country-specific executive orders, such as those addressing Russia, Iran, or North Korea.
[25] *See* 31 CFR Apx. A to Pt. 501; 50 U.S.C. § 1705.
[26] Civil liability arises without having knowledge or reason to know one was engaging in a sanctions violation.
[27] *See, e.g.*, 18 U.S.C. §§ 1956, 1957, and 1960.

transaction details means it may not readily lend itself to fulsome compliance with regulations such as BSA requirements – though it remains an open question whether and to what extent smart contracts and code are subject to the requirements under the regulations described. As mentioned above, in its 2019 guidance, FinCEN explicitly exempts software code from the BSA's scope, and thus a truly decentralized protocol with no individual or group behind its operation is not required to – nor is it even clear how it could – collect and retain KYC information or file SARs on users. Similarly, the enabling statutes and cybersecurity executive order which would govern the imposition of any sanctions refers to "property and interests in property" of targeted individuals and entities, which suggests that software and computer code is itself outside the scope of sanctions.[28] And recent guidance from OFAC seems to indicate that publication of software is not itself a sanctionable activity.[29] However, in light of OFAC's designation of certain smart contract addresses associated with Tornado Cash, this conclusion is far from clear.

Nevertheless, zero-knowledge proofs can be designed to mitigate some risks of exposure to illicit financial activity and economic sanctions liability through privacy-enhancing protocols, including mitigation of the very national security risks that OFAC sanctions seek to address. In particular, there are several measures that privacy-focused protocols could implement to better manage these risks, without undermining their effectiveness. Three feasible measures are summarized below, each of which is evaluated in the context of the privacy-protecting protocol Tornado Cash.

The Tornado Cash Example

One way of demonstrating the potential for zero-knowledge proofs to overcome the current binary choice between potential liability under existing sanctions regimes raised by privacy-enhancing technologies is through the lens of Tornado Cash – the privacy-enhancing protocol recently sanctioned by OFAC. Tornado Cash is a protocol deployed on the Ethereum blockchain that seeks to anonymize user assets in order to protect their privacy. Anyone could send funds from their Ethereum address to the Tornado Cash smart contracts, and those funds would remain deposited in the contracts until the owner chose to withdraw them. Typically, users would wait anywhere from several weeks, to months, or even years before withdrawing, as the intervening time

---

[28] *See* OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 15, 2021) (stating that sanctions compliance programs and risk assessments apply to "companies"), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf [hereinafter: "OFAC Guidance"]; *but see* Frequently Asked Questions, OFAC, No. 445, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546, (stating "[a]s a general matter, U.S. persons, including firms that facilitate or engage in online commerce, are responsible for ensuring that they do not engage in unauthorized transactions or dealings with persons named on any of OFAC's sanctions lists or operate in jurisdictions targeted by comprehensive sanctions programs. Such persons, including technology companies, should develop a tailored, risk-based compliance program, which may include sanctions list screening or other appropriate measures.").

[29] Frequently Asked Questions, OFAC, No. 1076, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1076.

period (during which other users deposit and withdraw funds) can increase or decrease the effectiveness of Tornado Cash's privacy-preserving features. Upon withdrawal, the protocol utilized zero-knowledge proof technology to transfer the funds to a new Ethereum address, breaking the link between the address from which the funds were initially deposited into Tornado and the new address to which the funds were later withdrawn from Tornado.[30] The Tornado Cash protocol is immutable, trustless, and fully-automated.[31] The anonymity provided by Tornado Cash depended upon multiple users simultaneously employing the service to break the connection between wallet addresses used for deposits and withdrawals. In addition, users maintained a certificate that only they could reveal which proved ownership of the deposited tokens. Consistent with the recent uptick in illicit mixer usage, the Tornado Cash platform was similarly and frequently used to launder stolen funds. For example, in the hack of the Ronin bridge in April 2022, approximately $600 million was stolen from the bridge and transferred to an Ethereum address owned by the attacker. A few days later, the hackers moved some of the stolen funds into Tornado Cash.[32] On August 8, 2022, OFAC designated, among other things, the website tornado.cash and several Ethereum addresses associated with the service, many of which were smart contract addresses without an identifiable key holder.[33] In the public announcement accompanying the designation, Treasury pointed to over $7 billion in illicit proceeds laundered through Tornado Cash, including $455 million laundered by the North Korean state-sponsored hacking syndicate known as the Lazarus Group, and significant sums associated with the Harmony Bridge[34] and Nomad Heists.[35] Although users engaged in a significant amount of legitimate transaction activity through Tornado Cash, Treasury made the choice to take action against the protocol and its smart contracts despite considerable collateral impacts on innocent third parties, including preventing non-sanctioned individuals from withdrawing fully legitimate funds deposited using the protocol. This issue arises from the decentralized and non-custodial nature of Tornado Cash, which makes it difficult to identify an organization or individual responsible for its activities. As a result, applying traditional sanctions enforcement techniques and blocking property interests in this context can pose technical legal challenges. Although such protocols are sometimes cast solely as attempts to circumvent regulatory requirements, from a cybersecurity perspective, the technical architecture of Tornado Cash can also represent the robust privacy-preserving technology necessary to deter unauthorized third parties and malicious actors from obtaining sensitive information of

---

[30] *See generally* Tornado Cash, https://tornado.cash (2022).

[31] A new version of Tornado Cash, called Nova, supports direct account-to-account transfers without having to first withdraw funds from Tornado. *See generally* Tornado Cash Nova, https://nova.tornadocash.eth.link (2022).

[32] Tim Hakki, *Nearly $7M of Hacked Ronin Funds Sent to Privacy Mixer Tornado Cash*, Decrypt (Apr. 4, 2022), https://decrypt.co/96811/nearly-7m-hacked-ronin-funds-sent-privacy-mixer-tornado-cash.

[33] *See* OFAC Cyber-Related Sanctions Frequently Asked Questions, Nos. 1076 and 1095, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546.

[34] *See* Elizabeth Howcroft et al., *U.S. Crypto Firm Harmony Hit by $100 Million Heist*, Reuters (June 24, 2022), https://www.reuters.com/technology/us-crypto-firm-harmony-hit-by-100-million-heist-2022-06-24.

[35] *See* Elizabeth Howcroft, *U.S. Crypto Firm Nomad Hit by $190 Million Theft*, Reuters (Aug. 3, 2022), https://www.reuters.com/technology/us-crypto-firm-nomad-hit-by-190-million-theft-2022-08-02.

individuals and businesses who operate on-chain. This approach is preferred and may be technologically far superior to the traditional operational controls restricting access to information that more centralized custodial systems impose, and that have proven increasingly vulnerable to malicious attacks and insider threats.

In its press release accompanying the OFAC designation, Treasury indicated that "[d]espite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors . . . ."[36] In fact, and as described in more detail below, Tornado Cash did have some technical controls in place to guard against the platform's use for illicit financial activity. The question is – were there more effective technical controls, such as ones leveraging zero-knowledge proofs, that Tornado Cash could have implemented and that would have persuaded Treasury not to take the actions that it did? Let's consider those zero-knowledge proof solutions, including some which Tornado Cash implemented, and others that might improve effectiveness. While none of these approaches alone is a silver bullet, taken together they may improve the ability to detect, deter, and disrupt illicit financial activity and the use of privacy protocols by sanctioned state actors. These are: (i) deposit screening – checking wallets making inbound transactions against blocklists and allowlists; (ii) withdrawal screening – checking wallets that are requesting returned funds against blocklists and allowlists; and (iii) selective de-anonymization – a feature that would provide federal regulators and law enforcement with access to transaction information.

Deposit Screening

Digital assets native to the Ethereum blockchain or bridged onto it from another chain can be swapped for ETH and deposited in Tornado Cash in an attempt to preserve the privacy of users' transactions. To prevent deposits of assets coming from sanctioned persons or wallets connected with exploits or hacks, Tornado Cash used deposit screening that relied on a "blocklist" of designated addresses. The additional use of an "allowlist," however, could be used to address national security concerns while also minimizing risks to lawful users of the protocol, as further outlined below.

Blocklisting

Tornado Cash's deposit screening enabled it to restrict automatically who can use the protocol by blocking any proposed deposits from addresses that are sanctioned or otherwise blocked by the U.S. government. Tornado Cash accomplished this by utilizing a blockchain analysis firm's on-chain oracle service for testing whether an address is currently designated on economic or trade embargo lists (or "blocklists") from various entities, including the U.S., E.U., or U.N.[37] Tornado Cash's smart contracts would "call" the

[36] *See supra* note 17.

[37] *See Chainalysis oracle for sanctions screening*, Chainalysis, https://go.chainalysis.com/chainalysis-oracle-docs.html.

analytics firm's contract before accepting funds into one of its pools.[38] A deposit request would fail if the funds are from one of the blocked addresses included on the analytic firm's Specially Designated Nationals (SDN) list.

While deposit screening using blocklists is a good first step, there are several practical problems with this mechanism. First, when cybercriminals steal funds from a victim, they can immediately move the funds into Tornado Cash before the victim even realizes that the funds are gone, and certainly before an analytics firm has flagged the funds as stolen or on the SDN list in their software. Second, in the event that the cybercriminal's address is placed on the SDN list prior to depositing in Tornado Cash, the thief could simply transfer the funds to a new address, and immediately deposit the funds into Tornado Cash from that new address, before the new address is added to the sanctions list. Sophisticated hacking syndicates, like the DPRK's Lazarus Group, use these techniques quite effectively to avoid detection. But, blockchain analytics firms attempt to overcome this limitation by using change address analysis and heuristics to identify non-designated wallets that are also controlled by designated groups.[39] Lastly, relying on a non-governmental entity as the arbiter of truth with respect to who or what is on a sanctions list could result in accuracy issues that would be difficult to identify and rectify. For instance, an analytics firm could mistakenly include an address on its blocklist, and it is unclear whether the owner of such an address would have any recourse to have the mistake fixed (unlike in the case of traditional financial institutions which can field complaints from their customers). There is also the problem of which sanctions list gets added, since all sanctions represent policy decisions of the issuing government.

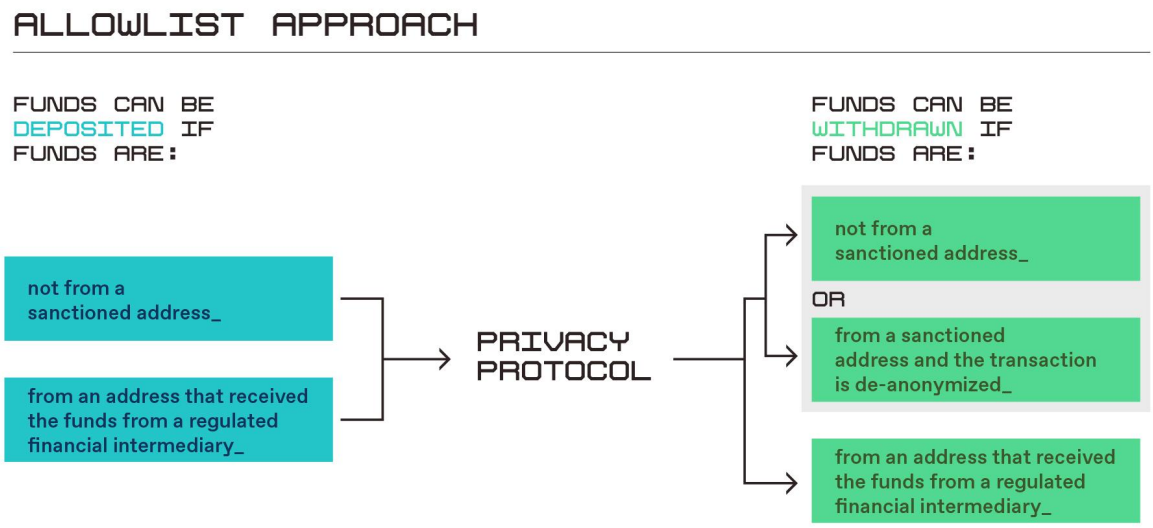
Allowlisting

In order to reduce the risk that an analytics firm or government entity could use blocklisting to unfairly censor law-abiding users, privacy-preserving protocols might consider a more robust form of deposit screening that also relies on an "allowlist" of wallet addresses to which deposit screening restrictions would not apply. That allowlist would consist of wallet addresses associated with regulated financial intermediaries – such as fiat on-ramps like Coinbase – that conduct comprehensive KYC screening as part of their onboarding processes, thereby obviating the need for the privacy-preserving protocol to screen those addresses, as depicted below.

---

[38] Jeff Benson, *Ethereum Privacy Tool Tornado Cash Says It Uses Chainalysis to Block Sanctioned Wallets*, Decrypt (Apr. 15, 2022), https://decrypt.co/97984/ethereum-privacytool-Tornado-cash-uses-chainalysis-block-sanctioned-wallets.

[39] *See Brian Armstrong & Vitalik Buterin Discuss Decentralization, Privacy, and More*, Coinbase: Around the Block, at 35:00 (Aug. 30, 2022) (available on Spotify), https://open.spotify.com/episode/2vzctO7qgvYqGLKbnMnqha?si=X3eu221lRvGlJn3kd4tWFA&nd=1; *see, e.g.*, Ben Fisch, *Configurable Privacy Case Study: Partitioned Privacy Pools*, Espresso Systems (Sept. 11, 2022), https://www.espressosys.com/blog/configurable-privacy-case-study-partitioned-privacy-pools.



This approach would allow a user to deposit funds in a privacy-protecting protocol only if the deposit address (i) is not on the applicable analytics firm's SDN list (i.e., the address *is not* on a blocklist) or (ii) received said funds from a regulated financial intermediary (i.e., the address *is* on the allowlist). That allowlist could be managed and updated over time by the decentralized autonomous organization (DAO) that controls the protocol or could be sourced from an on-chain oracle of addresses associated with regulated financial intermediaries (similar to the blocklist oracle operated by Chainalysis). Certain privacy-preserving technologies could take this concept a step further by bridging their protocol directly to regulated financial intermediaries, allowing users to deposit funds directly from those intermediaries into the protocol, without needing to transfer the funds to a separate wallet address first.

Utilizing both a blocklist and an allowlist as part of the deposit screening process has several distinct advantages over a blocklist-only approach. First, a lawful user that is either erroneously or maliciously added to a blocklist would be able to avoid censorship so long as they utilized a regulated financial intermediary to deposit their funds into the protocol. And since most unlawful actors should not be able to establish an account with a regulated financial intermediary, they could not take advantage of the allowlist and would remain subject to censorship, thereby addressing national security concerns. Additionally, an allowlist approach would improve privacy for the customers of all regulated financial intermediaries, as it would guarantee their ability to enjoy the benefits of privacy-preserving protocols without fear of censorship.

Ultimately, while deposit screening would facilitate Tornado Cash's obligations to block prohibited transactions, for other privacy service providers that may be deemed an MSB

and subject to the BSA, or for individuals or entities that may be required to perform a sanctions-related risk assessment of business activities, it would not improve those entities' transaction monitoring capabilities for risk assessment purposes.[40] Deposit screening is a good first step, but it is unlikely to reduce illicit finance use of the protocol completely.

Withdrawal Screening

For those wallet addresses that aren't included on an allowlist as outlined above, one additional approach to deposit screening would be to check the oracles on withdrawal and block any proposed withdrawals by sanctioned addresses or addresses that have been identified as associated with illegal activity. For example, suppose an illicit actor sends funds to Tornado Cash from an address immediately following a hack. At the time of the deposit, the address is not on the allowlist and has not been identified as being associated with stolen funds or sanctioned individuals or entities, and the deposit is successfully completed. However, if the illicit actor attempts to withdraw the funds at a later time, and during the intervening time period the address is flagged as being associated with stolen funds or on a sanctions list, then the withdrawal request will fail. The funds will remain frozen, and the thief will not be able to withdraw them. This approach has multiple benefits. First, it prevents the thief from laundering the funds with the Tornado Cash protocol. Second, Tornado Cash's implementation of a withdrawal checkpoint acts as a deterrent and should make it clear to nefarious actors that if they send stolen funds to Tornado Cash, those funds could be frozen by the smart contracts indefinitely, preventing them from accessing the fruits of their illicit activity. Such a deterrent would only affect cybercriminals and not impact law-abiding users of Tornado Cash. Indeed, given the deposit time period characteristic discussed above, and the likelihood that illicit actors would park funds in Tornado Cash for longer time periods in order to most effectively anonymize their source, this withdrawal screening feature would be very useful in its ability to screen against continually updating Treasury sanctions lists.

Although withdrawal screening can address many of the shortcomings of deposit screening, like deposit screening it does little to address any necessary risk assessments.[41] In addition, it would perpetuate Tornado Cash's reliance on blockchain analytics firms' faithful operation of sanctions oracles. Further, as with deposit screening, there is also the problem of government censorship – only in the case of withdrawal screening, a government's misuse of the sanctions list could result in a user losing its funds.

Selective De-anonymization

Selective de-anonymization is a third approach to meeting potential regulatory requirements, and it comes in two flavors: voluntary and involuntary.

[40] *See* OFAC Guidance at 12-16 (outlining risk assessment obligations).
[41] *Id.*

Voluntary Selective De-anonymization

Through its deposit receipt function, Tornado Cash implemented a form of voluntary selective de-anonymization, which provides a person who believes that they were erroneously added to a sanctions list the option to de-anonymize the details of their transaction to selected or designated parties.[42] If a similar voluntary de-anonymization function was instead coupled with withdrawal screening of wallet addresses not on an allowlist, a user could opt to de-anonymize their transaction, and the Tornado contract responsible for withdrawals would remove any block in place as a result of the withdrawal screening process described above. As a result, a user would receive its funds, but the user would not have received the benefits of Tornado's privacy-preserving technology, as its withdrawal address would clearly be linked on-chain to its deposit address. Voluntary de-anonymization would enable protocols like Tornado Cash to address certain shortcomings of withdrawal screening (e.g., innocent users would not be at risk of getting their funds frozen), but it would also reduce the effectiveness of withdrawal screening as a deterrent because bad actors would then be able to withdraw their funds from Tornado by merely de-anonymizing their transaction. In that scenario, illicit users would receive no benefit at all from having used the privacy-enhancing service.

Involuntary Selective De-anonymization

Involuntary selective de-anonymization is an additional measure that could be integrated into Tornado Cash's smart contracts to provide the government with the ability to track and trace illicit proceeds. While the applicability of BSA requirements to non-custodial web3 services is not likely, the traceability associated with blockchain protocols represents one key control to preventing illicit financial activity more broadly, including by sanctioned parties. Involuntary selective de-anonymization represents a powerful tool for maintaining traceability for authorized purposes while protecting privacy against malicious actors and unauthorized third parties. The key question is, who maintains the private key to unlock traceability?

One solution may involve providing a private key to a neutral gatekeeper-type organization or similar trusted entity, and another private key to government authorities. Both keys would need to be used to de-anonymize a deposit-and-withdrawal transaction that did not originate from a wallet address on the allowlist, and the details of such a transaction would only be revealed to the law enforcement agency that requested such de-anonymization. The role of the gatekeeper organization would be to resist de-anonymization without law enforcement first obtaining and presenting a valid warrant or court order for the de-anonymization. This would not only enable law enforcement to identify the source address that provided the funds used for any Tornado Cash withdrawal, thereby allowing the government to carry out its enforcement and national

[42] *See generally* Tornado Cash, *Tornado.cash compliance*, Medium (June 3, 2020), https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370.

security mandate, but it would also alleviate the government from the burden of holding the keys, which would be suboptimal for both the government and Tornado Cash's users.

There are several challenges associated with this approach. First, it is not clear which entities would have access to the private keys. No known gatekeeper organization in operation today is set up to manage such a process. Further, there are numerous jurisdictional issues. Will every country – even repressive regimes – have its own private keys, providing them access to transaction data? If so, how does one ensure that such regimes do not de-anonymize transactions of U.S. citizens? Also, how would the gatekeeper organization and government authorities manage their keys to ensure that they cannot be stolen? These questions are not new. They come up in every discussion of key escrow, which is what involuntary selective de-anonymization is. This solution is perennially unpopular and rife with operational challenges – the idea of a "back door." It is nonetheless an option that developers could consider in order to satisfy regulatory requirements or to mitigate against the use of platforms for illicit purposes.

One possible solution to the foregoing challenges would be to allow a user, during withdrawal, to choose which public key they want to use to encrypt the address.[43] The Tornado Cash contract might have multiple law enforcement public keys, say one public key for each country. During withdrawal, the user can choose which public key to encrypt with based on its local jurisdiction. The user may need to provide evidence of its jurisdiction, and that would determine which public key it uses for encryption. That evidence could be hidden under the zero-knowledge proof, so that no one other than the relevant government agency will learn the jurisdiction of the withdrawal.[44] In theory, this would address the issue of repressive regimes having access to a transaction's secret key, but it does not address the possibility that a malicious government could require the keyholders to provide their private keys under the guise of a bona fide – but bad faith – legal process.

For those BSA-obligated entities, selective de-anonymization would have the benefit of retaining the regulatory feasibility of withdrawal screening, including the ability to conduct OFAC-mandated sanctions screening, as well as the ability to collect KYC information and transaction data, and potentially file SARs. Moreover, the involuntary selective de-anonymization method outlined above could be modified such that the two keyholders would only have private keys for information specifically required to be collected, retained, and reported under the BSA (e.g., KYC information and SARs), and could only present those keys to FinCEN and OFAC, or to law enforcement upon service of valid legal process. That approach would help to ensure the privacy of users' data, while allowing government agencies to meet their regulatory mandates.

Conclusion

[43] The newer Tornado Nova protocol supports private transfers while the funds are in the Tornado system. In this case, the "address" encrypted under the law enforcement public key must be the entire chain of transactions that led to the funds currently being withdrawn – more data than just a single address.
[44] *See* Fisch, *supra* note 39.

In order for web3 technologies to flourish in the United States, the development of privacy-protecting regulatory solutions is crucial. In formulating these approaches, zero-knowledge proofs can supply a powerful tool for keeping cybercriminals and adversarial state actors from using blockchain technology for illicit purposes while still protecting the privacy of users' personal information, data, and financial activities. Depending on the operational and economic model and regulatory compliance obligations for a given protocol or platform, use of zero-knowledge proofs could enable deposit screening, withdrawal screening, and selective de-anonymization to meet those obligations and better protect the ecosystem from illicit use and prevent harm to the security of the U.S. and other nations. The diversity of activity in the blockchain space may require developers and founders to consider multiple approaches, including those posed in this paper, in addressing illicit finance risk.

Reiterating the previously discussed principle that protocols should not be regulated and that developers must have total freedom to choose whether or not they want to adopt protocol-level restrictions to alleviate these important risks, it is the authors' hope that these ideas will spark creative discussion, further research, and development around the possibilities of zero-knowledge proofs among builders and policymakers alike.

***

Acknowledgements: With thanks to Jai Ramaswamy and Miles Jennings for their feedback and contributions to the concepts in the piece, including Miles's "allowlist" proposal. Thanks also to David Sverdlov who helped put this together.

***

†**Joseph Burleson** is an associate general counsel at a16z crypto, where he advises the firm and its portfolio companies on legal, governance, and decentralization matters.

Michele Korver is the head of regulatory at a16z crypto. She previously served as FinCEN's Chief Digital Currency Advisor, DOJ's Digital Currency Counsel, and as an Assistant United States Attorney.

Dan Boneh is a senior research advisor at a16z crypto. He is also a professor of computer science at Stanford University, where he heads its Applied Cryptography Group; co-directs the Stanford Center for Blockchain Research; and co-directs the Stanford Computer Security Lab.