Tornado Cash: The End of Blockchain Neutrality?

The principle of "*network neutrality,"* first coined by Columbia University professor Tim Wu in 2003, holds that all internet packets shall be treated equally and consistently—irrespective of their content, source, or destination. The demand for net neutrality was a rallying cry of early internet activists who were concerned that allowing Internet Service Providers (ISPs)— supposed to act as "mere conduits"— to unilaterally prioritize certain packets for monetary compensation from content providers eager to deliver content more rapidly to their customers) would necessarily undermine competition and democratic participation on the internet. Indeed, if publishers can pay for their content to be delivered before that of their competitors, the ideal notion of a "free market of ideas" will turn into an actual "marketplace" where paid-for ideas will take priority over other, non-sponsored ones. Beyond the obvious implications for competition, this practice might also jeopardize the basic tenets of democracy, as the Internet may progressively evolve from being a public agora and open space for deliberation to becoming an increasingly commercialized and commodified space, where people have to pay to be heard louder (or faster). Hence, the proponents of network neutrality deem regulation necessary to protect users and content providers from discriminatory treatment by ISPs, in order preserve the principle of permissionless innovation and democratic participation.

Public and permissionless blockchain networks rely on the work of specific network agents (miners and validators) for processing transactions by including them in a block. As these networks are increasingly used to process large financial transactions, they also present opportunities for discriminatory treatment. Just as network neutrality plays an important role in preserving an open and permissionless web, the principle of "blockchain neutrality" is equally important to guarantee the equality of all network users in an open and permissionless Web3 ecosystem.

Miners and validators are responsible for maintaining a blockchain network by aggregating a series of transactions into a new block that will be appended to the current chain of blocks. Most public and permissionless blockchain networks operate according to an economically-driven incentive system, whereby the greater the fees associated with a transaction, the more likely it is that such a transaction will be included in the next block. This type of "paid prioritization" is precisely what the principle of net neutrality is trying to prevent: the prioritization of packets (or transactions, in the blockchain case) to maximize one's economic interests. Yet, in the case of a blockchain, paid prioritization is a "necessary evil" to guarantee the proper operations of the network, as transaction fees represent a key incentive for miners and validators to include the corresponding transactions into a block. This means that network users are not only *allowed*, but also *expected* to reward (*i.e.* to "bribe") these transaction processors, given that transactions with the highest fee will be processed faster than those associated with a lower fee.

Accordingly, the notion of blockchain neutrality is much narrower than the traditional concept of network neutrality. In fact, the economic discrimination inherent in the protocol's rules of most public and permissionless blockchains departs from the strict non-discrimination principle of net neutrality. Yet, blockchain neutrality subsists insofar as all transactions submitted to a blockchain network are treated *equally* and *consistently* according to the protocol rules, in a way that is transparent for all to see. Although the "neutrality" of this model is clearly imperfect, the blockchain neutrality principle is an important one, to the extent that it enables users to remain confident that the higher the transaction fees, the faster the processing of their transactions will be—independently of the content, origin, or destination of these transactions.

Efforts at undermining blockchain neutrality have already been attempted in the past. Already in 2013, in the aftermath of the FBI's shutdown of Silk Road (a shadow marketplace using Bitcoin to facilitate the sale of illicit goods or services), Bitcoin core developer Mike Hearn suggested the introduction of a new feature into the Bitcoin client that would differentiate between "clean" transactions and "tainted" transactions, i.e., transactions that can be traced back to an address that has been declared as 'criminal' by the government. This attempt failed, as it soon became clear that, even if Bitcoin core devs were to develop a new client with such a feature, no one could force people to adopt this software. Indeed, no Bitcoin miner would willingly agree to install a software that would dramatically reduce the profits that can be derived from the Bitcoin network. Hence, even if the US government had forced software developers to implement such a feature, it would have had no recourse against network participants who refused to adopt the revised Bitcoin client. Bitcoin's distributed consensus ultimately depends on the miners' choice to adopt a particular protocol over another—a decision that is often based on a combination of economic interests and ideology. In the case of Bitcoin, the crypto-libertarian ideology espoused by a large majority of miners is core to the belief that the Bitcoin network should remain immune from any governmental—and therefore regulatory— intervention.

Now, the US government might have found a new way to undermine blockchain neutrality, by regulating the way in which US persons may or may not interact with a particular account on a blockchain network. And this was done through a very powerful, and somewhat controversial means, by relying on the brute force of US sanctions.

On 8 August 2022—and again on 8 November 2022—the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, a blockchain-based *software system* that enables cryptocurrency users to preserve the privacy of their transactions. A user can send cryptocurrency to the Tornado Cash smart contract from one address—where it is pooled with deposits from other users—and then withdraw it to another address. In doing so, the link between the deposit and withdrawal addresses is obfuscated, without the user ever losing control over their cryptocurrency. This mixing service can be used for both legitimate privacy-preserving purposes (for example, donating to a political cause without making the details public) and illegitimate purposes—with both the first and second sanction notices explicitly mentioning the use of Tornado Cash by a collective of North Korean hackers, known as the Lazarus Group, for laundering proceeds from their hacks of US-based crypto-firms and supporting the activities of the North Korean State, including the development of its weapons of mass destruction program. The intention of this sanction was to deter people from transacting with the specified smart contract addresses—without prejudice to the people who (re)publish or access the code.

The sanctioning of cryptocurrency mixers has already happened in the past. In May 2022, the US Treasury sanctioned Blender.io, another cryptocurrency mixer that had also been allegedly used by North Korean hackers to launder money. Yet, while the sanctioning of Blender.io did not generate much controversy in the blockchain community, the sanctioning of Tornado Cash was regarded as highly problematic due to the "entity" that these sanctions were targeted at.

With Tornado Cash, the subject of the OFAC sanction is not a legal person, but rather a collection of smart contracts deployed on Ethereum. Unlike the case of Blender.io which was operated by a company that could either modify or shut down its operations, the operations of the sanctioned Tornado Cash smart contracts is not under the control of anyone. Hence, no one can intervene to stop or modify the operation of this cryptocurrency mixer—not even the team that developed the software and deployed the smart contracts in the first place. Regardless of whether this qualifies as a feature or a bug, such a design choice was deliberately made by the Tornado Cash team. Indeed, while a particular governance system was put into place in order to allow for the Tornado Cash protocol to evolve, the immutability of the smart contracts that pool and mix the cryptocurrencies had to be preserved at all costs. As the developers team explained on Medium on 20 May 2020, their objective was to live "by the precepts that code is law."

In that regard, less than a decade ago, Ethereum co-founder Gavin Wood gave a presentation in London where he argued that blockchain-based systems are fundamentally *alegal*. Alegality, Wood contended, was a feature of systems that "cannot care" whether their actions are "interpreted as legal or illegal." Behind his reasoning was a simple idea: blockchains and the systems built around them cannot be regarded as either the subject or the object of the law—they exist beyond the purview of the law. As such, the blockchain protocol and associated smart contracts constitute a new form of *regulation by code* (an extreme interpretation of Lessig's "code is law") which defines the rules that regulate conduct on the underlying blockchain network.

This reasoning, while true to an extent—in that the law cannot directly affect blockchain code, no more than it can affect the weather—also displays a certain degree of naïvité, as cases such as the Tornado Cash sanctions and the FTX chapter 11 bankruptcy application have made it clear that law can at least indirectly affect the operation of blockchain code by regulating the people and organizations interacting with such code. As we have argued elsewhere, this includes, amongst others, custodian wallets, cryptocurrency exchanges, as well as the users who submit transactions to the network and the miners or validators who are in charge of processing such transactions and including them into a block.

While the sanctions are intended to prevent US persons and organizations from transacting with the black-listed smart contracts addresses—at the risk of incurring strict criminal liability—it is unclear whether a new form of vicarious liability might extend to miners and validators who chose to include these illicit transactions into a block. Indeed, under certain circumstances, block producers might be held liable for 'aiding and abetting' in the commission of a crime, as they are receiving economic benefits from these activities by collecting transaction fees for processing illicit transactions. This is reflected in the fact that the Ethereum validators using the Flashbots' relay software for Maximum Extractable Value (MEV)—who currently account for more than 50% of Ethereum block producers—are censoring by default all of the transactions originating from the sanctioned Tornado Cash addresses. According to the Flashbots team, this censorship is driven by a desire to remain perfectly compliant with regulatory requirements. Such a "collateral effect" could have been foreseen, perhaps even purposefully considered by US federal officials, who almost certainly have the capabilities to identify a large portion of Lazarus group's financial flows, given the large amounts of money involved.

As blockchain lawyer Gabriel Shapiro recently argued, miners and validators are the most obvious targets of state regulation intended to censor blockchain transactions, because they have the ability to selectively pick and choose among transactions. Yet, holding miners and validators (acting as 'mere conduits') vicariously liable for the processing of transactions that originate from, or point towards, an OFAC-sanctioned address would further undermine the principle of blockchain neutrality and ultimately reduce confidence in the operation of the blockchain network, as users might no longer be guaranteed that transactions will be processed in accordance with the amount of transaction fees paid. Besides, such a liability claim would potentially contribute to extending the scope of OFAC sanctions beyond the US jurisdiction, since even transactions executed by non-US persons (who are not, as such, subject to the sanctions) would likely be ignored by miners or validators that are US persons, for fear of potential liability. Glimmers of this world can already be seen, as key players in the blockchain space—large cryptocurrency exchanges and service providers, such as Coinbase or Circle—have proceeded to blacklist the addresses of Tornado Cash smart contracts from their own databases in order to prevent users from transacting with the sanctioned addresses, while smaller cryptocurrency exchanges such as dXdY went as far as suspending the accounts of users who had previously interacted with some of these addresses. This new form of *infrastructural imperialism* marks the rise of a new code-based regulation that extends beyond the rules of the blockchain protocol, and implements the restrictions of centralized platforms operating on top of that protocol.

We might, therefore, find ourselves at the top of a slippery slope. The sanctions against Tornado Cash could become a precedent with a significant chilling effect on many other Web3 protocols and applications, especially the ones oriented towards the protection of financial privacy and the creation of private digital spaces for online interactions and communications. If the use of a technological tool becomes prohibited only because the same tool is also being used by a North Korean group of hackers, then North Korean hackers will effectively have the power to outlaw a large majority of our privacy-enhancing technologies, including PGP, Tor, and even cryptography altogether through their mere use of these technologies. And if the developers of these tools can be held accountable for the malicious use of their tools by criminals—as happened with Tornado Cash developer Alexey Pertsev who was arrested shortly after the OFAC sanctioned Tornado Cash—then criminals have the power to dissuade open source developers from ever releasing their code to the public.

As with earlier efforts to promote network neutrality on the Internet, it has become crucial today—perhaps more than ever before—to promote the principle of blockchain neutrality, in order to ensure the flourishing of an open, permissionless and uncensored Web3 ecosystem. Indeed, if network neutrality is necessary to guarantee that all content publishers operate on a level-playing field, and that all voices on the Internet have the same chances of being heard, blockchain neutrality is a precondition to ensure healthy competition in the Web3 ecosystem—which is already compromised by the growing popularization of Maximum Extractable Value (MEV) practices—as well as the preservation of unobstructed innovation in the space without fear of potential legal liability. As such, the principles of blockchain neutrality should be enforced, first and foremost, against private actors— i.e. miners or validators—who might be tempted to engage into new forms of economic discrimination—discriminating among transactions not only according to the transaction fees (as prescribed by the blockchain protocol) but also on the basis of factors external to the blockchain (e.g. as a result of off-chain agreements with specific transaction issuers or recipients). But the same principles should also be enforced against governmental authorities (like OFAC or other regulatory authorities) to prevent them from enacting rules that would force ‘mere conduits’ to discriminate between the transactions submitted to a blockchain network in order to escape from legal liability. Only then will we be able to witness a Cambrian explosion of new Web3 applications, whose success will depend—only and exclusively—on their capacity to provide a valuable service to the ecosystem, rather than the extent to which they serve the commercial and/or political interests of a small constituent group.

(old version — ignore)

The Alegality of Tornado Cash
or
The Tornado Cash Sanction: The End of 'Code is Law'?

On 8 August 2022, the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, a collection of open source smart contracts on Ethereum and other blockchain protocols that enable cryptocurrency users to preserve the privacy of their transactions. A user can send cryptocurrency to the smart contract from one address—where it is pooled with deposits from other users—and then withdraw it to another address. In doing so, the public link between the deposit and withdrawal addresses is decoupled, without the user ever losing control over their cryptocurrency. This mixing or tumbling service is used for both legitimate privacy-preserving purposes and illegitimate purposes, with the sanction notice explicitly mentioning the use of Tornado Cash by a collective of North Korean hackers, known as the Lazarus Group, for laundering proceeds from their hacks of US-based crypto-firms. The sanctioning of cryptocurrency mixers has happened in the past, but this time was different. Several organizations are presently arguing that, unlike previous instances, no entity, organization, or person can stop or modify the smart contracts—even if someone wanted to. This includes the team that developed the software and deployed the smart contracts, as well as the Tornado Cash DAO, since neither the developers nor the DAO participants can update or remove these smart contracts. This is by deliberate design, as the developer team wished to allow user governance over certain aspects of how the Tornado Cash protocol evolves, but also preserve the immutability of the smart contracts that pool and tumble the cryptocurrencies. As the Tornado Cash team explained on Medium on 20 May 2020, they did this so as to live "by the precepts that code is law".

In this essay, we wish to make two provocations building on the illustrative case of Tornado Cash. First, we show how the recent sanctioning of Tornado Cash is an archetypical example of what two of us have previously called *alegality by design*, whereby the technical features of blockchain technology have destabilized the boundaries of an existing legal order. We use the earlier 'cryptowars' of the 1990s as an example to illustrate how such alegal acts and artifacts have been addressed in the past. Second, we argue that though the *rule of code*, in which 'code is law,' offers a sense of equality and equal treatment, other principles of the *rule of law*, such as the possibility of seeking effective remedies are ignored. In doing so, we hope to expose some of the limitations of the principle, code is law.

—

Less than a decade ago, Ethereum co-founder Gavin Wood gave a presentation in London where he fervently argued that blockchain was fundamentally alegal. Alegality, Wood contended, was a feature of systems that “cannot care” whether its actions “are interpreted as legal or illegal.” Behind his reasoning, there was a simple idea: blockchains and the systems built around them should not be regarded as either a subject or an object of the law. [MM: Add a bit more on the theory of alegality and alegality by design] That Tornado Cash is alegal by design is evident from the fact that it destabilizes the *subjective boundaries* of the US sanction system, as it puts into question who or what can be sanctioned. This boundary can be regarded as a *fault line* in this instance as the legal system cannot address this alegal act (i.e., by placing a sanction) without compromising the ‘identity’ of the system. In this case, by placing a sanction, not only does OFAC extend the subject of such actions beyond those that have long been recognized by US law, they also create tension with a well-established principle that ‘code is speech’ and, due to the sanction’s broad approach and limited real effectiveness, potentially threaten the constitutional right to free speech as well.

Even after Github removed the codebase and the Tornado Cash website was done, one can still resort to other interfaces to transact through the smart contract.

[Are sanctions in these cases a legitimate course of action?]

History, as we can see, tends to repeat itself. Similar claims were made not long ago during the 1990s Crypto Wars, where the “right to privacy” was also defended under the First Amendment against the US government’s control over encryption exports and measures to prevent its mass adoption. Most recently, the arrest of the Tornado Cash developer in Amsterdam has fanned the fire in the same direction, leading protestors to voice that “#opensource is not a crime. #privacy is a human right”.

There is also the argument that Tornado Cash is a technology *not* specifically designed with the intent to aid and abet criminals and that sanctioning open-source code is, in fact, sanctioning free speech.

[Should the Rule of Code *always reign* over the Rule of Law? What happens when the activity is not only illegal but also immoral?]

[To be continued (...)]

While the matter of the case is to be defined within the US legal framework, there is, however, precedent in 11th-century English common law to make inanimate objects that caused a person’s death—“deodants”—objects of law and request for these to be forfeited.