# COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION REGARDING DIGITAL ASSETS RESEARCH AND DEVELOPMENT

**88 Fed. Reg. 5043**

Submitted on March 3, 2023 to the
White House Office of Science and Technology Policy

The Electronic Frontier Foundation (EFF) submits the following comments in response to the White House Office of Science and Technology Policy (OSTP) request for information regarding digital assets research and development.

EFF is a non-profit organization that has worked for over 30 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With more than 30,000 contributing members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

EFF is encouraged to see the White House taking interest in the future of digital assets. These technologies have the potential, if used properly, to increase individuals' privacy while facilitating online commerce and research in this area could push forward the domain of advanced cryptography in ways that could radically change the landscape of online services that we all use every day. The White House and OSTP have the opportunity to guide this future today.

## I. Coders' Rights

Fulfilling OSTP's goal of encouraging this important research requires at the very least ensuring that researchers and software developers do not face legal jeopardy for legitimate research. The Treasury Department's Office of Foreign Assets Control (OFAC) in August of 2022 placed the Tornado Cash smart contract on their sanctions list, sending shock waves through the digital assets community. OFAC's actions, taken without consultation with the community or input regarding questions such as what jurisdiction they have, what entities may be sanctioned, and what liability can attach

to people who write code that ends up in a sanctioned smart contract, was extremely concerning.

Courts have consistently held that computer code is protected speech under the First Amendment. In particular, legal regimes that target the publication of speech and knowledge (in the form of code or other information), bear a heavy burden to establish that they are consistent with the First Amendment. A regulation that punishes researchers and software developers who are not responsible for harmful or illegal activity is very likely to fall afoul of these constitutional protections.

In addition, targeting developers in this way is a strategy guaranteed to discourage people from developing the very technologies and services in which OSTP is seeking to boost research and development. The chilling effect of seeing other digital assets developers placed on sanctions lists and even put at risk of arrest can not be overstated.

The White House should make it clear that writing code by itself cannot give rise to liability, it is only the actions taken with code that can create legal liability.

## II. Non-Blockchain Ledgers

As OSTP suggests in the Request For Information, digital assets are not confined to blockchain-based solutions, and, in reality, blockchains may not end up being the ideal backing technology for keeping track of digital assets. Blockchains suffer from a number of issues that make them unsuitable to acting as the backing technology for a digital asset.

First, and most importantly, blockchains inherently place every transaction into a public ledger and require that ledger to be distributed to every other participant. Aside from the purely logistical problems that this poses, particularly as the size of the blockchain grows over time, this fact poses massive privacy problems. While transactions are usually pseudonymous on blockchain ledgers, eventually money needs to be used if it is to be valuable and that use enables tracing of coins to individuals with a modicum of investigation. There are blockchain systems that use anonymity technologies to blur the participants in the exchange, there are also countermeasures.

Secondly, the proof-of-work method of securing a blockchain against double spending, which Bitcoin uses and Ethereum used until very recently, uses electricity far in excess of what is reasonable for a transfer of value system and exacerbates an already-dire climate change situation. The proof-of-stake system that Ethereum now

uses is a great improvement in terms of electricity use, but is still young and needs further research into its long term stability and its actual efficiency benefits. The White House should encourage research into newer exchange systems with lower energy costs, especially ones that take less energy than the traditional payment systems such as cheques or credit/debit cards.

Finally, as the cybersecurity research organization Trail of Bits showed in a report from June of 2022 entitled "Are Blockchains Decentralized," blockchains tend not to live up to their largest claimed benefit: that of decentralization. According to Trail of Bits, at the time of publication of the report even just a handful of entities held enough control to disrupt the Bitcoin and Ethereum blockchains.

The White House should avoid assuming that blockchain is inevitably the solution for digital assets, and encourage research and development into other alternatives.

## III. Privacy

One of the largest points of contention that will inevitably arise surrounding any digital asset system is that of financial privacy. We have already witnessed the opening salvos of this fight in the actions taken by OFAC against Tornado Cash. The administration should lay out a firm expectation at the outset of any process leading to the creation of digital assets that the financial privacy of ordinary Americans is fundamental.

Financial data can reveal enormous amounts of information, including medical status, religious or political affiliation, and sexuality. Charitable donations can obviously reveal a lot about a person, but even everyday purchases, particularly when taken in aggregate, are capable of painting a detailed picture of a person's likes, dislikes, habits, and income. These pieces of information should not be the business of any private bank, credit card issuer, or government agency.

Financial privacy also enables and protects people's constitutional free speech rights to support unpopular political and social campaigns and organizations without fear of reprisal. In an era of extreme political polarization, the demonization of marginalized groups, and movements to intimidate people away from accessing healthcare such as abortions, it is essential to preserve this freedom. Similarly, the US dollar is used around the world in places where giving money to certain charities or religious institutions could be dangerous. Giving those people financial privacy through the use of digital assets could improve human rights under repressive regimes everywhere.

Finally, building in financial privacy has the welcome side effect of ensuring that an asset can be used to buy anything and everything that is not illegal. For many years the major payment processors have acted as morality police, unilaterally deciding what they would and would not allow their systems to be used to purchase. Pre-internet this was perhaps more of an annoyance, as cash could always be used as a fall back. Since commerce has moved online, however, and credit and debit cards have become essential to transactions, these unelected intermediaries have become the unreviewable arbiters of what can and cannot be sold. Any digital asset contemplated by the White House should expand the options that purchasers have. Private transaction processors should not be empowered to force their restrictive preferences on the populace.

If the White House decides to undermine this privacy for the purpose of combating money laundering, the focus should be on large denomination transfers of value. Routine transactions of small denominations, as nearly all people make on a daily basis, should remain private under all circumstances. Some proposals, such as Senator Lynch's ECASH bill, directly address these issues. By calling for non-blockchain, direct-cash payments of under $10,000, it looks directly at the real issues that need proposals, test deployments, and infrastructure.

## IV. Conclusion

EFF is encouraged by the White House's interest in digital assets, and we hope the administration will pay particular attention to making sure that any system created ensures privacy for everyday Americans and that researchers and developers working to advance the state of the art in digital assets are not burdened by legal liabilities for their work.