International Journal of
Strategic Research in Education, Technology and Humanities
p-ISSN: 2465-731X | e-ISSN: 2467-818X
IJSRETH
November, 2022
Vol. 10, No. 2

The Competing Priorities Facing Us Crypto Regulation

Josephine Wolff
The Fletcher School,
Tufts University, United States

Article DOI:
10.48028/iiprds/ijsreth.v10.i2.06

Abstract

As the Biden administration has worked in recent months to develop cryptocurrency regulations, the U.S. government finds itself caught between two extremes: unwilling to actively block cryptocurrency transactions for fear of restricting a growing and potentially lucrative industry but also determined not to give up completely on policing illegal cryptocurrency payments and going after their role in the cybercrime ecosystem. In a recent executive order and subsequent strategy documents, President Biden has pledged to both support development of cryptocurrencies and to restrict their illegal uses, two goals that the United States has long struggled to reconcile when it comes to digital money. And the Biden administration made clear in their executive order just how much the U.S. government wants to have it both ways, touting the potential benefits of virtual currencies for "responsible financial innovation" as well as the risks they pose to consumers, investors, and the "financial stability and financial system integrity." This paper seeks to examine the competing priorities facing US crypto regulation including all digital assets not just cryptocurrencies including other property that exists only in a digital form, such as non-fungible tokens. But of all forms of digital assets, cryptocurrencies are the kind that present the biggest security risks, as well as the greatest potential economic benefits.

Keywords:
Competing priorities, Facing US, Crypto regulation

Corresponding Author:
Josephine Wolff

First Published: https://www.brookings.edu/techstream/the-competing-priorities-facing-u-s-crypto-regulations-bitcoin-ethereum/

Background to the Study

In the past year, the balance struck by the U.S. government between encouraging entrepreneurial cryptocurrency ventures and discouraging criminal activities leveraging cryptocurrencies seems to have shifted somewhat, due both to the volatility of the virtual currencies themselves as well as the growing concerns about the types of crimes enabled by those currencies. In particular, the United States seems increasingly interested in developing domestic cryptocurrency policies that can have a global impact on overseas criminal enterprises, including sanctioning cryptocurrency exchanges and individual cryptocurrency wallets, as well as recovering cryptocurrency payments made to criminals. While these are restrictions on the behavior of U.S. individuals and companies, they are ultimately aimed at overseas criminal operations and making it more difficult for those foreign actors to profit from international cybercrime. It is too soon to say whether these recent measures will be effective or enforceable or whether they can be scaled up to address the full extent of the challenges posed by cryptocurrencies. But it is clear that they mark a significant step forward in the history of U.S. cryptocurrency regulation in terms of how aggressive the government is willing to be about going after criminal virtual currency enterprises and also how willing it is to enter the virtual currency space itself with a potential central bank digital currency (CBDC).

Sanctions, Arrests and Ransom Reclamations

Few countries have excelled at writing and enforcing clear regulations governing digital currencies, but even by the standards of a profoundly ambiguous and poorly enforced area of regulation, the United States has struggled when it comes to defining not just what policies to promote but also what the goals of those policies should be. China, for instance, has taken a strong stance against cryptocurrencies by banning all transactions of virtual currencies in hopes of cracking down on cybercrime and fraud, and it has simultaneously begun rolling out a state-backed blockchain services network. El Salvador's government, by contrast, has made Bitcoin a form of legal tender, requiring that all businesses accept the cryptocurrency as payment and creating a $150 million trust to facilitate conversions between Bitcoin and dollars. The United States has largely split the difference by extending many existing financial regulations to the cryptocurrency market in the United States. Know Your Customer laws and anti-money laundering policies and procedures have been applied to U.S. cryptocurrency exchanges for years, but these measures have done little to prevent people from simply using exchanges in other countries for their illicit transactions. In response, the U.S. government has stepped up its efforts to combat cybercrime in court and to seize virtual currencies allegedly obtained as part of criminal schemes. Perhaps the highest profile success story of this effort was the seizure last year of 63.7 bitcoins, or roughly $2.3 million, of the $4.4 million ransom paid by Colonial Pipeline to hackers that penetrated the company's system and crippled the supply of fuel to the Eastern Seaboard. The Justice Department's announcement of the seizure was light on details how exactly the FBI had obtained the private key for one of the bitcoin wallets the criminals had been using, for instance but heavy on official rhetoric about how this seizure signalled the end of an era when criminals could use virtual currencies with impunity. “There is no place beyond the reach of the FBI to conceal illicit funds,” FBI Deputy Director Paul Abbate was quoted as saying.

The implication was that this was not a one-off success but instead the beginning of a period of much more serious policing of cryptocurrency transactions that would result in similar such seizures in the future. Less than a year later, in February 2022, the Justice Department arrested the married couple Ilya Lichtenstein and Heather Morgan in New York for laundering roughly $4.5 billion in cryptocurrency stolen from the exchange Bitfinex in 2016 and seized more than $3.6 billion in stolen cryptocurrency. That's an unusually large sum for law enforcement to seize in ill-gotten cryptocurrency gains by comparison, the recovered portion of the Colonial Pipeline ransom amounted to only $2.3 million and several other recovered ransoms and cryptocurrency sums have been much smaller, around $500,000. By comparison, the recent breach of exchange Binance resulted in losses of $570 million. While it's hard to say exactly what portion of stolen or extorted cryptocurrency payments have been recovered since very little is known about the overall costs of these cybercrimes, the recovered sums probably remain a relatively small but growing fraction of the overall pool of criminal cryptocurrency funds. At the same time, the retrieval of the Bitfinex funds suggests that law enforcement may be successfully targeting some of the most important or large-scale criminals with their investigations.

The most promising signs of progress for cryptocurrency regulation lie not in law enforcement efforts to catch cybercriminals and take back their illicit profits, but instead in efforts by the Treasury Department to make it harder for them to receive those profits in the first place. On September 21, 2021, the Treasury Department announced its first ever sanctions against a virtual currency exchange and blocked transactions with the Russia-based Suex exchange. According to the Treasury Department, more than 40% of transactions on Suex were associated with criminal activity, and by cutting off the exchange from the U.S. financial system, the department aimed to make it more difficult for online criminals to process transactions. Of course, circumventing these restrictions is simple just shift to a non-sanctioned exchange so the only way for this strategy to work was for the U.S. government to continually monitor which exchanges criminals were relying on and update their blocklist. So, it was a promising sign when on November 8, 2021, less than two months after the Suex sanctions, the Treasury Department followed up with more sanctions, this time aimed at the virtual currency exchange Chatex, another Russian exchange linked to Suex, as well as three of Chatex's suppliers. Then, in April 2022, the Treasury Department added a third exchange operating in Russia, Garantex, to the list, after determining that more than $100 million in transactions processed by Garantex were associated with illicit actors and illegal online markets. In May 2022, Treasury went a step further and sanctioned virtual currency mixer Blender.io that helped actors including North Korea obfuscate their illegal cryptocurrency activity by mixing together funds from different virtual currency transactions before transmitting those funds to their ultimate recipients, making the transactions more difficult to track.

It remains to be seen whether the United States can keep that list of sanctioned cryptocurrency intermediaries up-to-date and comprehensive enough to put a real dent in overseas cybercrime profits, but for the first time, they are pursuing a strategy that might actually have a chance at succeeding. Success would mean that criminals have to

expend real time and effort to identify and move to new intermediary organizations, including exchanges and mixers, in order to receive payments and ransoms from U.S. victims. So, if the rate of ransomware attacks slowed, or shifted to non-U.S. targets, or victims were routinely being asked to make payments via sanctioned entities, that would suggest that this approach might be effectively preventing criminals from receiving payments or finding organizations that would help them process such payments.

The Push for U.S. Central Bank Digital Currency

These more aggressive sanctions and policing efforts directed at cryptocurrencies in the past year have occurred alongside a call for the United States to develop a central bank digital currency (CBDC). In the March 2022 executive order, President Biden called this out as a priority on par with cracking down on cryptocurrency-enabled cybercrimes, writing, "My Administration places the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC." But the executive order also acknowledged that development of a U.S. CBDC was still at a relatively early stage and encouraged the Federal Reserve "to continue its ongoing CBDC research, experimentation, and evaluation" rather than committing to a specific timeline or implementation. Unlike cryptocurrencies, CBDCs are intended to be centralized, issued, and, in some cases, directly managed by central banks rather than public, decentralized blockchains. Given the backing of a central bank, CBDCs might compete more directly with stablecoins than other cryptocurrencies like Bitcoin that are not pegged to a reference asset. Ideally, CBDCs would offer some of the benefits of cryptocurrencies fast transactions, innovation, financial inclusion while also, like stablecoins, offsetting some of the risks, such as volatility, criminal activity, and energy-intensive mining. The effort to develop CBDCs is driven in part by a desire on the part of national governments to supplant cryptocurrencies with a form of virtual currency that will be designed to conform to existing financial systems and regulations. But it is difficult to imagine many of the users of cryptocurrencies who were drawn to the decentralized blockchain design of Bitcoin or Ethereum wanting to use something like a CBDC. And so much depends on the specifics of those designs exactly how centralized these currencies will be, how anonymous, how traceable, how susceptible to fraud that it is difficult to determine at this early stage who, if anyone, will want to use such state-backed virtual currencies and what benefits, if any, they will provide over and beyond existing forms of currency. Thus far, China is the country that has been most aggressively committed to the development of a CBDC, perhaps in part due to its determination to stamp out any private sector competitors in the cryptocurrency space.

If the policing efforts and exchange sanctions represent the United States' attempts to go after the downsides of cryptocurrencies through more aggressive policy measures, the push for CBDC pilot projects seems geared towards trying to preserve some of the potential benefits that virtual currencies were supposed to provide. Many of those benefits, particularly financial inclusion and easier access to currency for unbanked people, have proved largely elusive. The people who seem to have gained the most from cryptocurrencies were not unbanked but rather entrepreneurs with easy access to capital

and the ability to treat cryptocurrencies as investments rather than use them as a means of covering needed expenses. In that regard, developing CBDCs may be not so much a means of replacing cryptocurrencies as an attempt to make good on some of their as-yet-unrealized promise for a larger group of people.

There are also significant concerns around privacy and security linked to CBDCs. For instance, central banks might decide to implement CBDCs in such a way that they have insight into individuals' spending decisions and payment history. This is a particular fear that authoritarian governments that might view CBDCs as an opportunity to conduct surveillance on their population, though many central banks, including the U.S. Federal Reserve, have committed to intermediated CBDC models that would protect users' privacy through a combination of strong encryption and intermediaries who would shield data from being accessed directly by the government. But the exact mechanisms by which that data would be protected as well as who would have access to it under what circumstances remain hazy since many countries have not yet decided on the implementation of their CBDCs.

U.S. central bankers appear to be aware of these concerns. "While the level of personally identifiable information (PII) collected from users will vary widely depending on the implementation, a general-purpose CBDC would likely involve the collection and storage of sensitive PII and information about users' financial transactions. Given the sensitivity of this information, central banks and other institutions involved in the implementation of a CBDC would need to ensure this information is securely held to prevent harm to consumers from fraud and theft arising out of stolen PII as well as unauthorized disclosure of information," the Federal Reserve observed in a February blog post. But as that statement implies, U.S. bankers are no closer to figuring how, exactly, to mitigate those risks or what it would mean to hold such information "securely." The rise of cryptocurrencies has demonstrated just how difficult it is both to enforce existing financial regulations in the context of new currencies and to predict how those new currencies will be used, and by whom. That's not a reason to forswear all new forms of currency but it is a reason to approach them cautiously and with an eye to the opportunities for abuse and illicit activity. It's also a reason to be less confident about what types of benefits a CBDC will realistically be able to offer, especially since many of those could potentially be addressed through other, less radical changes to existing financial institutions and instruments.

A Way Forward for Cryptocurrency Regulation

It has taken years for regulators to acknowledge and address the fact that requiring U.S. based cryptocurrency exchanges to adhere to certain requirements about gathering information about their customers and preventing money laundering has had minimal effects on the largely international cybercrime industry. Even after a decade of efforts aimed at figuring out how to regulate cryptocurrencies effectively, the United States and other countries continue to struggle to enforce their own regulations due to the inconsistency of international regulations and the ease with which criminals can create

new cryptocurrency wallets and accounts when theirs are targeted by law enforcement. There are clearly positive developments in the past few years that indicate the U.S. government is making strides in using the full range of regulatory mechanisms at its disposal to target not just criminals but the underlying cryptocurrency infrastructure supporting them, including exchanges and mixers. This approach to targeting malign cryptocurrency intermediaries may prove effective, but much will depend on how rapidly these lists of intermediaries known to be associated with criminals can be updated and how difficult it proves for criminals to find alternative companies to work with.

Conclusion

Ideally, cryptocurrency regulation would progress in two phases moving forward. The first phase would emphasize the importance of controlling the flow of cryptocurrencies to criminals by maintaining up-to-date lists of sanctioned intermediaries and providing U.S. individuals and companies with easy and clear instructions for how to figure out whether they were doing business with any such foreign companies. At the same time, a large-scale analysis of whether these efforts were actually reducing illicit financial flows to criminal enterprises would be needed to understand the overall impact of these measures. By focusing government resources on policing cryptocurrency intermediaries and measuring the impacts of those policing efforts, regulators could get a better grasp on whether or not there is a viable path forward for lawful use of cryptocurrencies as a tool for financial inclusion. The measurement components of this first phase of policymaking will inform the second phase. If these measurement efforts indicate that law enforcement has been successful in choking off illegal cryptocurrency flows, then that will be a strong signal to the government to move forward with plans for a CBDC because the illegal uses of virtual currencies can be effectively controlled. However, if the first phase's measurement efforts suggest, instead, that little or no progress has been made toward stemming criminal uses of virtual currencies, that will be an indicator of how risky introducing new forms of those currencies could be. In that case, the U.S. government would be wise to focus on new avenues for enforcement before taking steps toward implementing a CBDC ahead of any understanding of how best to control theft, fraud, and extortion. Even as new efforts to target overseas exchanges and other powerful intermediaries with sanctions begin to gain some momentum, regulators would be wise to be cautious about introducing new currencies too rapidly before they have a handle on cryptocurrencies. The United States has long been focused on both promoting the positives of virtual currencies and combating their illicit uses, but at least for the time being, it might make sense to focus on the latter goal before opening up new opportunities for cybercriminals in the form of yet another kind of currency.

Reference

https://www.brookings.edu/techstream/the-competing-priorities-facing-u-s-crypto-regulations-bitcoin-ethereum/