

RESEARCH

# Stablecoins and national security: Learning the lessons of Eurodollars



Shutterstock / metamorworks

**Timothy G. Massad**  
April 17, 2024

33 min read

Sections







Read more from

Series on Financial Markets and Regulation

As Congress struggles to resolve big issues like funding for Ukraine and Israel, the debate over legislation to regulate stablecoins seems like small potatoes. But there is a connection, which is that stablecoins could have national security implications: Unless we strengthen their regulation, they could undermine our ability to use sanctions to advance our national interests. This was illustrated recently by [news](#) that Russian smugglers have used Tether, the largest stablecoin, to avoid Western sanctions and purchase billions of dollars worth of weapons.

Stablecoins are a type of cryptocurrency that is far more useful as a means of payment than Bitcoin.<sup>1</sup> That is because stablecoins are designed to maintain a constant price in terms of another asset.<sup>2</sup> Stablecoins pegged to the U.S. dollar are more “money-like” than other cryptocurrencies. They can be used to move value across borders without going through banks, and it is the banking system—and in particular the role of U.S. banks—that is key to the implementation and efficacy of

and Eurodollars are U.S. dollar-based liabilities that had their origins outside the regulated banking system. U.S. policymakers initially paid little attention to Eurodollars because the market was small. But it quickly grew, and—luckily for policymakers—Eurodollars ultimately helped cement the international role of the dollar. It is the global dominance of the dollar, coupled with the role of U.S. banks in facilitating dollar payments, that gives the U.S. its tremendous financial leverage.

Could stablecoins undermine that leverage? As with the early days of the Eurodollar market, stablecoin use is minimal today, and so their national security risk may also be minimal. But just as Eurodollar use grew quickly and unexpectedly, stablecoins could also grow. While they are [used](#) principally to trade other crypto assets today, they could become a more widespread means of payment. They have also [become popular](#) as a means for people in countries with weak currencies to acquire a dollar substitute. Moreover, that growth could come even if the U.S. does not take action. That is because many other jurisdictions are creating frameworks to license stablecoins, including [Europe](#), the [U.K.](#), [Japan](#), [Singapore](#) and the [U.A.E](#). While those frameworks may lead to stablecoins in native currencies, they could also give rise to new dollar-based stablecoins.

This paper discusses how stablecoins could destabilize what Eurodollars helped to create—the global financial system plumbing that has been a means to implement sanctions<sup>3</sup>—and what to do about it. First, I provide a brief summary of the history of Eurodollars and their rapid growth. I discuss how Eurodollars strengthened the role of the U.S. dollar and U.S. banks. I then discuss the risks that stablecoins pose, in particular how they could be used to circumvent the existing financial system plumbing and sanctions. Finally, I suggest a path forward to promote responsible financial innovation while protecting our national security interests.

## A brief history of Eurodollars

Eurodollars are very similar to stablecoins. They are U.S. dollar-based liabilities issued by foreign banks outside the U.S. regulatory perimeter. Eurodollars began as a way to hold dollars out of the purview of U.S. authorities. As early as the late-1940s, the U.S.S.R., China, and their satellites [occasionally needed U.S. dollars](#) for what little trade they conducted with the West and each other. But they worried their dollar balances in New York could be seized. Most ended up in Paris at the Banque [Section](#) [ciale pour l'Europe du Nord \(BCEN\)](#) whose owner was [well-known](#) in Moscow. It is, in fact, after that bank's telex address (BCEN-Eurobank) that

The market grew quickly, as banks soon found ways to earn arbitrage profits by issuing Eurodollars and attracted deposits by paying higher interest rates than U.S. law allowed.<sup>4</sup> Initially, policymakers in the U.S. and elsewhere were wary of the Eurodollar market. The ability of foreign banks to accept U.S. dollar deposits as a funding source was essentially unlicensed money creation—arguably a violation of monetary sovereignty. But they did not make a significant attempt to regulate it because, among other things, it was too small to be worth the effort. By 1960, Eurodollars were a [\\$1 billion market ↗](#)—spectacular growth by any measure but still a tiny fraction of [U.S. bank deposits ↗](#).

The market continued to grow over the next few decades, in part due to unforeseen events and in part due to fluctuations in official attitudes—from concern to outright support at times. In the 1960s, the Kennedy administration decided to encourage the market rather than curb it to help stabilize the dollar and address balance of payment concerns.<sup>5</sup>

By 1970, Eurodollars were a [\\$50 billion ↗](#) market, or a fifty-fold increase in a decade. Policymakers soon grew wary that “hot money” in the Eurodollar market could lead to the dollar’s collapse. Eurodollars had become the “[villain ↗](#)” of an approaching crisis, or, as French Finance Minister Valéry Giscard d’Estaing put it, a “[hydra-headed monster ↗](#).”

These worries were set aside after the oil shock of 1973. In retaliation for U.S. support for Israel in the Yom Kippur War, most major oil producing states suspended exports. Shortages forced panicked buying and prices skyrocketed. The value of global oil trade quadrupled in only a few months, which stressed the international financial system to the breaking point. Henry Kissinger, who was secretary of state at the time, thought it was the [most significant threat to global security ↗](#) since World War II.

William E. Simon, Nixon’s treasury secretary, and others [argued ↗](#) that private markets and in particular Eurodollars could facilitate ‘petrodollar recycling’—that is, critical intermediation between the buyers and sellers of oil, both of whom were primarily using U.S. dollars.<sup>6</sup> The market struggled under the weight of those flows until European central banks pledged to act as a collective “lender of last resort” to the Eurodollar market.<sup>7</sup>

some respects the reverse: to make sure that money support is not cut by large amounts by accident.”<sup>8</sup> Regulators had, in a sense, missed their moment. The Eurodollar market grew nearly ten-fold over the next decade and continued its exponential expansion until the mid-2000s; by that point there were significantly more Eurodollars than deposits in U.S. banks.<sup>9</sup> That expansion was, of course, in large part driven by events outside of Europe, but the term “Eurodollars” continues to be used for all dollar deposits held outside of the U.S.

## Eurodollars and national security

Luckily for U.S. officials, even if not by conscious design, the growth and maturation of the Eurodollar market has enhanced the ability of the U.S. to project power by non-kinetic means. The expansion of the global dollar system and preeminence of the dollar<sup>10</sup> also strengthened the role of U.S. banks in international payments. Although Eurodollar deposits can be used to affect dollar-based payments between two foreign counterparties, those payments must transit the global correspondent banking network. Owing to a variety of practical and economic necessities, these payment chains almost always transit through U.S. banks.<sup>11</sup> That remains just as true today as in the 1970s. The same can be said of foreign exchange transactions themselves—even when trading Yen for Euros, for example, traders often execute the transaction through two legs with dollars as the common base.<sup>12</sup>

That global dollar system has created leverage for U.S. national security objectives. Rogue actors and nations can be blocked from doing business with the U.S and excluded from the entire global dollar system. The potency of that leverage was recognized as early as the late-1970s with sanctions against Iran.<sup>13</sup>

After 9/11, this power was enhanced: The U.S. used its influence over the Society for Worldwide Interbank Financial Telecommunications (SWIFT, a near-universal cross-border messaging protocol) to obtain transactional data with which to improve the accuracy and efficacy of sanctions. The potency of this “economic weapon” has been even stronger when the U.S. has succeeded in building support for sanctions among a broad network of allies. That was evident when sanctions were deployed against North Korea and Iran in the early 2000s<sup>14</sup> and of course Russia in 2014 and 2022.



with our allies, we should ensure that the architecture of financial networks continues to reinforce their efficacy.

## The national security risks of stablecoins

Recent events highlight the potential risk that stablecoins pose to our national security interests:

In February 2022, the U.S. and its allies imposed a raft of sanctions against Russia in response to its invasion of Ukraine. As soon as those sanctions were announced, however, [many](#) [speculated](#) that they could be avoided via cryptocurrency markets. Offshore crypto exchanges [added to the risk](#) by providing a potential off-ramp to convert crypto holdings into dollars or other sovereign currencies. Some worried that crypto assets could eventually facilitate an alternative international payments system for [unfriendly countries](#) and [rogue actors](#).<sup>16</sup>

That didn't happen, at least not at first. In early March, only a couple of weeks after the invasion began, Deputy National Security Advisor and chief architect of the [sanctions regime](#) Daleep Singh [told CNN](#) that "crypto's not really a workaround for our sanctions." It seemed the crypto markets [lacked](#) the depth and size to allow for sanctions evasion at scale.

However, a recent [Wall Street Journal story](#) claimed Russian smugglers were using Tether to purchase weapon parts on a regular basis, with some estimating this "shadow trade" was \$10 billion a month.

In addition, the October 7, 2023, attacks by Hamas on Israel highlighted the risk of [rogue actors using crypto](#) for terrorist financing. Early reporting pointed not just to crypto but to the stablecoin Tether as a [primary means](#) for Hamas to [evade](#) law enforcement and sanctions. Subsequent reports concluded the flow of tokenized funds to Hamas was [too small](#) to truly matter, but there is no assurance they won't be more widely used in the future.

Could crypto eventually provide a "workaround" to sanctions enforcement and prohibitions on terrorist financing? The fundraising techniques of those seeking to

Stablecoins are certainly not the only threat to sanctions enforcement. Many countries are engaged in projects that have the potential to circumvent U.S. sanctions. This includes the creation of shared payment platforms among multiple countries which would link existing payment systems or proposed central bank digital currencies (CBDCs).<sup>17</sup> But stablecoins arguably have greater potential to become a widely accepted medium of exchange for international payments in the near term. That is because stablecoin networks already exist, most central banks are only in a [research and development phase](#) with CBDCs, and multi-country shared platforms face technological hurdles as well as complex governance questions.

In addition, stablecoins offer something those other alternatives do not, which is a means to make *dollar-denominated* payments that are not entirely dependent on the U.S. banking system. That is why they could represent a way around the financial plumbing on which sanctions depend.

## The road ahead for stablecoins

I have [argued](#) that we are better off [bringing stablecoins within the regulatory framework](#) in order to minimize the risks they pose as well as capitalize on any potential they may have to improve the efficiency of payments. But while the [Treasury](#) and the [White House](#) have called for new legislation, there remains a wide division of opinion in Congress on whether and how to regulate stablecoins. Those who believe in the innovative potential of stablecoins want to create a regulatory framework to provide clarity and encourage their development. The Republican-led House Financial Services Committee passed [legislation](#) last summer that would create federal licensing and allow state chartering of stablecoin issuers. But the bill received only a handful of [votes from](#) committee Democrats and it is unclear whether it will move forward in the Senate Banking Committee even if the full House approves it.

Many who are skeptical of the potential of crypto generally and stablecoins in particular are reluctant to create a framework that might legitimize them and encourage further growth. Indeed, some believe we are better off not taking any regulatory action—an approach most evocatively characterized as “[let crypto burn](#).” It appears motivated in large part by the crash in crypto prices and failures of big firms like FTX in 2022. But the recent recovery in prices, coupled with events

Policymakers have focused on financial stability and consumer protection risks posed by cryptocurrencies, particularly stablecoins. As Treasury Secretary Janet Yellen [put it](#) [in April 2022](#), “Our regulatory frameworks [for digital assets] should be designed to support responsible innovation while managing risks—especially those that could disrupt the financial system and economy.” That has meant a focus on how to ensure that reserves are conservatively managed and invested so that holders can always redeem tokens and the risks of a run are minimized. But those are arguably the easier regulatory challenges. We can impose requirements on the *issuer* of stablecoins that are designed to achieve those objectives, such as restrictions on how to invest reserves, capital and liquidity requirements, reporting and disclosure standards, and structuring requirements to ensure that holders’ claims take priority over issuer debt or other claims.

The harder issues are [raised](#) [by the fact](#) that stablecoins are transferred on decentralized blockchains for which there is no central operator, no entity responsible for end-to-end risk management. Once issued, stablecoins are bearer instruments that can be transferred without any entity maintaining accounts of, or screening, the transferor or transferee. That is one of the most important innovations of crypto compared to traditional payment network architectures, but it also creates the risk that transfers could facilitate illicit activity and evade sanctions. Although stablecoin issuers can be required to meet the same know-your-customer (KYC), anti-money laundering (AML), and combating the financing of terrorism (CFT) requirements that banks and other financial institutions must meet, those requirements work best to police transactions when the issuer is issuing or redeeming stablecoins.

To date, there has been a global effort to combat money laundering and terrorist financing in crypto by imposing requirements on institutions, such as crypto trading platforms, that facilitate conversions between crypto and fiat currency. The multilateral Financial Action Task Force (FATF) issued [guidelines](#) [recommending](#) that all “virtual asset service providers” (VASPs) be licensed by national authorities and required to follow those guidelines. The FATF also promulgated the “Travel Rule” which requires VASPs to obtain and share information about addresses to which they are transferring crypto. That rule is designed to minimize the chance that a transfer is made from a licensed platform to an unhosted wallet beneficially owned by a criminal or suspicious person. Stablecoin issuers are fond of pointing out that most stablecoins are held either at licensed VASPs or at wallets a mere “one hop” away.



capital or infrastructure, thus increasing the risk that new ones can be established easily in noncompliant jurisdictions. In addition, “mixers” can be used when transferring crypto assets so as to hide on-chain identity, as explained in a recent proposed [regulation](#) to address the illicit activity risks related to their use.<sup>18</sup>

[Stuart Levey](#) has seen these issues from all sides, having served as the first undersecretary of the treasury for terrorism and financial intelligence (where he led the development of sanctions programs and other financial tools to combat threats to U.S. national security), chief legal officer of HSBC, and chief executive officer of the Libra/Diem Association (initiated by Facebook to create a blockchain-based payment system and stablecoin). His determination of whether these measures are sufficient is a clear “no.” He believes the regulatory framework should set a high bar by effectively requiring that all transactions involving a stablecoin—whether directly with the stablecoin issuer or some other centralized entity, or otherwise when transferred on permissionless blockchains—satisfy U.S. standards for anti-money laundering, anti-terrorism financing and sanctions enforcement. Like rogue nations blocked from accessing the global dollar system, stablecoin issuers should be blocked from accessing the U.S. financial system (either directly or indirectly) unless they can meet that prerequisite.<sup>19</sup> That would allow U.S. regulators to extend those requirements beyond their immediate territorial jurisdiction.<sup>20</sup>

The question is how to achieve that higher standard while also respecting reasonable expectations of privacy. The legislation recently approved by the House Financial Services Committee does not address the issue. Prohibiting transfers to unhosted wallets—which is what Libra/Diem eventually proposed—is one approach, but it might just push the market to noncompliant stablecoins.

At minimum, we should require stablecoin issuers to engage in enhanced monitoring of blockchains for suspicious transactions and consider when the issuer must “freeze” stablecoins—that is, prevent the holder from using them further. Japan’s [new framework](#) requires that the stablecoin issuer engage in such monitoring and have the capability to freeze or seize stablecoins, for example. When should law enforcement authorities have the ability to order such actions, and should issuers be expected to do so on the basis of their own due diligence? This requires striking a balance between having adequate tools to detect and prevent illicit activity on the one hand and preventing unreasonable searches and seizures and protecting privacy

miners, validators, and other network participants that may validate or facilitate crypto transactions. Many in the industry believe this is impractical and would [undermine](#) crypto markets. They question how a miner or validator can be held responsible for screening the identities of those involved in a transfer. But Congress has expanded the definition of persons with BSA responsibilities before: The [Anti-Money Laundering Act of 2020](#) included persons engaged in the antiquities business, for example.

By contrast, a recent [paper](#) proposes a more nuanced approach, in which we would distinguish between “genuine DeFi [decentralized finance] protocols,” or those which truly operate without the need for intermediaries, on the one hand, and systems that employ smart contracts but in which intermediaries still retain some authority, on the other hand. With the latter intermediaries, we might still assign BSA-type responsibilities, depending on their business model and activities, similar to the Warren-Marshall approach. With respect to genuine DeFi protocols, the paper proposes enhancing their security and resilience by classifying them as “critical infrastructure” subject to government oversight and requiring businesses that transmit communications involving such protocols to perform certain risk management practices, without being classified as financial institutions under the BSA. The risk management practices could include wallet screening or “scoring”—that is, assigning a “risk score” for illicit activity to particular digital wallets based on a due diligence

review—and identifying to authorities the high-risk wallets through the equivalent of suspicious activity reports (SARs).

Other technological solutions are often suggested, such as [whitelisting](#) blockchain addresses and incorporating [decentralized identity](#) mechanisms into stablecoin smart contracts so that transactions with unverified or sanctioned addresses cannot be consummated in the first place. But it is not clear whether such systems are ready for market today nor what the privacy implications would be.

Finally, there are those who question whether decentralized blockchains are acceptable at all, or whether we should only license stablecoins that are transferred on blockchains where access is controlled. In describing the United Kingdom’s current thinking on regulating stablecoins, Jon Cunliffe, the recently retired deputy governor of the Bank of England, [noted](#) that the U.K. will require that there be a “legal entity

In any event, U.S. authorities have more leverage than they might think. The stable value of stablecoins is built on confidence in their ultimate convertibility into fiat currency. This redemption process relies on access to the U.S. banking and financial system. While it is possible to launch a dollar-based stablecoin from a non-U.S. jurisdiction, query whether any stablecoin issuer can afford to be cut off from that access.<sup>22</sup> Even if access cannot be blocked entirely, imposing procedures that create friction in cashing out a stablecoin could cause a stablecoin's value to diverge from par, which might limit its appeal. We should therefore condition access to the U.S. banking and financial system on the stablecoin issuer complying with reasonable requirements to detect, deter, and prevent illicit activity.

International coordination will be critical in the development and implementation of any standards. So, too, will be timing their rollout: Pushing for stringent standards before they are technologically feasible could push illicit financial activity further into the shadows. But ignoring the market on the assumption that it is small and can be contained could be risky, especially with other jurisdictions moving to permit wider use of stablecoins.

As Singh told me recently, "Stablecoins and other unregulated digital assets could erode the potency of U.S. economic statecraft by reducing our ability to exclude a

rogue actor from the global dollar system. Now is the time to act to ensure sanctions remain an effective tool for future presidents."<sup>23</sup>

Regulatory challenges posed by stablecoins are not as novel as they might appear. History is a useful guide, as much for its analogies as for its contrasts. First, policymakers should expect the unexpected. Financial innovations can scale more rapidly than ever thought possible for reasons nobody could have anticipated. That is a strong caution against the "let it burn" mentality with respect to crypto. Second, we should take a broad view, incorporating national security as well as macroprudential concerns into regulating digital assets. Finally, regulators should not wait too long to act. The passage of time invites more opportunities for the unexpected to arise, for the crypto market to grow, and for illicit actors to become more sophisticated in their tools. That could make it harder to create the appropriate regulatory framework. The growth of Eurodollars happened to complement national interests; that may not happen with stablecoins.

## Timothy G. Massad



Nonresident Senior Fellow - Economic Studies, Center on Regulation and Markets

Acknowledgements and disclosures



Footnotes



### MORE ON



## Cryptocurrency

## Defense & Security

PROGRAM

Economic Studies

CENTER

Center on Regulation and Markets

### U.S. FOREIGN POLICY







## Don't relax, Europe — the US hard right isn't finished yet ↗

Constanze Stelzenmüller  
April 22, 2024

U.S. DEMOCRACY



## Ukraine urgently needs support to defend democracy

Jonathan Katz, Lily Conway, Norman Eisen, Robin J. Lewis, Andrii Borovyk, Josh Rudolph  
April 19, 2024

MIGRANTS, REFUGEES & INTERNALLY DISPLACED PERSONS



Sections





## Ukraine Index: Tracking developments in the Ukraine war

Michael E. O'Hanlon, Constanze Stelzenmüller, David Wessel, Alejandra Rocha, Sophie Roehse, Mallika Yadwad  
April 15, 2024

# B

## Get the latest from Brookings

Email Address



The Brookings Institution is a nonprofit organization based in Washington, D.C. Our mission is to conduct in-depth, nonpartisan research to improve policy and governance at local, national, and global levels.

Donate