FOREIGN AFFAIRS

November/December 2021

Volume 100 • Number 6

America's Crypto Conundrum

Protecting Security Without Crushing Innovation

Justin Muzinich

America's Crypto Conundrum

Protecting Security Without Crushing Innovation

Justin Muzinich

This is the year that digital currencies went mainstream. In the span of just three months last spring, China tested its first-ever digital currency in some of its largest cities, hackers breached a major U.S. oil pipeline and successfully demanded a ransom of more than $4 million in Bitcoin, cryptocurrencies surged to a record combined market capitalization of over $2 trillion, and Jerome Powell, the chair of the U.S. Federal Reserve, warned that cryptocurrencies are "highly volatile" and "may carry potential risks to . . . users and to the broader financial system."

What for years many in Washington had dismissed as a pet project of techies and West Coast libertarians suddenly became one of the most important, if least understood, policy issues on the agenda of the Biden administration. Digital currencies are driving tremendous innovation that has the potential to make whole economic sectors more efficient. But they also pose various national security and financial threats and could even diminish U.S. influence abroad.

One reason that digital currencies are so potentially transformative is that their software design often reflects a particular policy view—that government should have less control over money. Early adopters routinely imbued their use of digital currencies with political and philosophical meaning. And even if many people buying Bitcoin today are just looking to make a profit, the values embedded in the code still come with every purchase. Reduced government control of money

JUSTIN MUZINICH is a Distinguished Fellow at the Council on Foreign Relations. He previously served as Deputy Secretary of the U.S. Treasury.

has potential benefits, such as lowering the cost of payments. But it can also undermine the ability of authorities to respond to economic crises or fight cybercrime and financial crime, among other basic services that citizens across the political spectrum expect.

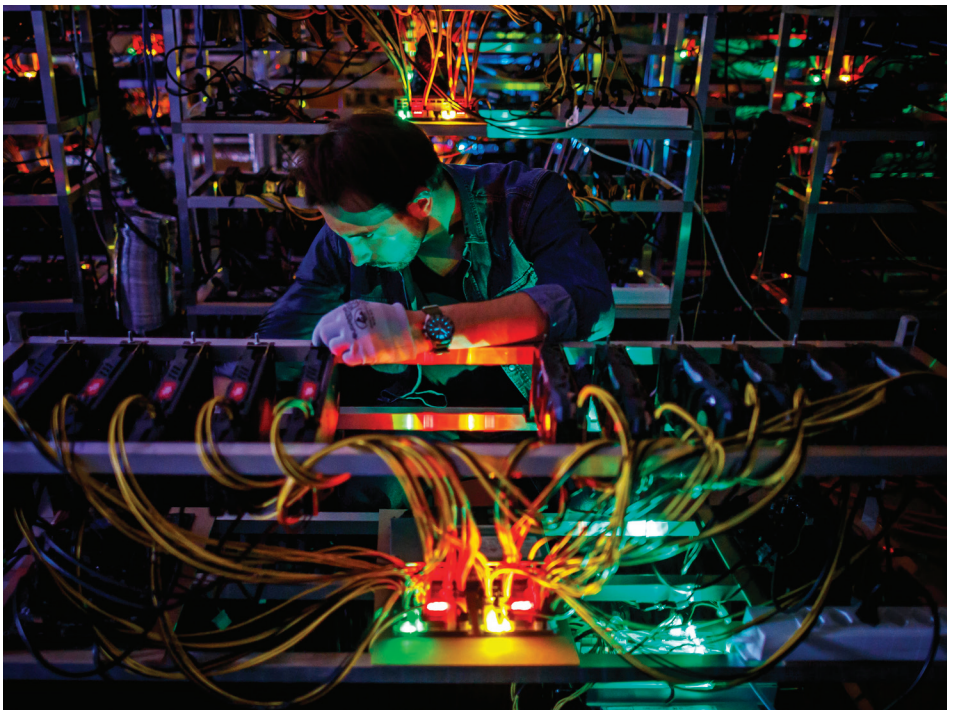
The enormous potential for upside as well as downside has driven the policy debate around digital currencies to extremes. On one side, opponents of digital currencies see them mainly as tools for illicit finance and have called on the government to curb their spread, in some cases going as far as advocating a ban on private-sector coins. On the other side are evangelists who see digital currencies as revolutionary and have pushed for the private market to determine their fate.

But what the United States needs is a public policy framework that takes a balanced approach, preserving the market's ability to innovate without sacrificing the government's capacity to perform essential functions. In other words, policymakers need both the humility to recognize that markets will be best at separating useful innovation from hype and the confidence to adopt critical safeguards. To that end, the Biden administration should establish guardrails in the areas where these currencies pose the greatest collateral risk—namely, in the government's ability to set monetary policy, ensure financial stability, and fight illicit finance. At the same time, the United States should lay the groundwork to launch a digital dollar or bless a private-sector solution that ensures the dollar's preeminent role in international payments. This two-track approach would chart a shrewd path between the fruitless extremes of banning digital currencies and allowing the market to operate unhindered.

U.S. policymakers should act swiftly. Beijing recently cracked down on the mining of Bitcoin, and China and other countries are forging ahead with sovereign digital currencies. Uncertainty about what the United States will do has added to the cloud of regulatory risk that hangs over the industry. The sooner the United States takes common-sense steps to provide policy clarity, the sooner innovation will be able to thrive.

CHEAPER, FASTER, RISKIER

Digital currencies come in public- and private-sector variants. Sovereign digital currencies, such as China's digital yuan, are government issued and give holders a direct claim on the central bank. Like transactions with normal currencies, transactions with sovereign digital currencies are validated by a central bank. In other words, these cur-



Tales from the crypto: at a cryptocurrency mine in Gondo, Switzerland, May 2018

VALENTIN FLAURAUD / KEYSTONE / REUTERS

rencies are just digital extensions of regular currencies—except they can make central banks look more like retail banks. Depending on their design, sovereign digital currencies can even enable ordinary depositors to have accounts directly with central banks and can potentially increase, rather than decrease, government control of money.

Private-sector digital currencies, by contrast, generally rely on decentralized blockchain technology to settle accounts between users. These currencies include cryptocurrencies such as Bitcoin and Ether, which fluctuate in value relative to the U.S. dollar, and a subset of cryptocurrencies called "stablecoins," such as USD Coin, commonly known as USDC, and Facebook's Diem, which are pegged to a fiat currency and designed not to fluctuate in value. The blockchain technology that undergirds these currencies comes in a number of variations, but it generally allows a community of users to validate transactions on a ledger instead of relying on a central authority such as the U.S. Federal Reserve. For instance, a certain number of coin holders might have to validate a transaction before coins can move from one user to another, or coin holders might have to confirm a cryptographic key. Regardless of the exact process, network users perform the formerly centralized job of a central bank.

One consequence of moving transactions outside the banking system is that transaction fees may be lower. Since 2018, sending Bitcoin from one digital wallet to another has cost an average of about $4. For transactions of a similar speed, the largest American banks charge consumers far more: roughly $28 for a domestic wire transfer (slower options, such as using the Federal Reserve banks' Automated Clearing House, cost less) and about $40 for an international transfer. But decentralized systems are not inherently cheaper than centralized ones. A centralized ledger can be run as efficiently as a decentralized one. One reason that sending Bitcoin is cheaper than sending dollars is that Bitcoin avoids much of the infrastructure—and associated fees—of the legacy centralized banking system. Some of this infrastructure, such as anti-money-laundering systems, serves a vital function. To a certain degree, therefore, the lower cost of transferring Bitcoin and other cryptocurrencies reflects lower regulatory and compliance costs that may not last. But other costs associated with the legacy payments system stem from inefficiencies that could be eliminated through competition. If the challenge posed by cryptocurrencies forces the legacy payments system to cut costs, that will clearly be good for the United States as a whole.

Cryptocurrencies can undermine essential government functions.

In addition to offering lower fees, cryptocurrencies are giving rise to a new generation of decentralized business models. For instance, blockchain-enabled file-storage businesses allow anyone who joins a network to rent spare hard-drive capacity directly to others on the network, instead of relying on Dropbox or Amazon Web Services in the middle. Other businesses allow the sharing and monetization of social media content without Facebook or Instagram as an intermediary. And in what is known as "decentralized finance," the blockchain can facilitate lending without a bank. Lots of business models might be reimagined with a community of users managing a network rather than a central company. How successful emerging technologies will be at replacing legacy systems is always difficult to predict, but the market will do a much better job of determining this than the government.

Decentralization is not, however, just another example of a new technology upending entrenched businesses, as some cryptocurrency evangelists argue. True, companies threatened by blockchain technol-

ogy will have to adapt. But cryptocurrencies don't just promise to displace private-sector incumbents. They can undermine some essential government functions valued on both sides of the aisle—and therein lies the risk that a limited public policy framework should address.

WHO CONTROLS THE MONEY SUPPLY?

One of the biggest risks posed by cryptocurrencies is that they could weaken the U.S. Federal Reserve's ability to set monetary policy. Although such a scenario is unlikely, a cryptocurrency such as Bitcoin could conceivably become a common enough medium of exchange that it puts a meaningful portion of the money supply beyond the Fed's control. In addition, although cryptocurrencies usually have predetermined formulas for coin growth or limits on the total number of coins, most allow a certain group of decision-makers, such as a majority of coin holders, to alter these protocols. As a result, coin holders, rather than central bankers, could end up deciding to increase or decrease the amount of digital currency in circulation.

So far, this is a theoretical concern. Despite being labeled "currencies," Bitcoin and its cryptocurrency brethren are mostly held as investment assets in the United States. Goods and services are not priced in Bitcoin, so most holders are using it as a substitute for assets such as gold or equities, sometimes as a hedge against inflation. One reason Bitcoin has not become a medium of exchange is that the Internal Revenue Service has said that any transaction involving digital currency is a taxable "realization event"—meaning that users need to pay tax on any gain in the value of Bitcoin between when they bought it and when they used it to purchase something. In other words, for tax purposes, Bitcoin is treated like stock, which makes it impractical to use as currency.

But even if the IRS were to change its view, Bitcoin and similar cryptocurrencies would not be widely used as a medium of exchange for a more fundamental reason: their price volatility relative to the dollar. The price of Bitcoin has varied widely in just the last year—from a low of less than $15,000 to a high of over $60,000 per coin. As a result, anyone pricing goods and services in Bitcoin would either have to accept this volatility risk or perpetually change their prices to maintain purchasing power in dollars.

Not all digital currencies face the same obstacles to widespread use, however. Unlike Bitcoin and similar cryptocurrencies, stablecoins,

such as Diem, are for the most part neither volatile nor taxable at the time of use. They are stable, as their name suggests, because they are tied to the value of a fiat currency—for example, always being worth $1. For this reason, there are no gains to be taxed when stablecoins are used in transactions, nor is there a price risk for merchants who denominate their goods and services in a stablecoin.

Over the last year, the total value of stablecoins has grown from about $10 billion to over $100 billion. And the fact that large platforms such as Facebook are behind these currencies makes them even more likely to achieve widespread use as a medium of exchange. This would not necessarily pose a risk to the Fed's ability to set monetary policy, as long as stablecoin platforms deposit a fixed dollar amount in a reserve account for every stablecoin that is in circulation. But if a stablecoin were to achieve widespread use and then change its reserve requirement from, say, $1 per coin to ten cents, the money supply could increase meaningfully. Such a decision would be made not by the Fed but by whatever group is permitted to alter the stablecoin's protocol—a private governing association or some proportion of coin holders, for example. Not only would that take important monetary policy decisions out of the hands of the government, but it could potentially allow foreign powers to gain influence over the U.S. money supply, for instance, by acquiring a majority of that particular stablecoin.

Such possibilities remain remote, but in a world where it is difficult to predict how technology will develop, policymakers should take proactive measures to prevent private-sector digital currencies from eroding the Fed's control over monetary policy. In particular, they should step up the enforcement of tax rules, including those requiring the payment of capital gains tax on cryptocurrency transactions, so that non-stablecoins remain more attractive as an asset than as a medium of exchange. Congress's effort to include properly tailored cryptocurrency tax reporting language in recent legislation is a good step in this direction. Policymakers should also require that stablecoins always maintain a fixed reserve ratio, so that they will not impede the Fed's ability to set monetary policy even if they achieve widespread use.

UNCLEAR RULES, UNCERTAIN AUTHORITIES

In addition to complicating monetary policy, cryptocurrencies could create risks within the financial system, as Powell warned earlier this year. They trade on secondary markets, both over the counter and

through exchanges that are broadly accessible to the public, but the regulatory regime around them is unclear. One source of confusion is whether cryptocurrencies are securities, which fall under the jurisdiction of the Securities and Exchange Commission (SEC), or commodities, which are the purview of the Commodity Futures Trading Commission (CFTC). Lawyers differ on this question, and there is considerable uncertainty within the industry over which regulatory regime, if any, applies to which currency. A $2 trillion market needs more clarity than this.

Even if a cryptocurrency were to fall clearly in the CFTC's jurisdiction, a second set of ambiguities would remain. The CFTC can regulate futures markets for cryptocurrencies such as Bitcoin, but it has more limited powers—just the ability to punish fraud and manipulation—when it comes to cash markets. The same exchange might facilitate trading in both futures and cash markets for Bitcoin, for instance, but the CFTC would have regulatory authority only over the former. Absent federal regulatory authority, cash markets could be subject to different regulations in all 50 states, which would be both confusing to consumers and bad for American competitiveness; entrepreneurs will do less business in the United States if they have to comply with 50 different legal regimes there but only a single regime in other countries.

Federal regulators may be able to find creative ways to assert jurisdiction, depending on the nuances of individual digital currencies. But since cash markets for digital currencies can slide through a gap in regulatory coverage between the SEC and the CFTC, Congress needs to ensure that someone has clear regulatory authority. Congress need not be heavy-handed; setting price controls to stop speculation is not the government's job. But Congress should act quickly.

Beyond jurisdictional questions, cryptocurrencies also raise financial stability concerns. For example, few rules govern reserve or liquidity management for stablecoins. As a result, coin holders may have trouble exchanging their coins for dollars, and they may assume more risk than they realize. The popular stablecoin Tether, for instance, initially claimed that its coins were backed by dollars but later disclosed that it had invested its reserves in a variety of risky assets, to the surprise of many coin holders.

As long as these currencies are not widely held, such risks will be borne solely by individual coin holders. But if the collateral underlying

a systemically important stablecoin were to be impaired, a run on the currency could occur and affect the stability of multiple markets—a scenario that becomes more likely when the economy is already experiencing difficulty. These are solvable problems that policymakers are discussing, and existing regulatory frameworks, such as the one that governs money markets, could be partially adopted for cryptocurrencies. But so far, Washington has taken few steps in this direction.

ILLICIT FINANCE

Perhaps the most immediate risk posed by cryptocurrencies stems from the anonymity they allow. The United States does not permit large numbers of dollars to move both anonymously and electronically. It requires that banks and money transfer businesses, such as Western Union, collect identifying information and perform some due diligence for high-risk transactions. Suspicious transfers and those over $10,000 must be reported to the Financial Crimes Enforcement Network, the bureau of the U.S. Department of the Treasury devoted to fighting illicit finance. These regulations haven't put financial criminals out of business, but they have created many obstacles for them. Suitcases of cash are cumbersome and risky, and electronic payments are difficult to anonymize.

Unlike bank accounts, most digital currency ledgers do not require any identifying information beyond a cryptographic key. This makes illicit activity much easier, even though anonymous flows can be tracked on a blockchain ledger that occasionally facilitates recovery from criminals. The majority of digital currency transactions—roughly between 60 and 99 percent, depending on how one measures—are for legal purposes, but the appeal of cryptocurrencies for criminals is obvious: virtually all ransomware attacks, including the one earlier this year on a U.S. oil pipeline, demand payment in digital currency, and money launderers, terrorists, drug traffickers, and tax evaders also make use of the technology.

U.S. banking laws allow the government to require identifying information for some digital currency accounts, but only at financial institutions, such as the currency exchange platform Coinbase, that are already taking steps to be good corporate citizens. The government has less clear authority to require the identification of users who hold their currency directly—on a thumb drive, for instance, or in some other form of "unhosted" digital wallet. Some private companies are developing

technology that would help identify the users of anonymous accounts, but as long as banking laws permit anonymity, there is only so much they can do. Tracing digital currency transactions across countries and through previously unused, unhosted wallets is extremely difficult.

Congress needs to pass legislation to limit the harmful effects of anonymity, in particular by barring large anonymous transfers of cryptocurrency that would be illegal within the banking system. Anonymity isn't all bad, however, and policymakers could preserve it under certain circumstances. For instance, in authoritarian countries, ID verification would make it easier for governments to track their opponents and potentially seize their assets. Policymakers must therefore balance the interest of promoting freedom abroad against the need to ensure security at home. One way to do this would be to forgo ID requirements for digital currency transactions under $10,000. Such an exception would allow most families to meaningfully protect their assets—the median savings of a U.S. family is under $10,000, and it is far less for families in most autocratic countries—while making it much more difficult to buy expensive weapons with digital currencies or demand six- and seven-figure ransoms. Such an exception could also allow anonymity for smaller day-to-day transactions, consistent with the use of cash.

Perhaps the most immediate risk posed by cryptocurrencies stems from the anonymity they allow.

One obstacle to limiting anonymity is the lack of a centralized authority to oversee ID verification. By their very nature, decentralized digital currencies resist this type of oversight. But creative thinking can likely overcome this challenge. For instance, digital currency exchanges or other private companies could maintain lists of wallets whose users have been verified, and the programs running these currencies could automatically check users against such a list. Policymakers should maintain a degree of humility, however, and not be too prescriptive about how to regulate a fast-evolving industry. If policymakers require ID verification, the market will find solutions that are compatible with decentralization and that minimize disruption.

Policymakers will also have to think creatively about enforcement. Requiring ID verification could end up driving some digital currency users to so-called anonymity-enhanced coins or to offshore exchanges and wallets beyond U.S. jurisdiction. Anonymity-

enhanced coins, such as Monero, are more difficult to track, since in addition to not requiring ID verification, they obscure other transaction details, including amounts and wallet addresses. Because their brands are so closely tied to anonymity, these coins might be less likely to comply with ID verification rules and therefore more likely to attract illicit users. Yet such an outcome would not necessarily be all bad, because it would give authorities tracking illicit finance a place to focus their efforts. The overwhelming majority of digital currency users are not doing anything illegal, and many would probably accept ID requirements similar to those needed for cash deposits or stocks, as evidenced by the broad use of regulated platforms such as Coinbase. Users who balk at these requirements and shift their transactions to anonymity-enhanced coins will have signaled something useful to law enforcement.

The spread of offshore digital currencies is a problem that the G-7 and the G-20 could tackle through the kind of coordination they already carry out on other financial issues. In fact, digital currencies are already a topic of discussion when these multilateral groups meet, and a number of countries have signaled a willingness to crack down on the use of digital currencies for illicit activity. The United States should actively engage in shaping these discussions and push other countries to adopt regulations similar to those it adopts at home in order to prevent criminals from forum shopping.

A DIGITAL DOLLAR

The final category of risks posed by digital currencies is geopolitical. Spurred by the growth of private digital currencies and the problem of slow and expensive payments, a majority of the world's major central banks are considering launching sovereign digital currencies, also known as "central bank digital currencies." Against this backdrop, the United States must consider the risks to the international role of the dollar if it does not launch its own digital dollar.

This danger is often framed too narrowly as a worry that China's digital yuan could threaten the dollar's reserve status. Beijing has made no secret about its desire to increase the share of international payments in yuan at the expense of the dollar. Mu Changchun, the digital currency chief at China's central bank, has spoken publicly about China's desire to reduce "dollarization" in the international economy. And the Chinese Communist Party certainly values the

data and surveillance capabilities the digital yuan will give the authoritarian state. Considered alongside its vast infrastructure investment project, known as the Belt and Road Initiative, China's ambition to use the digital yuan to project economic power seems clear.

Yet the United States must weigh Beijing's ambitions against its capabilities. China faces a host of structural disadvantages, including a managed exchange rate and a lack of economic transparency, that will make it difficult for its sovereign digital currency to threaten the dollar's reserve status anytime soon. Some will embrace the digital yuan, and others may be induced or forced to use it as a condition of doing business with China—something for which Washington must be prepared to hold Beijing to account. But wary of capital controls and weaker property rights in China, most people will likely think long and hard before ditching the dollar for the digital yuan at a scale that would threaten the dollar's reserve status. Put another way, the real world factors that have historically constrained China's fiat currency will also constrain its digital currency.

A more significant but largely overlooked risk of the digital yuan is that it could help Beijing facilitate sanctions evasion. One way the United States stops weapons sales to North Korea, for instance, is by imposing secondary sanctions that prevent Americans from doing business not just with the North Korean military but also with any foreign entity that transacts with the North Korean military. Because no bank can afford to lose access to the U.S. financial system, virtually none will facilitate payments for Pyongyang's military purchases. The digital yuan could provide North Korea with a way around the banking system. If a foreign company that does no business in the United States wants to sell to a North Korean military entity, both parties could open accounts with the Chinese central bank, and money could flow between them via the central bank without touching any commercial banks, avoiding the bite of U.S. sanctions. Launching a digital dollar would do little to address this threat.

Although the United States must be clear-eyed about the risks posed by the digital yuan, in particular that it could undermine U.S. sanctions, the threat to the dollar-based international system is much broader than China. International payments are notoriously slow and expensive. They flow through a patchwork of different national systems, touching multiple commercial banks in a process that adds cost and time. A new system built with a global economy in mind could

clearly improve efficiency, which is one reason so many countries are considering adopting central bank digital currencies. If central banks were to agree to provide foreigners direct account access, adopt common standards, or even share technology, international payments could become more seamless and cost effective than the current dollar-dependent system, thereby gradually eroding the dollar's international role.

Yet as real as this danger is, the United States should not panic. With the exception of China, most countries are in the early stages of developing central bank digital currencies, and the United States is engaged in international discussions aimed at setting standards for the underlying technology—meaning that it will be able to shape those standards. Moreover, the Federal Reserve is currently exploring possibilities for the technology that would enable a digital dollar, including by working with the Massachusetts Institute of Technology. Even if it does not adopt a digital dollar, the United States may be able to bless a private-sector digital currency—or currencies—that can facilitate low-cost international payments. A properly regulated stablecoin, for instance, might meet the need for efficient dollar transfers, depending on how the international landscape develops.

The United States must also consider the domestic policy implications of a digital dollar. Providing the public with direct access to accounts at the Fed could make it easier to integrate the roughly five percent of Americans who are currently unbanked into the country's financial system. But a digital dollar could also raise privacy concerns if the government has insight into individual spending decisions, or it could lead to government overreach if deposits are promised in exchange for conformity with a controversial social policy. In addition, Fed accounts could cause banks to lose deposits, diminishing their ability to make loans and hurting economic growth.

There are ways to mitigate these risks, such as using private-sector intermediaries that do not share spending information with Washington, limiting what the government can do through Fed accounts, or capping the size of Fed accounts. The United States, however, will have to balance these domestic considerations with the need to ensure that international dollar transactions are powered by technology that is efficient, resilient, and interoperable with technology being developed by other central banks. This could be achieved through a digital dollar or a properly regulated private-sector alternative, such as a stablecoin. But to secure the global role of the dollar, which has

for decades provided stability for the United States and its allies, Washington will need to adjust to—and shape—the global shift toward central bank digital currencies.

A PATH FORWARD

If digital currencies continue to gain traction, the debate over how to regulate them will only get louder. It will not be easy for Washington to find a middle path. Because digital currencies touch so many policy areas, they cut across the normal decision-making silos of the U.S. government, creating more potential for bureaucratic sticking points and risking an uncoordinated, patchwork approach. Within the executive branch, various agencies have a stake in the issue, including the Treasury Department, the SEC, the CFTC, the Federal Reserve, the Justice Department, and the State Department. In Congress, several different committees have an interest in digital currencies, including those on banking, finance, agriculture, and foreign relations.

To forge an interagency path forward, the Biden administration should regularly convene a high-level group akin to the President's Working Group on Financial Markets, which includes the treasury secretary, the Fed chair, the SEC chair, and the CFTC chair, but add the attorney general and the secretary of state or their deputies. Congress could also set up a bipartisan task force to seek consensus across committees.

Most Americans want their government to be able to respond to economic downturns, to prevent broad financial instability, and to fight terrorism and other types of crime. But most also wish to benefit from the innovative potential of new technologies such as digital currencies. Both these things can be achieved only with common-sense guardrails—and, ultimately, through a digital dollar or a properly regulated private-sector alternative. Decisions about the government's control of money must be shaped not just by software developers but by elected representatives who are accountable to the American people.