Remarks by Deputy Secretary of the Treasury Wally Adeyemo at LINKS Conference Presented by Chainalysis

November 4, 2021

As prepared for delivery

Hi everyone, and first let me thank Michael [Gronager], Jonathan [Levin], and Chainalysis for the invitation today. It's a pleasure to be with you.

Innovation has always been critical to the growth of the American economy. The industrial revolution transformed the United States from agrarian country into the most productive engine of growth the world has ever seen. Edison's invention of the light bulb illuminated the world, and the advent of the personal computer is still revolutionizing the exchange of information, goods, and services today. Our ability to promote and harness innovation has been a key ingredient in our ability to seed new industries, generate new jobs and opportunities, and maintain our global economic leadership and competitiveness.

Digital assets are yet another innovation with the potential to be transformative. Today, cryptocurrencies have a notional value of $2.5 trillion. We don't know how this new technology will evolve, but we know that like other innovations, they offer the potential to unlock new opportunities.

At the same time, experience has already shown that digital assets create certain risks. Government's goal is to create a regulatory environment that fosters responsible innovation, writing clear rules of the road that mitigate these risks while preserving the economic opportunities this technology creates.

Broadly speaking, there are three sets of risks from cryptocurrency and other digital assets that policymakers must address:

- First, there are issues of consumer and investor protection, working to make sure these assets are free from fraud and abuse.
- Then, there are issues related to financial stability, like ensuring that stablecoins are actually stable.

- And finally, there are national security concerns around anti-money laundering, terrorist financing, and ransomware.

Today, I will focus exclusively on the national security risks, and I'm grateful for the opportunity to speak with you about this. Because my sense is that there may be a misperception about the relationship between the blockchain industry and the government on this issue. There's a belief, to be frank, that we are at odds; that Treasury conceives of ransomware as a problem with cryptocurrency, and that in order to stop the former we must severely restrict what happens in this industry.

But this is not how we see things. We cannot stress that enough. It is not how we see them at all. When we regulate, rather, it's with an eye toward trying to foster innovation that creates economic opportunity and advances U.S. financial leadership while stamping out crime, abuse, and risks. We believe these goals go hand in hand with innovation.

We know that good data is critical to addressing these regulatory issues, and the US government does not have a monopoly on data in the cyber and crypto ecosystems. It is why we are investing in the public private partnership and it is why Chainalysis' work is so critical. We must expand both our data ontologies and sources of data to match the new opportunities to leverage online and technical data footprints to drive attribution and identification of criminal actors.

I am here today because we know the best way to address these national security risks is by working in partnership with the private sector. That's what I want to talk about today. I want to articulate, in some detail, what Treasury believes the relationship between our Department and the digital assets industry must be to adequately address these issues.

At its core, I think that relationship must be about keeping two stories in our heads at the same time.

Let me explain…

The first story is the story of one in every nine people on Earth, who are supported by a loved one—often working abroad and sending money back home. Some 250 million-plus migrants around the world send an average of $200 to $300 to their families each month. Today, they pay a high price for the privilege. Of that $300-dollar monthly payment to their family, they can expect to lose an average of $21 dollars – 7% -- to those operating the payments systems that get their money from Point A to Point B.

Even for people or companies transacting within wealthy nations, the cost of a cross-border payment, while lower than at any point in history, remains high. A payment among G7 nations still incurs about a 2% transaction fee. That presents a challenge, because history tells us that when that fee goes down, the pace and volume of commerce will increase.[1]

I know many of you entered the world of blockchain technology to solve problems like this one. You see cryptocurrency and related Fintech innovations as ways to make the global economy easier to navigate for everyone. And I want you to know: We share that aspiration.

Our Treasury Department is enthusiastic about financial innovation when pursued responsibly, and with an eye toward broad opportunity rather than just financial engineering. We hope that technology will help reduce the cost people pay to transact across borders, for example.

But while all of us should focus on this very hopeful story about technology, we cannot focus *exclusively* on it. There is, after all, a second and very real story that involves cryptocurrency. It's a story like the one that broke at almost the exact moment I was invited to deliver this speech last week. In Janesville, Wisconsin, a school district had its entire IT system held hostage by a ransomware attack.[2] This wasn't on CNN or in *The New York Times* – it was the local news – and for an obvious reason: It's a story that's all too common these days.

So far in 2021, cybercriminals have hacked and leaked student information from some 1,200 K-12 schools in this country, including those in Texas's Welasco Independent School District. When cyber criminals realized that the school district was never going to pay them a ransom, they leaked intimate details of 16,000 children: which kids were immigrants, which kids had dyslexia, which ones were homeless.[3]

Some version of this has happened to every kind of local institution you can think of: dentists' offices, police departments, regional hospitals. The University of Vermont's hospital was hobbled for weeks during the pandemic. Doctors were unable to pull up medical records or surgery schedules. Cancer patients had to delay their chemotherapy treatments.

And ransomware attacks like these are only a piece of the problem. You all know about the opioid epidemic deaths resulting from darknet sales paid in cryptocurrency, or the North Korean actors who stole or extorted more than $1.3 billion in fiat and cryptocurrency from financial institutions and U.S. companies. We have also seen fraud schemes involving cryptocurrencies targeted against the elderly, and terrorist networks such as Al-Qaeda

soliciting funds in cryptocurrency to support their violent campaigns. The U.S. government identified several key risks associated with virtual currency in our National Risk Assessments in 2018, and we look forward to sharing updated information in our forthcoming assessments early next year.

If we are going to recognize that cryptocurrency and blockchain technology can be the heroes of stories about more efficient and affordable financial transactions, then we also have to recognize they can be an enabler and accelerant of crime in others. Cybercriminals almost always demand ransom payments in virtual currency and exploit vulnerabilities in the virtual currency sector to receive those payments. While ransom attacks of course existed before digital assets, it's clear that these assets are a critical part of how ransomware has become such a pervasive threat. New technology is almost always susceptible to criminal use. The key question is what can we do to prevent the abuse of this technology?

As I said before, ransomware is not a cryptocurrency problem in the same way online fraud schemes are not the fault of the internet. Yes, the ability for criminals to access data online offer additional opportunities for bad actors to steal financial data, just as the unique characteristics of digital assets attract bad actors seeking the rapid, cross-border movement of funds outside of the traditional financial sector. But that is not a reason to get rid of online banking or cryptocurrencies. It is instead a reason to treat the misuse of virtual currencies for what it is – a cybercrime and national security problem – and that is a problem we can address together.

II. WHAT TREASURY MUST DO (AND IS DOING)

Let me start with what Treasury must do – and in many cases, already is doing. There are four broad sets of actions.

First, we want to build a public-private partnership around digital asset and blockchain innovation that can mitigate these security concerns. Last month, we published an OFAC Virtual Currency Compliance guide, detailing our sanctions compliance expectations. With the rollout of the guide, we pledged to work with industry to continue to clarify any issues or questions via direct engagement, which will help inform future guidance and updates. We also met with industry groups to ensure that we are tracking issues that are top of mind for all of you. This engagement is not a one time meeting, it is the first step of a sustained strategy aimed at supporting one another, and what I expect will be a continued collaboration.

The second measure is better, faster data sharing. Treasury recently released the first Bank Secrecy Act Report on Ransomware Trends to provide industry a snapshot of the suspicious activity reporting FinCEN received during the first half of 2021. But we know that information can't only flow in one direction, and we pledge to create a feedback loop. This way, the data you provide can be leveraged to inform your risk assessments and compliance decisions. The same goes for cyber threat intelligence data. We are working to create real-time data flows that will protect against future cyberattacks.

The third piece is using targeted sanctions designations not simply to hold bad actors responsible, but also to shine a light on the parts of the virtual currency ecosystem home to illicit activity – and to make it clear what Treasury sees as a threat. Right now, mixing services, darknet markets, and nested exchanges used to launder or cash out illicit funds are at the top of our list of concerns.

The fourth piece is supporting international organizations as they set standards for digital assets. Many nations haven't implemented AML or CFT standards yet for this technology, and these gaps are a real opportunity for bad actors. That's why Treasury is working with the Financial Action Task Force, which just issued updated virtual currency guidance last week. The goal is to help countries and the private sector interpret and effectively implement the Task Force's standards. We're also working with the G7 Cyber Expert Group and bilaterally with a number of countries on this issue.

III. WHAT THE PRIVATE SECTOR MUST DO

But we cannot prevent bad actors from misusing this technology alone. The private sector has an important responsibility here, too.

There are two messages that I want to stress, and the first is that compliance cannot wait. It is not something companies can put off until they scale or reach some corporate milestone. It is not something they can dismiss simply by telling us it would be too hard to comply. It must be present at the product launch and built into the fundamental architecture of your companies. I stress this point because I've seen what happens when it isn't the case.

We have uncovered a litany of examples where young virtual currency service providers have prioritized growth over compliance. They scale up. They transact worldwide, and by the time they focus on compliance, it's too late. They've discovered that they've already facilitated payments to sanctioned actors. They're on the other side of the law, and it could've been avoided.

My second message is: Don't wait for Treasury to act. Police your own platforms first for compliance, and police them to the full extent possible. We want to you to engage with us too, to tell us when you see suspicious information, and what trends you're noticing. In September, when Treasury sanctioned the SUEX exchange, it wasn't because the industry had taken no action against the entity. In fact, some industry members had frozen a few accounts. But it was a token effort. Roughly forty percent of their transaction history could be traced to illicit actors. We hope that the SUEX action demonstrated that OFAC requirements apply to the virtual currency industry the same way they do to traditional banks, and we will enforce them – although we'd much prefer not to have to. We'd prefer the industry did it itself.

I'm sure that's the preference for everybody, public and private sector alike. It certainly should be. After all, the companies who invest in AML/CFT compliance will have a competitive advantage because the standards are universal. And those investments will be good for the industry at large.

I don't think it's controversial to say that right now, some technology companies have not taken seriously the public trust and have undermined the public credibility of the entire sector as a result. If the cryptocurrency industry wants to scale – if it wants to take serious solving great public challenges like reducing the cost of cross-border payments– then it needs to operate with trust, inside the bounds of the law, and without tolerating the activity of cybercriminals and terrorists.

Treasury stands ready to help make this happen. We look forward to working with you.

###

[1] https://www.economist.com/leaders/2019/04/13/the-cost-of-cross-border-payments-needs-to-drop; https://www.un.org/sw/desa/remittances-matter-8-facts-you-don%E2%80%99t-know-about-money-migrants-send-back-home

[2] https://www.wpr.org/ransomware-phishing-and-cyberattacks-are-increasingly-hitting-wisconsin-school-districts-most

[3] https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926