Remarks by Deputy Secretary of the Treasury Wally Adeyemo at the 2023 Blockchain Association's Policy Summit

November 29, 2023

As Prepared for Delivery

Thank you to Kristin for the introduction. It's nice to be here with all of you.

Innovation, as you all know better than most, is at the core of America's economic success. We are the most important economy in the world in large part due to the ingenuity of our entrepreneurs. From airplanes and the internet to cars and smart phones, rapid technological transformations that have reshaped how we live our lives as well as the ways we think about commerce. And we don't shy away from change. A constant American advantage for centuries has been not only our capacity to embrace change but to also encourage it.

Many of you in this room are at the forefront of such change. It may be easy to lose sight of the scale of that change when you are immersed in the day to day, but over the last several years, the digital asset industry has grown at an exponential rate.

According to the Office of Financial Research, in 2021 alone, companies reported more than 2 billion transactions totaling $1.4 trillion in virtual currency transactions. That's about four times as many transactions and seven times the volume of the previous year. That's why more than a year ago, at the Consensus conference in Austin, Texas, I spoke about the tremendous opportunity digital assets present to promote innovation that helps us reimagine commerce.

But I also made clear the importance of industry proactively taking steps to prevent digital assets from being used by transnational criminal organizations, terrorists, and rogue states. I hoped the digital asset industry would take up this call to partner with government, design new tools, and pursue new ways to protect digital assets from being abused.

While some have heeded our calls and taken steps to prevent illicit activity, the lack of action by too many firms—both large and small—represents a clear and present risk to our national security.

INNOVATION WITHIN THE LAW

Today I would like to focus on the steps we must now take in order to prevent bad actors from using the digital asset ecosystem for illicit activity. I want to directly address those within the digital asset industry who believe they are above the law, those that willfully turn a blind eye to the law, and those that promote assets and services that aid criminals, terrorists, and rogue states.

My message is simple: We will find you and hold you accountable.

This is exactly what happened to Binance, the largest virtual currency exchange in the world. Over several years, Binance allowed itself to be used by the perpetrators of child sexual abuse, illegal narcotics trafficking, and terrorism, across more than 100,000 transactions. Groups like Hamas, Al Qaeda, and ISIS conducted these transactions.

In response to this egregious activity, Treasury announced our largest enforcement action in history, with a total settlement amount of over $4 billion. Equally important, we are placing a monitor within Binance that will have access to their systems, transactions, and accounts in order to ensure the largest virtual currency exchange in the world is no longer a permissive environment for illicit proceeds.

But our challenge extends beyond exchanges to other parts of the digital asset ecosystem. Earlier today, we sanctioned Sinbad.io (Sinbad), a virtual currency mixer that serves as a key money-laundering tool for a cyber hacking group sponsored by North Korea. Sinbad processed millions of dollars' worth of virtual currency from cyber hacks and enabled cybercriminals to mask illicit transactions.

Last month, Treasury announced a set of rulemakings intended to increase the transparency of mixers, making it harder for criminals and terrorists to use them to hide the source, destination, and amount of transactions. As we develop these rules, we have requested input from stakeholders in order to make sure we prevent illicit finance while permitting responsible innovation.

This action and others to cut other money-laundering mixers—like Tornado Cash—off from the U.S. financial system demonstrate that De-Fi services and platforms are not above the law. Taking steps like these to reduce the abuse of these types of services is not only in the government's interest; it is in the interest of those that seek to build an innovative industry that is on the right side of the law.

THE GROWING DIGITAL ASSET ILLICIT FINANCE RISK

It's important that we continue tackle this problem today, so that virtual currencies do not grow into a larger illicit finance threat. As we take steps to prevent terrorists, transnational criminals, and rogue states from using the traditional financial system, we cannot let them find a new outlet in virtual currencies. There are a number of reasons bad actors turn to virtual currencies, but I would like to highlight two of them.

First, illicit actors have always taken advantage of new technology. We saw this in the last decade when ISIS used social media to revolutionize jihadist recruitment. It mastered a new platform to spread its hate faster than social media companies or governments could impose appropriate safeguards. Addressing the challenge required establishing strategic partnerships between governments and social media platforms, which remain ongoing to this day.

Second, we know that risk tends to migrate to places where global regulation and enforcement are less well developed. As rogue states and terrorist groups find it harder to use the traditional financial system to move money, it is logical they would turn to less regulated ways to move assets. This is exactly what we are seeing states like North Korea and groups like Hamas do already.

The North Korean regime already accrues a great deal of its resources from cyber-criminal activity, including stealing virtual currency. Its preferred means of moving its ill-gotten gains is through the digital asset ecosystem rather than the traditional financial system. Our concern is that as Hamas is dislodged from Gaza and no longer able to extort and tax innocent Palestinians, it will increasingly use the digital asset ecosystem.

These are just a couple of examples of the risks we face today. A digital asset ecosystem that lacks a shared commitment to preventing illicit finance provides ample opportunity for groups, like North Korea and Hamas to move resources in ways that are intended to undermine our efforts to stop them.

ACCOUNTABILITY

In order to address these challenges, we need a shared commitment. When I talk about "shared commitment," I mean the digital asset industry and the government working hand in hand to cut off illicit actors before they are able to spread roots and for us to create a culture of accountability.

At Consensus 2022, I explained that our goal is to empower industry participants to do the right thing by building a responsible, compliant, and accountable digital asset ecosystem.

That means companies need to be proactive in identifying risks, establishing standards and protocols to mitigate those risks, and isolating bad actors. A shared commitment requires action from this industry.

Today, government and the traditional financial sector work in partnership to prevent the movement of illicit proceeds. We have built a regulatory framework that traditional financial firms not only adhere to, but help us to implement. These firms have invested in tools, personnel, and processes that help us identify and capture criminals, terrorists, and others that seek to move money illegally.

Just this week, the CEO of the American Bankers Association highlighted ongoing work to design, develop, and pilot a new information sharing exchange, which the ABA will manage, that focuses on combatting fraud, money laundering, and terrorist financing. This type of collaboration and proactive effort amongst industry participants both large and small is commendable and demonstrates the collective commitment that is necessary to stay ahead of bad actors.

We need those in the digital asset industry to do the same. You have the capacity to build new tools that help prevent money laundering while continuing to provide legitimate protections to individuals. You also have the capacity to cut off firms from your ecosystem that are failing to take steps to prevent illicit finance.

Without action by your industry, increased movement of illicit proceeds into the digital asset ecosystem will force us to restrict, restrain, and cut off elements of the digital asset ecosystem from the broader economy. Our actions over the last year send a clear message: we will not hesitate to bring to bear tools across government to protect our national security.

NEW TOOLS

Yesterday, Treasury provided Congress a set of common-sense recommendations to expand our authorities and broaden our tools and resources to go after illicit actors in the digital asset space.

First, we are pursuing the creation of new sanctions tools targeted towards actors in the digital asset ecosystem that allow terrorist groups and other illicit actors to move their assets. We are calling on Congress to create a secondary sanction regime that will not only cut off a firm from the U.S. financial system, but will also expose any firm that continues to do

business with the sanctioned entity to being cut off from the US financial system. This is a significant tool we do not request lightly. But we need to do everything in our power to make sure that groups like Hamas are not able to find safe haven within the digital asset ecosystem.

Second, we need to update our illicit finance authorities to match the challenges we face today, including those presented by the evolving digital asset ecosystem. For example, we cannot rely on statutory definitions that are decades-old to address the illicit finance risks we face in 2023. We cannot allow dollar-backed stable coin providers outside the United States to have the privilege of using our currency without the responsibility of putting in place procedures to prevent terrorists from abusing their platform. And we cannot permit offshore financial services providers to use jurisdiction-evasion tactics to avoid complying with our laws. We are working to close these gaps and others.

Finally, in addition to working with Congress, we are committed to working with the Financial Action Task Force (FATF) to make sure our allies and partners around the world join us in updating their regulatory approach.

The last time we pursed major reforms to this architecture was after the terrorist attacks on 9/11. The threat actors and tools at their disposal have changed, but their goals remain the same. As terrorist and criminals innovate their approach to illicit finance, we need tools to be able to keep up with them.

These reforms will not only help us curb illicit finances, but they will also level the playing field for the actors pursuing responsible and beneficial innovation and facilitate sustainable growth for the industry.

For those in the industry skeptical that the digital asset industry can grow if regulated, remember that the seat belt and air bag did not squelch Henry Ford's innovation. They simply protected people and helped to foster an environment where the automobile industry could enjoy sustainable growth. A regulatory environment that stops terrorists, criminal organizations, and rogue states from using virtual currencies to move their assets can also help legitimate firms thrive in the long term.

Thank you so much for having me here today. I look forward to the discussion.

###