Establishing the Facts Regarding Misconceptions in Senator Warren's Letter

The Crypto Council for Innovation (CCI) is a steadfast advocate for policies that spur responsible digital asset innovation, including in the context of combatting illicit finance. CCI staff and members include personnel, who come from long-standing careers in U.S. national security and law enforcement. To this end, it is important that our laws and financial crime regulations recognize the increasingly mainstream adoption of digital assets in the U.S. and abroad. Unfortunately, Senator Warren's recent letter to Treasury Secretary-Designate Scott Bessent in advance of his confirmation hearing includes many significant inaccuracies and misconceptions regarding digital assets and existing regulation. These inaccuracies and misconceptions undermine the development of sound and constructive policy, which should be focused on safeguarding our financial system, facilitating digital asset innovation, and empowering individuals, domestically and abroad, of whom the vast majority are law-abiding.

To be sure, it is a pivotal time for digital asset innovation, and it is important that the U.S. continues its tradition of leading when it comes to such innovation. To this end, CCI respectfully submits that it is critical for both the government and the industry to partner in best utilizing the benefits and attributes of blockchain technology and digital assets. This partnership and collaboration must be predicated on facts—not sensational sound bites and misconceptions. We accordingly respond in detail to some of the more severe inaccuracies and misconceptions below:

Misconception #1: Senator Warren's letter overstates the dangers that digital assets pose in facilitating illicit finance and sanctions evasion and, in turn, fails to recognize that blockchain technology can be used to help support legitimate law enforcement objectives.

Fact: Illicit finance is unfortunately a reality within all financial systems and should **not** be condoned in any form. New technologies present new risks, as we have seen since the advent of telephones, computers, and the Internet. However, the correct policy response is not to condemn the technology, but rather to learn how to use and leverage the same to combat bad actors.

Contrary to Senator Warren's assertions, the U.S. digital asset space is a model for how this can be done effectively to counter-illicit finance. More specifically, the U.S. has led global AML/CFT regulation by establishing guidance for crypto money service businesses since 2013. The sanctions evasion and terrorist financing activities that Senator Warren refers to in her letter mainly occur through exchange platforms and brokers outside the United States in jurisdictions with weak or non-compliant regulatory regimes. Additionally, it is critical to recognize that blockchain technology also possesses characteristics that can assist law enforcement in pursuing bad actors. The transparency of blockchains paired with leading-edge analytics tools enables a higher likelihood of detection and seizure. Unlike traditional financial investigations, blockchain

records are mostly public, immutable, available immediately and easily integrated into investigation tools. Therefore, rather than condemn blockchain technology and digital asset innovation, sound policy approaches will look to facilitate their responsible development and adapt law enforcement techniques to their unique characteristics.

Misconception #2: Senator Warren's reference to Treasury's November 2023 letter and term sheet reinforce fundamental misunderstandings of the inherent attributes and functions of digital asset technologies. (*See* Pgs. 20-21)

Fact*:* As has been broadly and systematically argued, Treasury's November 2023 proposal to amend the Bank Secrecy Act (BSA) and expand the definition of "financial institution" to include unhosted wallets, decentralized platforms, and blockchain validators **is not workable given the way blockchain technology works**. For example, the proposal would expand the BSA in a manner that would compromise customers' private data security and force inappropriate and unduly burdensome compliance obligations on businesses with **no** money transmission role. This expanded definition would be akin to requiring every person to register the contents of their physical wallets with a bank.

Blockchain software is open-source and permissionless, meaning much of its infrastructure is accessible to anyone on the Internet, without identification. What this means is that unlike in traditional financial investigations, blockchain records are mostly public, immutable, available immediately and easily integrated into investigation tools.

It is no coincidence that the largest government seizures of illicit assets – for instance, recovery of the Silk Road and Bitfinex Hack funds – were all enabled by tracing blockchain transactions. The world of crypto is not a "black box."

An overarching problem with the proposal Senator Warren cites is that it fails to pursue AML/CFT compliance in a manner that targets actual risks in the marketplace and that can be implemented by participants in the ecosystem. For example, it extends BSA and Know-Your-Customer (KYC) responsibilities to persons or entities (e.g., digital asset wallet providers, miners, and validators) **that cannot comply from a technical perspective with such requirements–not because they do not want to or because it is difficult to do, but because there is no actual way to do so.** This is not the risk-based approach that the BSA requires.

Misconception #3: Senator Warren suggests that OFAC does not have authority to address national security threats presented by dollar-denominated stablecoins. (*See* question 2.b (Pg. 21))

Fact: OFAC already has enforcement authority over persons and entities providing U.S. dollar-denominated financial services with U.S. touch points. Any stablecoin issuer with business operations accepting, reserving, or converting to U.S. dollars transacted in or through

the U.S. would be subject to sanctions enforcement actions through the touchpoints of those USD-related activities.

Instead of implying non-compliance with OFAC obligations, we would respectfully encourage Senator Warren to focus on working constructively on bipartisan legislation that would create a clear, comprehensive regulatory framework for USD stablecoins. This can help foster further responsible industry growth, and cement the role of the USD as the primary global reserve currency.

Misconception #4: Senator Warren's letter suggests that the Treasury lacks the authority to enforce the BSA and the International Emergency Economic Powers Act (IEEPA) with respect to foreign entities with U.S. touchpoints. (See question 2.c. (Pg. 21))

Fact: The U.S. has the authority to penalize—and indeed has penalized— foreign entities for BSA and sanctions violations with sufficient U.S. contacts. For example, FinCEN and OFAC in November 2023 fined Binance–a non-U.S. crypto exchange–over $4 billion for violating BSA and sanctions rules. In fact, going back more than a decade, multiple global banks such as HSBC and BNP Paribas have similarly been penalized for U.S. sanctions violations.

Misconception #5: Senator Warren's letter suggests that Treasury needs a secondary sanctions tool that would allow it to sever fintech and crypto operators from U.S. relationships (See question 2.a. (Pg. 21))

Fact: This is unnecessary. It is analogous to the Correspondent Account or Payable-Through Account (CAPTA) sanctions, but OFAC currently uses CAPTA sparingly, to target correspondent banks outside the U.S. Because there is no correspondent banking-equivalent role in the cryptocurrency space, the need for special targeting of crypto exchanges outside the traditional sanctions designation process would not be justified.

OFAC should use its primary designation authority (which can cover offshore exchanges servicing comprehensively sanctioned locations) instead of putting secondary compliance obligations on U.S. exchanges. In fact, Treasury has done this by designating foreign crypto exchanges like Russia-based Garantex that supported cyber criminals and Buy Cash, which serviced Hamas in Gaza. Secondary sanctions were not needed to target these entities.

***