TESTIMONY OF WILLIAM C. HUGHES
Senior Counsel & Director of Global Regulatory Matters
Consensys Software Inc.
Before the United States House of Representatives
Committee on House Financial Services
Subcommittee on Digital Assets, Financial Technology, and Inclusion
Hearing on Crypto Crime in Context: Breaking Down the Illicit Activity in Digital Assets
November 15, 2023

Chairman Hill, Ranking Member Lynch, and distinguished members of the Subcommittee, I thank you for the invitation to testify on the important issue of illicit activity in digital assets. This is a critical topic for the Congress to debate, and I applaud your leadership in bringing this to the attention of the Committee. Permissionless blockchain networks are new technologies that have real value and present exciting new opportunities, but we at the same time must not accept or equivocate about bad actors using these technologies to commit crimes.

I work as a senior legal counsel at Consensys Software Inc., a software developer that is headquartered in Fort Worth, Texas. As a U.S.-based technology company, we believe that it is good that technology providers are expected to follow the law. In our experience, US-based blockchain projects generally do. How the law should evolve to meet the dynamic threat of illicit finance is an important issue, and we are glad to be part of that discussion.

Our firm develops and offers the most popular unhosted wallet software in digital assets, the MetaMask wallet. This offering is open source software that can be downloaded for free from the Apple app or Google extension store, and installed on any Google Chrome browser, iPhone, or Apple desktop computer. The wallet is an interface that allows the user to read and write to the blockchain without any intermediary's help, akin to how a web browser is a consumer's direct connection to the open web. The wallet also safeguards a user's private key, which is the cryptographic password which the user must have to control a particular blockchain account, also called a public address.

In these respects, there is nothing particularly different about MetaMask from any other blockchain wallet software that serves as an interface to the Ethereum blockchain. Users in the U.S. and across the globe are free to use a long list of wallets to read and write to the blockchain and to securely store their private keys, and some users often use multiple wallets to control a particular address or switch back and forth among several wallets made by different developers.

In addition to the basic wallet functionality, MetaMask also offers users various software-as-a-service options that they can leverage as they explore or build on the blockchain. These offerings allow them to search smart contract protocols in decentralized finance, to explore the various methods of moving from one blockchain to another, to participate in the core consensus mechanism of the blockchain, and to engage regulated third parties who can offer them fiat-to-crypto exchange services. Our goal with MetaMask is to make Web3 accessible, intuitive, and useful for everyone.

And that especially includes software developers. MetaMask is a great tool for builders around the world who are inspired to create new applications and are now, with blockchain, empowered to do so in a way that allows them to connect directly with software users, cutting out Big Tech gatekeepers. It is our firm belief that the drive to build is in each of us, and we hope to cultivate the drive to make things better, for ourselves, our communities, and future generations.

While we have an unwavering conviction that Web3 can be an overwhelmingly powerful and good force for humanity, it also has been shown that a cutting edge and permissionless space can be abused by bad actors. Illicit activity on-chain is a challenge that must be addressed if this technology is going to make the world a better place.

Combating money laundering is a difficult task in any space, but digital assets present capabilities with respect to tracking money laundering that law enforcement and the public at large have never before had. Because open, permissionless blockchain ledgers are reviewable by anyone, transactions can be traced using blockchain analytics technology, even those that are purposefully complicated to obfuscate the flow of funds. Any policy response to the threat of money laundering should embrace the transparency of the blockchain and bolster the power of transaction analytics if it hopes to be successful. While analytics technology is helpful now, it must continue to improve if illicit finance in digital assets is going to be sufficiently addressed.

Digital assets also present some new challenges. Today, the critical weaknesses remain the centralized entities that provide exchange services off-chain. These run the gamut from billion-dollar, international crypto exchanges to neighborhood shops in far flung reaches of the world that will trade tokens for fiat currency over the counter. These centralized entities also include companies that offer stablecoins, which in certain instances have been used in the layering stage of the money laundering process. From our perspective, the single most important initiative in a fight against digital asset money laundering would be to regulate these entities under a common legal framework worldwide.

On-chain security is also key, and it is a core focus of Consensys when we think about MetaMask users. Users can be targeted by scams seeking to part them from their tokens, either through phishing campaigns, social engineering attacks, or malicious smart contracts. While it is a tiny fraction of users who may be affected by these scams, it is an issue that should be taken seriously. Effectively combating illicit activity in digital assets is not possible without addressing these issues as well. We are working hard at making the MetaMask interface more informative as to threats that a user may face when exploring web3, including a recent update that by our estimate has prevented roughly $500 million in lost funds to date. We also strongly believe that smart contract auditing, the process by which on-chain software is audited against security standards to ensure the code does not contain any latent vulnerabilities, is an important tool to thwart hackers. The ecosystem must continue to work on improving security best practices, and there is likely an important role that government can play in facilitating these types of efforts.

As everyone recognizes, money laundering and other illicit finance is not unique to blockchain. Traditional finance remains the overwhelmingly popular space for launderers to operate, and the estimated volume of illicit activity on-chain when compared with licit activity is remarkably low. But whatever the case may be, illicit finance is a serious concern that deserves our attention, and we must be vigilant that such use of digital assets does not become more prevalent.

This can be done by getting more global uniformity in regulating exchanges and stablecoins. It is regrettable that other jurisdictions are ahead of the U.S. in this regard, and we should work swiftly to correct that. Policymakers should consider regulatory sandboxes to improve not only blockchain analytics technology but also technologies around digital identity. Blockchain offers the opportunity to actually improve privacy protections and data security while also achieving compliance, and we should not turn it down but rather fully explore what is possible. We must also improve public/private collaboration on difficult policy issues such as those presented by decentralized finance, and bolster intelligence sharing to put law enforcement in the best position to trace, stop, and recover laundered funds.

Productive policies with respect to combating money laundering using digital assets is a net good for the blockchain ecosystem. Consensys is honored to have been asked to contribute to this discussion and applauds this Committee for taking a leadership role on these issues.