FOR IMMEDIATE RELEASE

Modulus Security Bulletin to Digital Assets Exchange Operators: Extreme Risk in Using Chinese Software Providers

Scottsdale, Ari. – July 17, 2023 – Today, Modulus, a US-based developer of ultra-high-performance trading and surveillance technology that powers global equities, derivatives, and digital asset exchanges, issued a security bulletin warning digital assets exchange operators of the dangers created by using Chinese software. This includes vendors which claim to be headquartered in Singapore but have strong ties to Chinese businesses and the government. In addition to ongoing security and privacy concerns across all sectors, China is known as a haven for cryptocurrency fraud. This is particularly acute among providers offering "big data analytics,", giving them unfettered access to client data. Certain Chinese software providers also offer custody and fund management services, creating a potential fraud nexus.

The Chinese government's engagement in the cryptocurrency industry, through companies offering software used to launch crypto exchanges, poses security threats to the United States and its allies:

Cybersecurity Risks: Cryptocurrency exchanges involve a high volume of sensitive information, including the personal and financial data of users. Modulus data scientists have studied software from dozens of providers across the globe, and they found that Chinese-backed firms, including those using Singapore as an official headquarters, routinely produced software with vulnerabilities and hidden backdoors. Both create tremendous potential for data breaches and other cyberattacks.

Financial Manipulation: Companies under the influence or direction of the Chinese government can manipulate the price, availability, or liquidity of certain cryptocurrencies, affecting global crypto markets and potentially destabilizing financial institutions or businesses that rely on these markets.

Sanction Evasion: Cryptocurrencies are often used to circumvent economic sanctions due to their borderless and semi-anonymous nature. If a hostile country provides the software for exchanges, it could enable sanctioned entities to evade these restrictions, thus undermining U.S. foreign policy objectives. It is recommended that the government of the United States, as well as allied nations, specifically ban exchanges using Chinese-backed technology within their borders. Regulators will be receiving a copy of this report, in addition to scientific studies completed by Modulus scientists.

Intellectual Property Theft: Cryptocurrency platforms are built from advanced and often proprietary technology. If American businesses utilize software provided by a foreign government-controlled entity, there is always a risk of intellectual property theft or espionage. Over the past decade, the risk of IP theft has been particularly acute within China and India.

Surveillance and Data Harvesting: Companies with close ties with the Chinese government can use the software they offer to exchange operators to conduct mass surveillance and harvest valuable data about users, including American citizens and corporations. This data could be used for various purposes, from identifying high-value targets for cyber-attacks to gaining competitive intelligence.

Digital Sovereignty: In a broader geopolitical context, the Chinese government's influence on global cryptocurrency infrastructure could represent a challenge to American digital sovereignty and its influence on the global financial system.

Regulatory Compliance Risks: There may be regulatory compliance risks for American companies that use a platform potentially controlled or influenced by a foreign government. These could come from U.S. regulators concerned about consumer protection or from international regulators. Over the past year, TikTok has seen this very risk play out on the American political stage.

Decentralization and Control: One of the main tenets of cryptocurrency is its decentralized nature, which could be undermined by the influence of a state actor. This could lead to a loss of confidence in the system and create potential negative economic implications.

National Security: If cryptocurrencies become a significant part of the economy, control over them would have national security implications. For instance, a hostile state could try to destabilize the global economy through the control or manipulation of cryptocurrencies.

Dependency and Influence: If Chinese companies' software becomes widely used, it could increase dependency on the software and allow China to exert greater influence over the global financial technology ecosystem.

Additionally, Modulus scientists have pointed out that China has a very high rate of cryptocurrency fraud. Examples include:

PlusToken Scam: One of the biggest cryptocurrency scams in history, PlusToken originated from China. PlusToken presented itself as a cryptocurrency wallet that would reward users with high rates of return if they purchased the platform's PLUS tokens with Bitcoin or Ethereum. In June 2019, the platform abruptly closed, and the founders

disappeared with an estimated $2 billion in cryptocurrency, affecting millions of investors.

WoToken Scam: Similar to PlusToken, WoToken was another Chinese-based Ponzi scheme that defrauded investors out of an estimated $1 billion worth of crypto assets from May 2018 to October 2019. Users were promised high returns for their investment and were incentivized to recruit others to invest in the scheme.

Cloud Token Scam: Cloud Token was a mobile app that claimed to generate profits through the use of a smart trading algorithm, promising users high daily returns on their investment. It was found to be a Ponzi scheme, and the operation was primarily promoted in Asia. While it was not exclusively based out of China, a significant portion of its activities were targeted towards the Chinese market. The scam collapsed in late 2019, leading to significant losses for investors.

Modulus executives have offered the following opinion:

While the Chinese government has publicly taken steps to crack down on cryptocurrency fraud and to regulate the industry, the anonymous and borderless nature of cryptocurrencies and very limited legal recourse for victims outside of China makes it an attractive country for fraudulent schemes.

To manage these risks, companies should consider utilizing software from countries with maximum legal recourse, conducting thorough background checks, audits, and consulting with legal experts to ensure compliance with all relevant laws and regulations. Governments outside of China may also need to step up their oversight and regulation of the cryptocurrency industry to mitigate potential threats.

###

About Modulus:

Since 1997, Modulus has provided advanced financial technology products and services to financial exchanges; brokerages; trading firms; hedge funds; and educational, governmental, and non-profit institutions throughout more than 100 countries. The company's products and services reach millions of users around the world. Modulus is the largest holder of fintech IP on the planet.

To schedule an interview with CEO Richard Gardner, contact Modulus Chief Communications Officer Charles Catania at chuck@modulus.io, or via telephone at 860-299-3689.