CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

NIST Stablecoin Report Highlights Security and Stability Concerns

By **Mercedes Kelley Tunstall**
Partner | Financial Regulation

The National Institute of Standards and Technology ("NIST"), a non-regulatory governmental agency that focuses upon the technological aspects of a wide variety of products and services, mostly non-financial in nature, published a final Internal Report titled, "Understanding Stablecoin Technology and Related Security Considerations" on September 5, 2023. An early draft of the report was first published in October 2022.

NIST explains that the report is intended to offer "a technical description of stablecoin technology to enable reader understanding of the variety of ways in which stablecoins are architected and implemented [and] then uses that technical foundation to explore related security, stability and trust issues." While the Cabinet is generally focused upon regulatory financial and economic considerations, the NIST report nevertheless provides an excellent grounding in stablecoin terminology and concerns that will be useful for any institution or regulator seeking to deal with stablecoins.

The report begins by identifying four "properties" that typically apply to all stablecoins. Stablecoins are "tokenized", meaning that they are a cryptocurrency token managed by smart contracts. Stablecoins also are "fungible", meaning that they can be substituted for each other and are not unique, but also meaning that they have little to no pricing volatility, relative to their pegged asset or index. They are "tradeable", and finally, they are "convertible" in that they can be converted to other currencies or the pegged asset.

The report then identifies six different use cases for stablecoins that are defined by the common properties discussed above and a combination of ten characteristics such as whether the stablecoin is designed in a custodial context or a management context. The use cases include: 1) fiat currency-backed stablecoins; 2) cryptocurrency-backed stablecoins; 3) non-currency asset-backed stablecoins (*i.e.*, "a stablecoin whose value is backed through reserves that are non-currency assets or financial vehicles tracking the price of such assets"); 4) algorithmic non-collateralized stablecoins (*i.e.*, "a stablecoin whose value is stabilized through an algorithm that shrinks and expands the supply of non-collateralized coins to adjust price"); 5) hybrid stablecoins; and 6) private institutional stablecoins (*i.e.*, stablecoins issued for use on private blockchains).

The security issues identified in the report potentially could apply to all stablecoin use cases, and include the following: 1) unauthorized or arbitrary minting of stablecoins could occur in certain situations; 2) vulnerability in smart contract codes could lead to the theft of the stablecoin's on-blockchain collateral or reserves; 3) smart contract codes used in conjunction with stablecoins could be maliciously hacked or updated; 4) the data streams that provide stablecoin smart contracts with off-blockchain information such as the price of a currency (which are called "data oracles") could be disrupted through denial-of-service attacks and thereby disrupt the functionality of the stablecoin; and 5) the underlying blockchain could be attacked, although this security risk is characterized as being "unlikely."

The stability and trust issues the report identifies vary based upon the use case of the stablecoin, as well as the kind of marketplace that the stablecoins are traded upon. For example, centralized finance marketplaces ("CeFi") can be more vulnerable to trust concerns due to their greater reliance on human trustworthiness, while decentralized finance marketplaces ("DeFi") can be more vulnerable to security issues due to "increasing smart contract code complexity and critical functionality." Other kinds of stability and trust issues discussed include some of the problems that already have arisen with some stablecoin ventures. These issues include topics such as data oracles not providing data to the stablecoin smart contract fast enough, mass user departure from the stablecoin, and native cryptocurrency devaluation.

In evaluating the security, stability and trust issues identified, the NIST report remarks that they "found that two stablecoins that function almost identically in third-party markets and enable the buying and selling of goods with coins at a pegged price can have vastly different risk profiles." Accordingly, companies and financial institutions that are interested in developing stablecoin projects must carefully weigh the security implications tied to the architecture, use case and marketplace for the stablecoin and design technological, as well as operational, controls to address those security problems, but also any applicable stability and trust issues.
