Trail of Bits
Defense Guided by Experience
228 Park Ave S #80688
New York, NY 10003

Dan Guido, CEO
dan@trailofbits.com
@dguido / @trailofbits
+1 (347) 455-0009
www.trailofbits.com

August 24, 2018

Gemini Trust Company, LLC
600 Third Avenue, 2nd Floor
New York, NY 10016

In April 2018, the Audit Committee of Gemini Trust Company, LLC ("Gemini"), a New York trust company, engaged Trail of Bits, Inc. ("Trail of Bits") to conduct a security assessment of the smart contracts underlying the Gemini dollar token, a fiat-pegged stablecoin issued by Gemini and built on the Ethereum network according to the ERC20 standard for tokens.

Trail of Bits performed this assessment from May 7th to June 8th, 2018. The assessment focused on the ERC20 capabilities of the Gemini dollar, including minting, burning, and sweeping, as well as the upgrade mechanism. Two engineers from Trail of Bits conducted the assessment over the course of eight person-weeks. The goal of the assessment was to discover flaws that could allow an attacker to perform actions meant only for the issuer, Gemini.

Trail of Bits brings decades of security knowledge to the field of smart contracts, and has invested in building the best available tools for assessing their security. In addition to reviewing the code through manual effort, the construction of the Gemini dollar was evaluated with static analysis, property testing, and symbolic execution. Review of the authorization schema, upgrade system, and sweeping mechanism were given priority. Gemini provided Trail of Bits with direct access to engineers on the project and all available source, testing, and deployment code.

The reviewed code was written with an obvious intention of minimizing security risks. The contract logic is composed of discrete, testable components, each with a clear purpose. Gemini conducted extensive security tests prior to the engagement and worked with Trail of Bits to improve them. Two high-, two medium-, four low-severity, and one informational issue were found in the course of the assessment. Gemini addressed the issues as they were discovered, and Trail of Bits reviewed their fixes during the final week. All discovered issues were resolved.

Sincerely,
Dan Guido