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

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

February 21, 2020

To Whom It May Concern:

Trail of Bits, Inc. (“Trail of Bits”), a cybersecurity research & development firm, was engaged to conduct a security review of the Chai ERC20 token smart contract.

Trail of Bits performed this assessment from February 3 to February 4, 2020 for a total of two days with one security engineer working from commit `e32f5acfbe268ac7255ce929ce7e68b6e255f986` from the dapphub/chai Github repository. The review was carried out using a combination of manual review and automated analysis using Slither and Echidna to detect any security-related issues. The review focused on identifying any additional risk inherent in using Chai over depositing into the Dai Savings Rate directly, such as locked funds. Additionally, Trail of Bits focused on verifying the contract contained no upgradeability mechanism or privileged user roles.

The contract is short and is mostly comprised of standard ERC20 token functionality. Chai does not contain any upgradeability mechanisms or special roles, even for administration. It does not appear to contain additional technical risk over similar products.

Trail of Bits identified one informational-severity issue for an area where documentation could be improved: Chai, mimicking the behavior of Dai, allows an infinite allowance to be set. This behavior diverges from expected ERC20 behavior but does not introduce security concerns we are aware of. However, it should be noted in documentation so that users are aware of this feature. No other issues were found during the two-day engagement.

Sincerely,
Dan Guido