February 20, 2015

Mr. Christopher Kirkpatrick
Secretary
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, D.C.

Dear Mr. Kirkpatrick:

I am submitting this comment on behalf of BitGo, Inc., a leading bitcoin security software provider based in Palo Alto, CA. BitGo is a pioneer in multi-signature ("multi-sig") technology and leads the industry in defining best practices and standards for security. We count among our customers exchanges like Bitstamp and TeraExchange, hedge funds like Binary Financial, miners like Bitfury, and consumer services like ChangeTip.

LedgerX plans to use the BitGo platform to secure the bitcoins held as collateral in its clearinghouse. In this comment, we want to provide our expert perspective on the robust and secure structure LedgerX has designed for its clearinghouse bitcoin account model.

For background, I encourage you to review two pieces of background reading that outline the importance for the bitcoin ecosystem players to move to multi-sig:

- *What is Multi-Sig, and What Can It Do? (A Backgrounder for Policymakers)* by BitGo co-founder Ben Davenport published on Coin Center (https://coincenter.org/2015/01/multi-sig/); and
- *It's Time to End the Cold Storage Ice Age and Adopt Multi-Sig* by BitGo co-founder and CEO Will O'Brien (https://medium.com/@willobrien/its-time-to-end-the-cold-storage-ice-age-and-adopt-multi-sig-8589733c9fd6)

The security model historically used by exchanges includes two single-key bitcoin accounts: a hot wallet (with the private key held on a server) and a pool of cold storage (with the private key held offline in a physical vault). This approach has led to numerous hacks at exchanges because the compromise of a single private key can reward a hacker with all of the bitcoins in that account.

With the advent of multi-sig, the security and transparency of bitcoins held by exchanges has reached a new level of sophistication and trust.

Using the BitGo platform, which has been in the market since August 2013 and scaled to support some of the largest volume customers in the ecosystem, LedgerX will use a 2-of-3 key multi-sig architecture where 2 keys are required to sign each transaction. One key is held in an operational key server by LedgerX, a second key is held in an operational key server by BitGo, and a third key is held cold, offline, by LedgerX for disaster recovery. LedgerX initiates each blockchain transaction and BitGo co-signs the transaction after running a robust set of authentication verification, transaction signing policies and fraud detection. For example, LedgerX can set a velocity limit such that BitGo will stop co-signing if too many sequential transaction requests are sent. LedgerX can also establish a whitelist of recipient addresses and set restrictions for what time of day transactions should be allowed.

By distributing the two operational keys across two organizations, there is no single point of attack like there has been historically at other exchanges. If the systems at either LedgerX or BitGo are compromised, a hacker cannot steal funds. If an operational key is lost, the backup cold key can be used to move funds.

Further, because keys are held by multiple institutions, there is increased transparency. LedgerX participants can view deposits and withdrawals for LedgerX accounts on the blockchain to confirm transfers. BitGo also provides a view-only role, via its software platform, which enables outside auditors to monitor holdings at all times.

In summary, LedgerX is deploying the best-in-class security software and operational processes, significantly increasing the security and transparency of its exchange as compared to its peers. There is no ambiguity as it relates to LedgerX's secure holding of bitcoin.

BitGo thanks the Commission for the opportunity to comment and stands by to provide more information as needed.

Thank you.

Will O'Brien
CEO
BitGo, Inc.