Brent Fields, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

Nov 5, 2016
Via e-mail: rule-comments@sec.gov

Continued Comments on SR-BatsBZX-2016-30 (Winklevoss Bitcoin Shares)

Mr. Secretary,

I am writing to make addendum and correction to my previous comments. In my previous correspondence, I stated:

> *I would like to see a monthly "proof of control" audit of all of the fund's bitcoin performed by the Custodian and provided to the Sponsor, who will display the signed messages on their website to publicly demonstrate proof of control. The message to be signed can be the mined hash of a predetermined block height, which is guaranteed to be both easily verifiable and unknown in advance.*
>
> *The signatures can be created with the private keys still in cold sold storage and air-gapped. Publicly identifying the addresses holding the funds adds no risk to them being stolen due to the nature of bitcoin. The funds remain secure from even quantum attack as the public key is never revealed. No additional risk is incurred by doing so, and opening control to public audit vastly increases confidence in possession and control of the underlying asset.*

It has been pointed out to me by a colleague that a message signed with the private key of an address does indeed reveal its public key, making it potentially vulnerable to a quantum attack. Since the last thing I would want to suggest be enshrined in regulation would be something that could one day lead to a compromise of the ETF's assets, I would like to rescind my request for a public proof of control audit.

I still believe that the spirit of the request; public transparency of the fund's assets to maintain confidence in the ETF's custodianship of the underlying bitcoin assets. This can be accomplished by publicly maintaining a list of all of the addresses currently holding bitcoin belonging to the ETF. Unlike signed messages, revealing Bitcoin addresses provide no risk of quantum attack as long as they have never been used to send funds. This, along with private audits confirming control of the addresses and a largely standard tranche size per address, should provide adequate transparency to assure public confidence in the custodian.

A condition can be made that the custodian must transfer to a new address if the funds have not moved in a significant amount of time, ex. one year, in order to demonstrate proof of control while remaining invulnerable to quantum attack. A hash of an auditor defined message can be included in the transactions to ensure it was actually the Custodian that transferred the funds and not another party.

I would like to take this opportunity to dispel some misinformation by other commenters regarding a potential quantum attack. A theoretical quantum computer would be able to reverse the ECDSA encryption of a bitcoin public key (once one is revealed) to determine a private key capable of transferring the funds, however a quantum computer provides no additional capabilities in reversing hash functions such as SHA-256 and RIPEMD-160 that are used in bitcoin. The latter of which is used to hash public keys into addresses, making them invulnerable to quantum attack.

Any assertion that "a quantum computer can try all key combinations at the same time" is absurd and patently false. The bitcoin private key space is 2^{256}; in decimal format the number of possible combinations is:
11,579,208,923,731,619,542,357,098,500,868,790,785,326,998,466,564,056,403,945,758,400,791,312,963,993

No computer conceived by man smaller than a galaxy, quantum or otherwise, would be able to even count to this number within human lifespan, let alone attempt hashing functions on each permutation. Quantum computers are potentially extremely powerful, but they are not magical.

Thanks again for the opportunity to comment.

Sincerely,

Michael B. Casey