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

July 31, 2016
Via e-mail: rule-comments@sec.gov

Comments on SR-BatsBZX-2016-30

(Winklevoss Bitcoin Shares)

Mr. Secretary,

Thank you for the opportunity to provide comment on the proposed rule change. Having read the rule change in its entirety, I can attest that it is an accurate representation of the machinations of Bitcoin and a feasible way to offer shares as an ETP. I have only one minor issue that I would like to address, but otherwise wholeheartedly endorse this rule change and the ETF it will allow into creation.

On page 45-46, the proposal states:

> *The Custodian's Cold Storage System was purpose-built to demonstrate "proof of control" of the private keys associated with its public Bitcoin addresses. More specifically, the Custodian can use Signers to sign a specific message chosen by the Custodian that references a current event (i.e., to prove recency), thereby proving control of the private keys associated with the public Bitcoin addresses in which the Trust's bitcoin are held. This allows the Custodian to evidence control of the Trust's assets periodically during audits on-demand and without necessitating the transfer of any of the Trust's bitcoin*
>
> *[…] Additionally, the Sponsor must engage an independent audit firm to biannually verify that the Custodian can demonstrate "proof of control" of the private keys that control the Trust's bitcoin ("Proof of Control Audit"). One Proof of Control Audit will be conducted at the end of each calendar year and the other at random.*

While in most instances this would be a satisfactory audit control to guarantee 100% reserve of an underlying asset, I don't find this satisfactory for bitcoin. The proposed rule change requests the process be performed twice a year by the Custodian for a 3rd party auditor commissioned by the Sponsor. While I in no way object to this procedure and schedule, I would like to see additional steps mandated by the SEC to ensure the unprecedented transparency and auditability Bitcoin be employed to protect the consumers of this ETP.

Built into the reference client at a very early version, and into the design of Bitcoin itself, is a method of establishing "Proof of Control" beyond any doubt. The private key controlling an address to be proven may be used to sign a message generated recently, thereby proving recency

of control (similar to a hostage holding up today's newspaper in a picture to demonstrate proof of life). Earlier in 2016, Dr. Craig Wright made the bold claim that he was in fact the creator of Bitcoin, Satoshi Nakamoto. This claim was not taken seriously by anyone of note in the Bitcoin community after his failure to publicly prove control of addresses known to belong to Satoshi.

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. Doing so would not place an undue burden on either the Sponsor or Custodian as less regular audits are scheduled anyway.

In 2013, the Mt. Gox exchange operated for months apparently running a fractional reserve after the majority of its funds were lost due to incompetence or malfeasance. Being a completely unregulated exchange, this is no surprise. I would like to know that in a legitimate, regulated Exchange Traded Fund that there will be no chance of that happening. Taking the steps outlined above will ensure that there isn't.

That being my only concern with the proposed rule change, I greatly look forward to the establishment of a Bitcoin ETF to allow entities access to this new asset class without the burdens of custodianship.

Thanks again for the opportunity to comment.

Sincerely,

Michael B. Casey

[redacted]