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

July 26, 2016
Via e-mail: rule-comments@sec.gov

Notice of Filing of a Proposed Rule Change to BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, to List and Trade Winklevoss Bitcoin Shares Issued by the Winklevoss Bitcoin Trust

(Release no 34-78262, File no SR-BatsBZX-2016-30)

Dear Mr. Fields:

We appreciate the opportunity to provide comments on the proposed rule change. We follow its terminology as closely as possible. Please also note that by "Satoshi Nakamoto" we refer, obviously, to the pseudonym commonly used to designate the father of Bitcoin.

1. Death of Satoshi Nakamoto

A mountain of electronic cash or gold, the "treasure" of Satoshi Nakamoto estimated to be approximately one million bitcoin, easily catches everyone's attention. This contributes, sadly, to the relentless drama and bizarre shenanigans around his real-life identity. It seems to threaten Bitcoin itself, supporting the picture of a controlled supply economic system with one person controlling around 5% of its total value – in the style of the massive wall of water resembling a menacing prolongation of Mount Fuji as depicted in The Great Wave off Kanagawa. These issues are likely less serious than they may appear at first glance.

Roland Barthes referred to the idea that the creation transcends its creator as the Death of the Author. In this respect we assume that Nakamoto, the creator, is dead. When many people wonder why he has vanished, this may be because Nakamoto, the individual, is well aware that he can hardly coexist with Bitcoin. For this reason, he is the least likely person to gesticulate in front of everyone to pretend to be alive. And reasonable people know that conjuring tricks have never brought someone back to life. We believe that a rather more appropriate Hokusai analogy would be The Watermill at Onden. There, the water is under control and predictable, as well as rationalised and exploitable. The mountain is just part of the landscape.

2. Timely Project

Bitcoin is in a pivotal year. It enjoys growing acknowledgement, both positive and negative. The mere fact that it has just appeared in a popular television programme, "Mr. Robot", is not insignificant: art mirrors life. The numbers speak, too. Currently the average number of daily transactions is 200,000, more than 350,000 unique addresses are being used, and the hash rate is more than a billion of billion hashes per second. The ecosystem is unequivocally maturing. Bitcoin is the first successful implementation of a chain of blocks of transactions used as a distributed database. However, at the same time, like the mind of a teenager in a growing body, it suffers from an identity crisis. This crisis is multiform. Is it digital cash or electronic gold? Is it a currency or a commodity? Is it dirty money or legitimate safety net/investment? Currently, the true answer is: all of the above. Only time will clarify a number of points, but there is no doubt that Bitcoin will always be used by regular people as well as bad guys: such is the nature of money in the broad sense. Bitcoin is not immoral, it is amoral. Bitcoin has no flesh nor soul.

It is intriguing to see that in 2016 some people still think Bitcoin is a Ponzi scheme, as demonstrated in the comment submitted to you on July 13. If, with a little bit of alchemy, we substitute "gold" for "Bitcoin" in this submission, we realize the gold market must be a Ponzi

scheme, too. The value of gold is not intrinsic, its price is speculative, the only way to make a profit is to sell the metal for more than the purchase price, ownership of gold does not yield any dividend or interest, etc. Gold, obviously, is not a Ponzi scheme. Neither is Bitcoin. We must add that Bitcoin has fundamentals. In a nutshell, supply is strictly controlled and limited, bitcoin are not created out of thin air but require a massive amount of electric and computational power... And, obviously, it has real-world applications. The fact that a man has travelled around the world only on bitcoin gives a demonstration of this statement[1]. It has to be observed that Bitcoin is far deeper, economically speaking, that some distorting mirror can make it seem.

A final thought. Bitcoin is fundamentally effortless from the user's perspective. A short string of text such as "1DD2PNmi3fi43TjzUgScf513iTj9GrL8o7" is enough information to be able to directly send and receive any amount of bitcoin to and from anybody in the world. In practice, however, using Bitcoin may appear more complex and forbidding: fear of theft, concerns about legal and tax issues... In this respect, the Trust can help a whole category of people to gain access, albeit indirectly, to Bitcoin. For them, the Trust may constitute a familiar and reassuring interface with an uncommon and powerful asset. (we even think that it can initiate a momentum contributing to the legitimation and democratisation of Bitcoin)

We then support the goals of the Trust and find it appropriate and timely.

3. No Insurance

According to the proposed rule change, the Trust's bitcoin are not insured. The brief history of cryptography based electronic payments indicates this choice is probably not the most insightful. Recent examples provided below can demonstrate this.

In July 2015, a chief security officer at Gemini, the Custodian, released a security review of several Hardware Security Modules: "Critical to this security design is that secret keys never leave the HSM itself; all operations take place within the secure execution environment of the HSM." "While evaluating the Luna G5, we discovered a vulnerability that allows the extraction of secret keys. As it turns out, the problem is not unique to the G5; it applies to the entire family"[2]. The very raison d'être of HSMs is to keep electronic secret keys secure. Some of them have failed to protect their keys, at least hypothetically, and some of them will possibly fail in the future. They are secured, but not impenetrable. It is worth noting that Gemini was able to discover such a failure by itself, which seems to indicate that, currently, the Custodian has adequate technical capabilities to make the Trust's bitcoin reasonably safe.

Between March and April 2016, the digital currency exchange ShapeShift has been hacked thrice and lost about US$230,000 in a process manifestly triggered by an employee aliased "Bob"[3]. In the colourful crypto-world, ShapeShift is one of the few companies thus far that has been able to instil a certain confidence. But, despite the best of intentions, it was unable to protect itself against a greedy attack from an inside job carried out by a dishonest employee. This demonstrates an obvious truth: the human element (and everything it involves) remains a vital part of businesses dealing with electronic payments.

In June 2016, a founder of the Slock.it company, following a recursive call bug discovery in the implementation of its Decentralized Autonomous Organization model on the Ethereum block chain, emphasised: "this is NOT an issue that is putting any DAO funds at risk today."[4] They were at risk six days later, when a recursive call bug was exploited to drain from them more than 3.6 million ethers, roughly US$50 million at the time. There would have been much said about the suitability of the use of an object oriented programming language to write self-enforcing electronic contracts if it was not irrelevant to Bitcoin, safe by design to this category of attacks. This example remains interesting because it demonstrates the contrast between a hubristic statement in

1 http://blog.bitcoin-traveler.com/
2 https://gemini.com/blog/your-bitcoin-wallet-may-be-at-risk-safenet-hsm-key-extraction-vulnerability/
3 https://news.bitcoin.com/looting-fox-sabotage-shapeshift/
4 https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b

this field and the harsh reality. We believe that, to a minor extent, the unwillingness to insure shares a similar hubristic nature.

Because safety measures cannot prevent thefts from the outside or the inside, because human rationality is inherently bounded, it is unfortunate that the Trust's bitcoin are not insured.

4. Vague Signing Requirements

According to the proposed rule change, "the Custodian's Cold Storage System utilizes multiple-signature ('Multisig') technology with an 'M-of-N' signing design that requires a signature from more than one (1) Signer (but fewer than the full complement of potential Signers) in order to move the Trust's bitcoin." In other words:

M = number of required Signers
N = number of potential Signers

$$1 < M < N$$

A M-of-N signing design alleviates the risk of an inside attack as long as M and N are well thought out. For example, if $M = 1$, the multisig in such a context is poorly designed because any signer can spend the funds. If $M > 1$ but $M \ll N$, e.g. 2-of-10, there is room left for a possible collusion between M conspirators. A conspirator is more likely to find M-1 conspirators if N is greatly superior to M. One should not underestimate the power of greed to gather people segregated by a multisig. We believe the proposed rule change fails to provide a meaningful description of the security level of the storage system multisig. It merely defines what a multisig is, in general, while only excluding the extreme cases $M = 1$, insecure, and $M = N$, unpractical. The present signing design is complicated by the fact that the Signers, hardware devices, are activated by Signatories, human beings. If p Signatories can activate M Signers and $p < M$, the signing design is in fact weakened to p-of-N.

The given definition is then far too abstract and incomplete. Because the whole signing design is critical to the safety of the funds, the Trust should communicate the following elements to the interested third parties such as the Commission or, as the case should be, the Trust's insurer:

1) Exact number of required Signers.
2) Exact number of potential Signers.
3) A detailed explanation of why the chosen M-of-N configuration is adequate.
4) A complete list of the Signatories and what Signer(s) they can activate.
5) Useful information related to the Signatories' keys (expiration date, attributes...).

Moreover the Trust should notify without delay to the relevant persons any modification of any of the above elements. 1) to 3) should be publicly announced. For security reasons, 4) and 5) should be notified to the interested third parties only.

5. Concluding Remarks

First, we fully support the concept of a Bitcoin Exchange-Traded Fund. Second, we think the Custodian currently demonstrates it has the technical capabilities to securely hold the Trust's bitcoin. Third, we don't support the fact that the Trust's bitcoin are not insured. Fourth, we recommend amending the proposed rule in order to unambiguously specify the M-of-N signing design used to secure the Custodian's Cold Storage System and to require the Trust to notify any modification of the multisig characteristics in the future.

Sincerely,
Guillaume Lethuillier