October 25, 2023

Secretary
Securities and Exchange Commission 100 F Street, NE
Washington, DC 20549-1090

Re: iShares Bitcoin Trust, SR-NASDAQ-2023-016

Dear Secretary:

Upon reading the Form S-1 Registration Statement submitted by iShares for the iShares Bitcoin Trust, I discovered what I believe to be factual mistakes in the filing that likely have a material effect on the validity of the application as well as the risks associated with the fund. I would like to comment on a small portion of these findings.

In the prospectus, paragraph one, the application mentions that Coinbase Custody Trust Company, LLC will be the "Bitcoin Custodian." However, I believe this claim is factually inaccurate and instead should state that Coinbase will be the pass-through custodian. The reason for this is because Coinbase will not have direct possession of the underlying token balance. Instead they will hold keys that can be used to sign transaction requests submitted to the true custodian which is the Bitcoin Network. As I understand it, the Bitcoin Network maintains the ledger of accounts for all bitcoin addresses via nodes who host the database and maintain it by updating account balances and synchronizing amongst other participants of this loose organization. These nodes work together with "miners" to append transactions to this ledger. The network by design does not allow the transfer of tokens to other ledgers including ledgers owned and operated by Coinbase. Because Coinbase will not have direct possession of the underlying balance, they will always rely on the cooperation of the operators of the Bitcoin Network, the true Bitcoin custodian,to manage their tokens. Any bitcoin ledgers maintained by Coinbase would thus represent pass-through claims on tokens held in Coinbase's account with the Bitcoin Network. In ledger based digital accounting, the transfer of a balance from one custodian to another requires the quantity transferred to be subtracted from the balance held with the source custodian and added to the balance held with the destination custodian. For example, if a person transfers their entire bank account from bank A to bank B, bank A subtracts the full balance to zero out the account at bank A while Bank B adds the exact balance quantity to the account held there. The transfer is settled when this process is finalized and both banks A and B agree on the final state of their ledgers. At this point, bank A has zero involvement in any further transactions performed in regards to the funds held in the account at bank B.   This process represents a true transfer of custodianship from Bank A to Bank B. In a pass-through arrangement, the balance is never subtracted from the true custodian. Instead, the ledger held by the pass-through custodian simply represents a pass-through reference to the account balance held by the true custodian. Coinbase never performs a balance transfer to remove their tokens from the Bitcoin Network and thus they represent a pass-through custodian and not a true custodian of the bitcoin. They only hold keys which are authorization devices used to submit signed, valid requests to the true custodian.

Further proof that Coinbase is not a true custodian is made evident by transaction fees. In order for Coinbase to transfer a balance off of their ledger, they must pay a transaction fee to the Bitcoin Network. Why is this the requirement if Coinbase is the base custodian? This is to say Coinbase's ability to to transfer a balance externally is dependent on the cooperation of a third party. If Coinbase were a true custodian then they should be free of all dependencies connected to the prior custodian. The reason why proper disclosure of custodianship is important is because it is indicative of the ability to both authorize and execute transactions. It implies the custodian has a high level or control over the assets they hold. This enables a custodian to transact at will with no counterparty imposed restrictions. Coinbase does not have this ability. At best they can authorize a transaction by submitting a signed transaction request to the Bitcoin Network, but it is up to the Bitcoin Network to decide whether that transaction will actually be processed into an update to their blockchain ledger. Coinbase does not have direct write access to the blockchain ledger. Most of the time the Bitcoin Network selects pending transactions based on the highest fee, but their choice can be arbitrary. They also reserve the choice to ignore requests from certain accounts or set a minimum fee to an arbitrary number. Coinbase cannot guarantee that their transaction requests will be executed which is consistent with a pass-through custodian's ability to submit requests to the true custodion, but the true custodian is ultimately responsible for executing those requests.

The lack of accurate disclosure of the true custodian means the iShares registration statement does not properly disclose the numerous risks introduced by using the Bitcoin Network as a custodian. This organization is not a traditional corporation. It is loosely comprised of participants who join by their own free choice. Many of these participants are anonymous. Many are located internationally with some being in heavily sanctioned countries. The network does not restrict participation whatsoever. The only criteria is that a participant must run the node and/or 'mining' software and perform the duties associated with the respective roles including mainting a high degree of synchronization amongst themselves. This structure leads to a complete lack of accountability and compliance with the law, not only because laws differ by juristiction of the participants, but any software updates that may be required to bring the network's operations into compliance will likely be extremely difficult to implement due to the vast differences in demographics and interests of the participants. There is no single person in a leadership position that can make executive decisions. In fact, many features that are consistent with financial industry best practices such as two factor authentication and robust record keeping practices have been seemingly willfully omitted from the software. The Bitcoin Network organization will process any transaction of any amount from any account/"wallet" to any other with an absolute bare minimum of information. The network only requires a transaction request that contains pseudononymous information like token quantity, recipient's account number (wallet address), and a proper signature by the source account's private key. This "swiss numbered bank account" style of accounting has attracted a significant amount of criminal activity and by some accounts is likely already illegal. One very common exploit account owners face is an attacker who compromises a victims keys and uses them to transfer the victim's balance to the attacker's account. These types of attacks are made possible because the network does not screen for suspicous activity or require any verification of identity besides the usage of the key. There is no method to verify proof of ownership, proof of identity, or proof of anything. Further, many attackers have publicly know addresses associated with criminal activity. Some of these addresses are even listed in the Treasury's OFAC SDN list. Despite this open information, the network will still continue to keep these individuals' accounts open as it sends funds to accounts/wallets linked to known criminals. The network does not deny accounts for anybody primarily because the network does not even check the identities of people who open accounts. The end user client software even lets individuals create their own account/wallet numbers that the network will simply honor as long as the keys and signatures can be validated.

Another consequence of the complete lack of accountability of network operators is the inability or extreme difficulty in enforcing property rights. Suppose a user owns a bitcoin token balance but they lose their key. In traditional finance the bank/custodian will offer a password recovery process or they will re-issue a new debit card key. Even if a user can prove via thorough documentation they are the lawful owner of a bitcoin balance held on account with the Bitcoin Network, the functionality to perform such a recovery is not present in the software and there is no official point of contact for a user to go to for support. There is no function to recover keys, and there is no function to deactiviate the old account while populating the new account with a new balance equal to the old balance. Even if a court issues a lawful order for custodians to return assets to the lawful owner, the network is unlikely to comply. These practices go against even the most basic best practices in account and ledger management of assets. Rather than pursue a traditional recovery of assets from a custodian in these types of situations, most bitcoin users who fall victim to lost keys or stolen key attacks go through great lengths to try to recover their keys or plead with attackers to authorize the Bitcoin Network to process a transaction to return the funds. Even when law enformcement is involved, rather than issueing a court order to force the custodian to transfer funds, they will pursue the attacker and use the attacker's keys to submit a transaction request to the network to send the funds to a bitcoin account/wallet owned by law enforcement. Meanwhile all accounts are held on the blockchain ledger that is actively managed by real people who perform critical functions as they run the software, host the database of accounts, and send and receive information as part of their duties to operat the system. Should Coinbase lose their keys or become victim of a key theft operation, the network will likely not provide them with any recourse or honor their property rights to the account balance. The network could potentially transfer billions worth of tokens under management to an attacker without secondary checks. This type of risk is not present in any traditional accounts like bank accounts. Banks take serious precautions to safeguard assets and ensure transfers are legitimate while the operators of the Bitcoin Network do the exact opposite.

Even users of the network do not have choice when it comes to selecting which particular sub-operators they will utilize for account services. This is relevant because the network is global and some service providers can be located in sanctioned countries such as North Korea. For instance, when Coinbase submits a request to transfer tokens, that request will first enter the mempool of pending transactions. A "miner" located in North Korea may wind up being the payment processor who accepts the transaction fee in exchange for validating and executing the transaction. Clearly it may be illegal for Coinbase to utilize such a service based out of North Korea, but the network software does not enable users like Coinbase to choose which participants of the organization they can and cannot use to process transactions. Prior to any kind of approval involving the Bitcoin Network as the underlying host of the fund's account, control measures should be put in place to ensure the pass-through custodian of the funds, Coinbase, does not serrendipidously engage in illegal activity through the course of normal business activity pertaining to fund management. Control measures should be put in place to ensure the base Bitcoin Network and its operators, both domestic and foreign, perform their duties in a lawful and compliant manner.

Another very important problem with the registration statement is in regards to the risk events that are disclosed. The Bitcoin Network association lacks an executive team. It lacks official statements in regards to the defining characteristics of what a Bitcoin even is. There are no official promises to uphold the current properties of the token system. However when a typical investor or layperson thinks of Bitcoin, they think of it as being defined by a handful of very specific key properties that many consider to be characteristic attributes that are 100% unique to Bitcoin and only Bitcoin. The collection of all these attributes separate Bitcoin from the other arbitrary cryptocurrency token systems that are possible. They form a unique signature of what Bitcoin is. Investors believe these characteristics will never change and will always be engrained as the fundamental definition of a bitcoin. One such property is the fact that the current embodiment of the software will restrict the total token supply to 21 million tokens. Another such property is that the work performed by miners will involve computational processing of a hash function as the basis for proof of work. Another such property is the belief that the network operators will never decide to blacklist/censor an account/wallet based on the account number, in other words that the system is censorship resistant. Most of the applicant's outlined risks indicate that changes to any of these key parameters may negatively impact the token price or functionality and value of the network. On page 25 of the application,it states "there is no guarantee that the current 21 million supply cap for outstanding bitcoin ... will not be changed." Further it is stated: "If a hard fork changing the 21 million supply cap is widely adopted, the limit on the supply of bitcoin could be lifted, which could have an adverse impact on the value of bitcoin and the value of the Shares." The primary problem with these high magnitude risk events is that they will fundamentally change the definition of the asset under management. If the network ever decides to raise the coin cap to 22 million tokens, is it accurate for iShares Bitcoin Trust to claim they continue to hold hold bitcoin when everybody knowns one of the key defining properties is that there will only ever be 21 million bitcoin? It is not that the supply cap can be lifted, it is that bitcoin can be superceded by a similar but alternative asset. How can truthful claims be made about the properties of bitcoin today when the properties can change at any time in the future as explained in the risk disclosures? The token does not represent an underlying asset, the token itself is the asset so the properties of the token balances and token system are absolutely critical because these properties are what drive investor interest based on the definitions and featureset of bitcoin. These are the attributes that investors trust. The practical consequence is that professional investment advisors will likely make claims based on todays properties that will become falsified in the future should a risk event occur. If this happens, what are investors to do because in hindsight they were lied to? Imagine an ETF tied to corn that discloses the possibility that the corn could suddenly transform into soybeans. Or imagine a gold ETF whos asset could suddenly change it's properties into those of copper. Changing the token cap of Bitcoin from 21 million to any other value would be exactly this type of sudden redefinition of the asset under management. Can a fund based on such an asset be the basis for a serious investment vehicle that can meet investor expectations and is resistant to manipulation? What types of factual claims can a professional asset manager make when explaining an asset like this to clients? Imagine a metal analogy as follows: "Today the fund holds 100 tons of gold, tomorrow it might transform into copper, then in five years there's a chance it becomes lead. The good news is two years ago the properties matched silver so a lot of value was added when it became gold." The inability to guarantee consistency is a huge problem.

Having the Bitcoin Network serve as the true custodian of the iShares Bitcoin Trust's tokens will completely undermine the safety and security investors have come to expect for securities traded in reputable markets. Fundamentally, the complete lack of knowledge of who the operators of the bitcoin network are means that it is impossible to implement sufficient control measures to ensure a fair market that is free from manipulation of both token trades, actions of the operators, or even the fundamental properties of the asset itself. The risk events that can happen are too complicated for a typical investor to fully understand because they are exclusive to cryptocurrency token systems and are unlike the types of events investors have familiarity with when they invest in other securities. The claims of any ETF salesman can be falsified on the whim of a network of strangers if they agree to deploy a routine software update.

For all of these reasons and many, many more, the comission should clearly reject the iShares Bitcoin Trust registration.

Sincerely,

Brandon B