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

Re: File Number SR-NASDAQ-2023-016

October 27, 2023

Dear Secretary,

I'm writing to highlight some medium-term concerns with Bitcoin's security model that are sometimes not given the attention they deserve or are not thoroughly addressed. The associated risks could be quite serious for investors and should be more thoroughly disclosed.

Summary: As the block reward declines, miners will face an increasingly competitive market with exponentially decreasing returns. This will create strong economic incentives for consolidation and collusion among mining firms. Once this consolidation occurs, it becomes possible that a single entity (possibly foreign) or cartel could have full control over the transaction ledger, in accordance with the Bitcoin rules. Two clear risks (among others) emerge:

1. Any trusts or custodians who hold large quantites of bitcoin put themselves directly at risk of extortion by the controlling entity.
2. The "Goldfinger attack," which is characterized by an attacker intentionally harming the network while also engaging in short selling of the asset or its derivatives, may become both profitable and attainable.

Block subsidy concerns. It is well known that the Bitcoin block reward is cut in half every four years. In the span of 20 years, the block reward is cut by 96.8%, while in 40 years, this represents a 99.9% reduction in new Bitcoin issued to miners.

Bitcoin advocates have largely taken a wait-and-see approach, claiming that we do not have a crystal ball to look into the future and tell us if this will be a problem. We can however, say some things with certainty. First, there is no reasonable possibility that the real value of bitcoin will double ever four years. Second, it is exceeding optimistic to suggest that fees will not only rise significantly but remain sustainably high: This would require wealthy entities to repeatedly choose to pay high fees. Among publicly recognizable institutions who are unlikely to engage in double-spending, there are efficient ways to settle large amounts of bitcoin off-chain, for example, multi-sig arrangements allow for an unlimited number of transactions to be kept in books off the blockchain. It defies human ingenuity to suggest institutions will continue to pay out billions of dollars to keep entries in a ledger.

Miner profitability concerns. In recent years, the total block rewards to miners have been somewhere around $8-10 billion per year. It would stand to reason that miner expenses have approached that from below. As future halvings occur, the price may increase sharply, spurring more investment by miners, or it may increase moderately, or it may not increase at all. Eventually there will be a time where the pie of rewards begins to shrink, leaving many mining firms unable to make a profit. Naturally, the profitable operations may be led to acquire resources (for example, ASICs and other infrastructure) of the unprofitable ones at a discount, putting more potential hashrate at their disposal. One expects the surviving miners' profitability margins to remain thin.

Coalitional game theory and the market fragility dilemma. Miners with dwindling profits and surplus hashpower will face a choice: If miners representing 51% or more of the hashpower choose to collude, they can agree to reduce hashrate produced, massively reducing operating expenses. If the size of the pie remains fixed, this move is a no-brainer; miners can agree to split the pie while ratcheting down their expenditures, leading to very large profit margins.

The question they have to wrestle with is the problem of market fragility. The market fragility hypothesis is the belief that an act of collusion by miners will cause market participants to no longer value Bitcoin, negatively affecting the price and miner rewards. This hypothesis held in 2013, but its validity today and into the future is very much unclear. However, given any likelihood one gives this assumption, miners should be able to either 1) profit by engaging in actions leading to this sell-off (for example by shorting the ETF), or 2) increase profits by collecting the rewards from collusive or monopolistic mining at lower costs. Miners may even be able to do both.

The math is straightforward. If profit margins are low while the market cap is high, miners have lucrative alternatives to mindlessly fighting one other: colluding to bring down the price, colluding to bring down their own costs, or both. While industry norms may serve as guardrails for some time, note that even threatening to collude, or leaking rumors of collusion could be sufficient to bring down the price if the market is sensitive to collusion. These same threats can also ward off competitive challenges by new miners.

If miners choose to collude for the purpose of reducing costs in a robust fee market, note that they gain another advantage: They may now set their own fees. When miners are competing with one another, they typically take any fees above a certain threshold and have no mechanisms for demanding higher fees. However, a cartel of miners could negotiate directly with large corporations who require blockspace, refusing to include any transaction without the requested fee. (I am not an anti-trust lawyer; what I'm describing may or may not be legal. However, it may occur outside our jurisdiction.)

Security phase shift. As Bitcoin gains more appeal as a commodity to broad financial markets, moving away from the its original stated purpose as a "peer-to-peer electronic cash system," the market fragility hypothesis becomes less likely. At the same time, block subsidies continue to decrease. Further, the production of ASICs has accelerated, leading to a situation where much of the machinery may one day become non-profitable to use in an ultra-competitive mining environment. These three factors suggest that within the next 10-15 years, bitcoin mining could undergo a phase shift: From an era of competitive mining to anti-competitive mining.

In the early days, anti-competitive mining would have doomed Bitcoin as a failed project, killing the goose. As long as the value of Bitcoin was surging upward, miners had no interest in jeopardizing their profit margins with anti-competitive behavior. But in an era where Bitcoin ETFs are traded on NASDAQ, all such bets are off.

As the value of Bitcoin has grown, the lack of past security issues has become conflated with future security assurances. This is not sound reasoning, as the economic landscape underlying the security model changes with time. As the author of *Bitcoin: A Game-theoretic analysis* (published by De Gruyter earlier this year), this is something I have explored in depth and feel requires deeper attention than is commonly given.

Sincerely

Micah Warren,
Associate Professor of Mathematics
University of Oregon
Eugene, OR, 97401