

---

---

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549**

---

**FORM 8-K**

---

**CURRENT REPORT  
Pursuant to Section 13 or 15(d)  
of the Securities Exchange Act of 1934**

**Date of Report (Date of earliest event reported): June 20, 2024**

---

**Grayscale Ethereum Trust (ETH)**  
(Exact name of Registrant as Specified in Its Charter)

**Delaware**  
(State or Other Jurisdiction  
of Incorporation)

**000-56193**  
(Commission  
File Number)

**82-6677805**  
(IRS Employer  
Identification No.)

**c/o Grayscale Investments, LLC**  
**290 Harbor Drive, 4th Floor**  
**Stamford, Connecticut**  
(Address of Principal Executive Offices)

**06902**  
(Zip Code)

**Registrant's Telephone Number, Including Area Code: 212 668-1427**

**N/A**  
(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

**Securities registered pursuant to Section 12(g) of the Act:**

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Grayscale Ethereum Trust (ETH) Shares	ETHE	N/A

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§ 230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§ 240.12b-2 of this chapter).

Emerging growth company

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

---

---

**Item 8.01. Other Events.**

Grayscale Investments, LLC, the sponsor (the “Sponsor”) of Grayscale Ethereum Trust (ETH) (the “Trust”), is filing information for the purpose of supplementing and updating the disclosures contained in the Trust’s Annual Report on Form 10-K for the year ended December 31, 2023 (the “Annual Report”), including those under the headings “Item 1. Business” and “Item 1A. Risk Factors.”

The supplemental disclosures are set forth in Exhibit 99.1, which is incorporated herein by reference.

**Item 9.01. Financial Statements and Exhibits.**

(d) Exhibits

<u>Exhibit No.</u>	<u>Description</u>
99.1	<a href="#">Supplemental Disclosures to the Trust’s Annual Report</a>
104	Cover Page Interactive Data File (the cover page XBRL tags are embedded within the inline XBRL document)

## SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned thereunto duly authorized.

Grayscale Investments, LLC as Sponsor of Grayscale  
Ethereum Trust (ETH)

Date: June 20, 2024

By: /s/ Edward McGee  
Edward McGee  
Chief Financial Officer

\* The Registrant is a trust and the identified person signing this report is signing in their capacity as an authorized officer of Grayscale Investments, LLC, the Sponsor of the Registrant.

## Supplemental Disclosures to the Trust’s Annual Report

*The following disclosure shall be newly added and incorporated by reference into the section titled “Item 1. Business” in the Annual Report and is inserted directly underneath the section titled “Item 1. Business—Activities of the Trust” in the Annual Report.*

### “Staking

Staking on the Ethereum Network refers to using Ether, or permitting Ether to be used, directly or indirectly, through an agent or otherwise, in the Ethereum Network’s proof-of-stake validation protocol, in exchange for the receipt of consideration, including, but not limited to, staking rewards paid in fiat currency or paid in kind (collectively, “Staking”). At this time, none of the Trust, the Sponsor, the Custodian, nor any other person associated with the Trust may, directly or indirectly, engage in Staking of the Trust’s Ether on behalf of the Trust, meaning no action will be taken pursuant to which any portion of the Trust’s Ether becomes used in Ethereum proof-of-stake validation or is used to earn additional Ether or generate income or other earnings, and there can be no assurance that the Trust, the Sponsor, the Custodian or any other person associated with the Trust will ever be permitted to engage in Staking of the Trust’s Ether or such income generating activity in the future.

To the extent (i) the Trust were to amend its Trust Agreement to permit Staking of the Trust’s Ether and (ii) NYSE Arca were to seek and obtain a rule change permitting the listing of a spot Ether investment vehicle engaged in Staking, in the future the Trust may seek to establish a program to use its Ether in the proof-of-stake validation mechanism of the Ethereum Network to receive rewards comprising additional Ether in respect of a portion of its Ether holdings. However, as long as such conditions and requirements have not been satisfied, the Trust will not use its Ether in the proof-of-stake validation mechanism of the Ethereum Network to receive rewards comprising additional Ether in respect of its Ether holdings. The current inability of the Trust to use its Ether in Staking and receive such rewards could place the Shares at a comparative disadvantage relative to an investment in Ether directly or through a vehicle that is not subject to such a prohibition, which could negatively affect the value of the Shares. See “Item 1A. Risk Factors—Risk Factors Related to the Trust and the Shares—The Trust is not permitted to engage in Staking, which could negatively affect the value of the Shares.””

*The following disclosure shall be newly added and incorporated by reference into the section titled “Item 1. Business—Overview of the ETH Industry and Market” in the Annual Report and is inserted directly underneath the section titled “Item 1. Business—Overview of the ETH Industry and Market—Summary of an ETH Transaction” in the Annual Report.*

### “Ether Markets

In addition to using Ether to engage in transactions, investors may purchase and sell Ether to speculate as to the value of Ether in the Ether market, or as a long-term investment to diversify their portfolio. The value of Ether within the market is determined, in part, by the supply of and demand for Ether in the global Ether market, market expectations for the adoption of Ether as a store of value, the number of merchants that accept Ether as a form of payment, and the volume of peer-to-peer transactions, among other factors.

Centralized spot Ether markets typically permit investors to open accounts with the trading platform and then purchase and sell Ether via websites or through mobile applications. Prices for trades on centralized spot Ether markets are typically reported publicly. An investor opening a trading account must deposit an accepted government-issued currency into their account with the spot market, or a previously acquired digital asset, before they can purchase or sell assets on the spot market. The process of establishing an account with a centralized Ether market and trading Ether is different from, and should not be confused with, the process of users sending Ether from one Ether address to another Ether address on the Ethereum Blockchain or decentralized on-chain trading platforms. This latter process is an activity that occurs on the Ethereum Network, while the former is an activity that occurs entirely within the order book operated by the centralized spot market. The centralized spot market typically records the investor’s ownership of Ether in its internal books and records, rather than on the Ethereum Blockchain. The centralized spot market ordinarily does not transfer Ether to the investor on the Ethereum Blockchain unless the investor makes a request to the Digital Asset Trading Platform to withdraw the Ether in their account to an off-exchange Ether wallet.

See “—Ether Value” below for a discussion of historical spot Ether prices on Digital Asset Trading Platforms and how such prices may differ from the Index Price.

Outside of the spot markets, Ether can be traded over-the-counter (“OTC”). The OTC market is largely institutional in nature, and OTC market participants generally consist of institutional entities, such as firms that offer two-sided liquidity for Ether, investment managers, proprietary trading firms, high-net-worth individuals that trade Ether on a proprietary basis, entities with sizable Ether holdings, and family offices. The OTC market provides a relatively flexible market in terms of quotes, price, quantity, and other factors, although it tends to involve large blocks of Ether. The OTC market has no formal structure and no open-outcry meeting place. Parties engaging in OTC transactions will agree upon a price—often via phone or email—and then one of the two parties will initiate the transaction. For example, a seller of Ether could initiate the transaction by sending the Ether to the buyer’s Ether address. The buyer would then wire U.S. dollars to the seller’s bank account. OTC trades are sometimes hedged and eventually settled with concomitant trades on Ether spot markets.

In addition, Ether futures and options trading occurs on exchanges in the U.S. regulated by the CFTC. The market for CFTC-regulated trading of Ether derivatives has developed substantially. As of June 17, 2024, regulated Ether futures represented approximately \$1.04 billion in notional trading volume on the Chicago Mercantile Exchange (“CME”). Ether futures on the CME traded around \$648 million per day in the one year ended June 17, 2024, and represented around \$684 million in open interest per day. Through the common membership of NYSE Arca and the CME Ethereum Futures market in the Intermarket Surveillance Group (“ISG”), NYSE Arca may obtain information regarding trading in the Shares and listed Ether derivatives from the CME Ethereum Futures market via the ISG and from other exchanges who are members or affiliates of the ISG. Such an arrangement with the ISG and the CME Ethereum Futures market allows for the surveillance of Ether futures market conditions and price movements on a real-time and ongoing basis in order to detect and prevent price distortions, including price distortions caused by manipulative efforts. The sharing of surveillance information between NYSE Arca and the CME Ethereum Futures market regarding market trading activity, clearing activity and customer identity assists in detecting, investigating and deterring fraudulent and manipulative misconduct, as well as violations of NYSE Arca’s rules and the applicable federal securities laws and rules. NYSE Arca has also implemented surveillance procedures to monitor the trading of the Shares on NYSE Arca during all trading sessions and to deter and detect violations of NYSE Arca rules and the applicable federal securities laws.”

***The following disclosure shall be incorporated by reference into, and replaces, the section titled “Item 1. Business—Overview of the ETH Industry and Market—ETH Value—The Index and the Index Price—Determination of the Index Price When the Index Price is Unavailable,” in the Annual Report (with ~~strike-through~~ representing deletions and double underlining representing additions, where applicable):***

*“Determination of the Index Price When Index Price is Unavailable*

On January 11, 2022, the Sponsor changed the cascading set of rules used to determine the Index Price. The Sponsor uses the following cascading set of rules to calculate the Index Price. For the avoidance of doubt, the Sponsor will employ the below rules sequentially and in the order as presented below, should one or more specific rule(s) fail:

1. Index Price = The price set by the Index as of 4:00 p.m., New York time, on the valuation date. If the Index becomes unavailable, or if the Sponsor determines in good faith that the Index does not reflect an accurate price, then the Sponsor will, on a best efforts basis, contact the Index Provider to obtain the Index Price directly from the Index Provider. If after such contact the Index remains unavailable or the Sponsor continues to believe in good faith that the Index does not reflect an accurate price, then the Sponsor will employ the next rule to determine the Index Price. There are no predefined criteria to make a good faith assessment and it will be made by the Sponsor in its sole discretion.
2. Index Price = The price set by Coin Metrics Real-Time Rate (the “Secondary Index”) as of 4:00 p.m., New York time, on the valuation date (the “Secondary Index Price”). The Secondary Index Price is a real-time reference rate price, calculated using trade data from constituent markets selected by Coin Metrics Inc. (the “Secondary Index Provider”). The Secondary Index Price is calculated by applying weighted-median techniques to such trade data where half the weight is derived from the trading volume on each constituent market and half is derived from inverse price variance, where a constituent market with high price variance as a result of outliers or market anomalies compared to other constituent markets is assigned a smaller weight. The Secondary Index Provider and the Sponsor have entered into the master services agreement, dated as of August 4, 2020, and order forms thereunder, pursuant to which the Sponsor may obtain and use the Secondary Index and the Secondary Index Price from the Secondary Index Provider. If the Secondary Index becomes unavailable, or if the Sponsor determines in good faith that the Secondary Index does not reflect an accurate price, then the Sponsor will, on a best efforts basis, contact the Secondary Index Provider to obtain the Secondary Index Price directly from the Secondary Index Provider. If after such contact the Secondary Index remains unavailable or the Sponsor continues to believe in good faith that the Secondary Index does not reflect an accurate price, then the Sponsor will employ the next rule to determine the Index Price. There are no predefined criteria to make a good faith assessment and it will be made by the Sponsor in its sole discretion.

3. Index Price = The price set by the Trust's principal market (the "Tertiary Pricing Option") as of 4:00 p.m., New York time, on the valuation date. The Tertiary Pricing Option is a spot price derived from the principal market's public data feed that is believed to be consistently publishing pricing information as of 4:00 p.m., New York time, and is provided to the Sponsor via an application programming interface. If the Tertiary Pricing Option becomes unavailable, or if the Sponsor determines in good faith that the Tertiary Pricing Option does not reflect an accurate price, then the Sponsor will, on a best efforts basis, contact the Tertiary Pricing Provider to obtain the Tertiary Pricing Option directly from the Tertiary Pricing Provider. If after such contact the Tertiary Pricing Option remains unavailable after such contact or the Sponsor continues to believe in good faith that the Tertiary Pricing Option does not reflect an accurate price, then the Sponsor will employ the next rule to determine the Index Price. There are no predefined criteria to make a good faith assessment and it will be made by the Sponsor in its sole discretion.
4. Index Price = The Sponsor will use its best judgment to determine a good faith estimate of the Index Price. There are no predefined criteria to make a good faith assessment and it will be made by the Sponsor in its sole discretion.

In the event of a fork, the Index Provider may calculate the Index Price based on a digital asset that the Sponsor does not believe to be the appropriate asset that is held by the Trust. In this event, the Sponsor has full discretion to use a different index provider or calculate the Index Price itself using its best judgment.

The Sponsor may, in its sole discretion, select a different index provider, select a different index price provided by the Index Provider, calculate the Index Price by using the cascading set of rules set forth above, or change the cascading set of rules set forth above at any time. The Sponsor will provide notice of any such changes in the Trust's periodic or current reports and, if the Sponsor makes such a change other than on an ad hoc or temporary basis, will file a proposed rule change with the SEC.

*The following disclosure shall be incorporated by reference into, and replaces, the section titled "Item 1. Business—Overview of the ETH Industry and Market—Government Oversight" in the Annual Report (with ~~strike-through~~ representing deletions and double underlining representing additions, where applicable):*

#### **"Government Oversight**

As digital assets have grown in both popularity and market size, the U.S. Congress and a number of U.S. federal and state agencies (including FinCEN, SEC, CFTC, the Financial Industry Regulatory Authority ("FINRA"), the Consumer Financial Protection Bureau ("CFPB"), the Department of Justice, the Department of Homeland Security, the Federal Bureau of Investigation, the IRS, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve and state financial institution and securities regulators) have been examining the operations of digital asset networks, digital asset users and the Digital Asset Markets, with particular focus on the extent to which digital assets can be used to launder the proceeds of illegal activities or fund criminal or terrorist enterprises and the safety and soundness of trading platforms ~~or~~and other service providers that hold or custody digital assets for users. Many of these state and federal agencies have issued consumer advisories regarding the risks posed by digital assets to investors. President Biden's March 9, 2022 Executive Order, asserting that technological advances and the rapid growth of the digital asset markets "necessitate an evaluation and alignment of the United States Government approach to digital assets," signals an ongoing focus on digital asset policy and regulation in the United States. A number of reports issued pursuant to the Executive Order have focused on various risks related to the digital asset ecosystem, and have recommended additional legislation and regulatory oversight. In addition, federal and state agencies, and other countries and international bodies have issued rules or guidance about the treatment of digital asset transactions or requirements for businesses engaged in digital asset activity. Moreover, the failure of FTX Trading Ltd. ("FTX") in November 2022 and the resulting market turmoil substantially increased regulatory scrutiny in the United States and globally and led to SEC and criminal investigations, enforcement actions and other regulatory activity across the digital asset ecosystem.

In addition, the SEC, U.S. state securities regulators and several foreign governments have issued warnings and instituted legal proceedings in which they argue that certain digital assets may be classified as securities and that both those digital assets and any related initial coin offerings or other primary and secondary market transactions are subject to securities regulations. For example, in June 2023, the SEC brought charges against Binance and Coinbase, and in November 2023, the SEC brought charges against Kraken, alleging that they operated unregistered securities exchanges, brokerages and clearing agencies. In its complaints, the SEC asserted that several digital assets are securities under the federal securities laws. The

outcomes of these proceedings, as well as ongoing and future regulatory actions, have had a material adverse effect on the digital asset industry as a whole and on the price of ~~ETH~~ **Ether**, and may alter, perhaps to a materially adverse extent, the nature of an investment in the Shares and/or the ability of the Trust to continue to operate. Additionally, U.S. state and federal, and foreign regulators and legislatures have taken action against virtual currency businesses or enacted restrictive regimes in response to adverse publicity arising from hacks, consumer harm, or criminal activity stemming from virtual currency activity.

**The CFTC has regulatory jurisdiction over the Ether futures markets. In addition, because the CFTC has determined that Ether is a non-security “commodity” under the CEA and the rules thereunder, it has jurisdiction to prosecute fraud and manipulation in the cash, or spot, market for Ether. Beyond instances of fraud or manipulation, the CFTC generally does not oversee cash or spot market exchanges, spot Digital Asset Trading Platforms or transactions involving spot Ether that do not utilize collateral, leverage, or financing. The National Futures Association (“NFA”) is the self-regulatory agency for the U.S. futures industry, and as such has jurisdiction over Ether futures. However, the NFA does not have regulatory oversight authority for the cash or spot market for Ether trading or transactions.**

**In February 2021, certain designated contract markets (“DCMs”) registered with the CFTC, including the CME, launched new contracts for Ether futures products. DCMs are boards of trades (commonly referred to as exchanges) that operate under the regulatory oversight of the CFTC, pursuant to Section 5 of the CEA. To obtain and maintain designation as a DCM, an exchange must comply on an initial and ongoing basis with twenty-three Core Principles established under Section 5(d) of the CEA. Among other things, DCMs are required to establish self-regulatory programs designed to enforce the DCM’s rules, prevent market manipulation and customer and market abuses, and ensure the recording and safe storage of trade information. The CFTC engaged in a “heightened review” of the self-certification of Ether futures, which required DCMs to enter direct or indirect information sharing agreements with spot market platforms to allow access to trade and trader data; monitor data from cash markets with respect to price settlements and other Ether prices more broadly, and identify anomalies and disproportionate moves in the cash markets compared to the futures markets; engage in inquiries, including at the trade settlement level when necessary; and agree to regular coordination with CFTC surveillance staff on trade activities, including providing the CFTC surveillance team with trade settlement data upon request.**

In August 2021, the chair of the SEC stated that he believed investors using digital asset trading platforms are not adequately protected, and that activities on the platforms can implicate the securities laws, commodities laws and banking laws, raising a number of issues related to protecting investors and consumers, guarding against illicit activity, and ensuring financial stability. The chair expressed a need for the SEC to have additional authorities to prevent transactions, products, and platforms from “falling between regulatory cracks,” as well as for more resources to protect investors in “this growing and volatile sector.” The chair called for federal legislation centering on digital asset trading, lending, and decentralized finance platforms, seeking “additional plenary authority” to write rules for digital asset trading and lending. **At the same time** **However**, the chair has **also** **subsequently** stated that the SEC **already** has **explicit** authority under existing laws to regulate the digital asset sector and several enforcement actions were filed against digital asset trading platforms during the first half of 2023.

The SEC has **also** **taken steps to interpret its existing authorities as covering various digital asset activities. For example, the SEC has** recently proposed amendments to the custody rules under Rule 406(4)-2 of the Investment Advisers Act. The proposed rule changes would amend the definition of a “qualified custodian” under Rule 206(4)-2(d)(6) and expand the current custody rule under Rule 406(4)-2 to cover digital assets and related advisory activities. If enacted as proposed, these rules would likely impose additional regulatory requirements with respect to the custody and storage of digital assets and could lead to additional regulatory oversight of the digital asset ecosystem more broadly. See “Item 1A. Risk Factors—Risk Factors Related to the Regulation of Digital Assets, the Trust and the Shares—Regulatory changes or actions by the U.S. Congress or any U.S. federal or state agencies may affect the value of the Shares or restrict the use of ETH, validating activity or the operation of the Ethereum Network or the Digital Asset Trading Platform Market in a manner that adversely affects the value of the Shares,” “Item 1A. Risk Factors—Risk Factors Related to the Regulation of Digital Assets, the Trust and the Shares—A determination that ETH or any other digital asset is a “security” may adversely affect the value of ETH and the value of the Shares, and result in potentially extraordinary, nonrecurring expenses to, or termination of, the Trust” and “Item 1A. Risk Factors—Risk Factors Related to the Regulation of Digital Assets, the Trust and the Shares—Changes in SEC policy could adversely impact the value of the Shares.”

Various foreign jurisdictions have, and may continue to, in the near future, adopt laws, regulations or directives that affect a digital asset network, the Digital Asset Markets, and their users, particularly Digital Asset Trading Platforms and service providers that fall within such jurisdictions' regulatory scope. For example:

- China has made transacting in cryptocurrencies illegal for Chinese citizens in mainland China, and additional restrictions may follow. China has banned initial coin offerings and there have been reports that Chinese regulators have taken action to shut down a number of China-based Digital Asset Trading Platforms.
- South Korea determined to amend its Financial Information Act in March 2020 to require virtual asset service providers to register and comply with its AML and counter-terrorism funding framework. These measures also provide the government with the authority to close Digital Asset Trading Platforms that do not comply with specified processes. South Korea has also banned initial coin offerings.
- The Reserve Bank of India in April 2018 banned the entities it regulates from providing services to any individuals or business entities dealing with or settling digital assets. In March 2020, this ban was overturned in the Indian Supreme Court, although the Reserve Bank of India is currently challenging this ruling.
- The United Kingdom's Financial Conduct Authority published final rules in October 2020 banning the sale of derivatives and exchange-traded notes that reference certain types of digital assets, contending that they are "ill-suited" to retail investors citing extreme volatility, valuation challenges and association with financial crime. A new law, the Financial Services and Markets Act 2023 ("FSMA"), received royal assent in June 2023. The FSMA brings digital asset activities within the scope of existing laws governing financial institutions, markets and assets.
- The Parliament of the European Union approved the text of the Markets in Crypto-Assets Regulation ("MiCA") in April 2023, establishing a regulatory framework for digital asset services across the European Union. MiCA is intended to serve as a comprehensive regulation of digital asset markets and imposes various obligations on digital asset issuers and service providers. The main aims of MiCA are industry regulation, consumer protection, prevention of market abuse and upholding the integrity of digital asset markets. MiCA was formally approved by the European Union's member states in 2023 **and is expected to come into effect in 2024. [Certain parts of MiCA became effective as of June 2024 and the remainder will start to apply as of December 2024.](#)**

There remains significant uncertainty regarding foreign governments' future actions with respect to the regulation of digital assets and Digital Asset Trading Platforms. Such laws, regulations or directives may conflict with those of the United States and may negatively impact the acceptance of [ETH Ether](#) by users, merchants and service providers outside the United States and may therefore impede the growth or sustainability of the Ethereum ecosystem in the United States and globally, or otherwise negatively affect the value of [ETH Ether](#) held by the Trust. The effect of any future regulatory change on the Trust or the [ETH Ether](#) held by the Trust is impossible to predict, but such change could be substantial and adverse to the Trust and the value of the Shares.

See "Item 1A. Risk Factors—Risk Factors Related to the Regulation of Digital Assets, the Trust and the Shares—Regulatory changes or actions by the U.S. Congress or any U.S. federal or state agencies may affect the value of the Shares or restrict the use of ETH, validating activity or the operation of the Ethereum Network or the Digital Asset Markets in a manner that adversely affects the value of the Shares."

***The following risk factors shall be newly added and incorporated by reference into the section titled "Item 1A. Risk Factors—Risk Factors Related to Digital Assets" in the Annual Report:***

***"Validators may suffer losses due to Staking, or Staking may prove unattractive to validators, which could adversely affect the Ethereum Network.***

Validation on the Ethereum Network requires Ether to be transferred into smart contracts on the underlying blockchain network not under the control of the person who owns such Ether. If the Ethereum Network source code or protocol were to fail to behave as expected, suffer cybersecurity attacks or hacks, experience security issues, or encounter other problems, such transferred (i.e., staked) Ether may be irretrievably lost. In addition, the Ethereum Network's underlying protocol dictates requirements for participation in validation activity, and may impose penalties, if the relevant activities are not performed correctly. The Ethereum Network imposes three types of sanctions for validator misbehavior or inactivity, which would result in a portion of staked Ether being destroyed or "burned": penalties, slashing and inactivity leaks.

A validator may face penalties if it fails to take certain actions, such as providing a timely attestation to a block proposed by another validator. Under this scenario, a validator's staked Ether could be burned in an amount equal to the reward to which it would have been entitled for successfully performing the actions.

A more severe sanction (i.e., "slashing") is imposed if a validator commits malicious acts related to the proposal or attestation of blocks with invalid transactions. Slashing can result in the validator having a portion of its staked Ether immediately confiscated, withdrawn, or burned by the Ethereum Network, resulting in losses to them. After this initial slashing, the validator is queued for forceful removal from the Ethereum Network's validator "pool," and more of the validator's stake is burned over a period of approximately 36 days (with the exact amount of Ether burned and time period determined by the protocol) regardless of whether the validator makes any further slashable errors, at which point the validator is automatically removed from the validator pool.

Staked Ether may also be burned through a process known as an "inactivity leak," which is triggered if the Ethereum protocol has gone too long without finalizing a new block. For a new block to be successfully added to the blockchain, validators that account for at least two-thirds of all staked Ether must agree on the validity of a proposed block. This means that if validators representing more than one-third of the total staked Ether are offline, no new blocks can be finalized. To prevent this, an inactivity leak causes the Ether staked by the inactive validators to gradually "bleed away" until these inactive validators represent less than one-third of the total stake, thereby allowing the remaining active validators to finalize proposed blocks. This provides a further incentive for validators to remain online and continue performing validation activities.

As well as sanctions, as part of the "activating" and "exiting" processes of Staking, staked Ether will be inaccessible for a variable period of time determined by a range of factors, including network congestion, resulting in potential inaccessibility during those periods. "Activation" is the funding of a validator to be included in the active set of validators, thereby allowing the validator to participate in the Ethereum Network's proof-of-stake consensus protocol. "Exit" is the request to exit from the active set of validators and no longer participate in the Ethereum Network's proof-of-stake consensus protocol. As part of these "activating" and "exiting" processes of Staking on the Ethereum Network, any staked Ether will be inaccessible for a period of time and will not earn any income during this period. However, depending on demand, un-staking can take between hours, days or weeks to complete.

If validators' staked Ether are slashed or otherwise subject to sanctions by the Ethereum Network, their assets may be confiscated, withdrawn, or burnt by the network, resulting in losses to the validator, or the users who provided the Ether to the validator to stake on their behalf. Any cybersecurity attacks, security issues, hacks, penalties, slashing events, or other problems could damage validators' willingness to participate in validation, discourage existing and future validators from serving as such, and adversely impact the Ethereum Network's adoption or the price of Ether. Any disruption of validation on the Ethereum Network could interfere with network operations and cause the Ethereum Network to be less attractive to users and application developers than competing blockchain networks, which could cause the price of Ether to decrease. In addition, the limited liquidity during the "activation" or "exiting" processes could dissuade potential validators from participating, which could interfere with network operations or security and cause the Ethereum Network to be less attractive to users and application developers than competing blockchain networks, which could cause the price of Ether to decrease.

There can be no guarantee that penalties, slashing or inactivity leaks and resulting losses will not deter validators from Staking. Any such deterrence would affect the Ethereum Network's ability to process transactions, thus making the Ethereum Network less attractive to potential users thereof and negatively affecting the value of the Shares.

***Liquid staking applications pose centralization concerns, and a single liquid staking application has reportedly controlled around or in excess of 33% of the total staked Ether on the Ethereum Network.***

Validators must deposit 32 Ether to activate a unique validator key pair that is used to sign block proposals and attestations on behalf of its stake (i.e., participate in the proof-of-stake consensus mechanism). For every 32 Ether deposit that is staked, a unique validator key pair is generated. This validator key pair is only used in validation processes (block proposal and attestation, and the staking associated therewith), and is separate from the public-private key pair generated in respect of the blockchain address on the Ethereum Network which is used to hold the Ether. An application built on the Ethereum Network, or a single node operator, can manage many validator key pairs. For example, Lido, an application that provides a so-called "liquid staking" solution that permits holders of Ether to deposit them with Lido, which stakes the Ether while issuing the holder a transferrable token, is reported by some sources to have or have had up to 275,000 validator key pairs (each representing 32 staked Ether) divided across over 30 node operators. At times, Lido has reportedly controlled around or in excess of 33% of the total staked Ether on the Ethereum Network. While it is widely believed that Lido has little incentive to attempt to interfere with transaction finality or block confirmations using its reported 33% stake, since doing so

would likely cause its entire stake to be slashed and thus lost (assuming good actors unaffiliated with Lido controlled the remainder), and also because Lido is believed to not control most of the third party node operators where its Ether is staked, and finally because the occurrence of such manipulation of the Ethereum Network's consensus process by Lido or any other actor would likely cause Ether to lose substantial value (which would hurt Lido economically), it nevertheless poses centralization concerns. If Lido, or a bad actor with a similar sized stake, were to attempt to interfere with transaction finality or block confirmations, it could negatively affect the use and adoption of the Ethereum Network, the value of Ether, and thus the value of the Shares."

*The following risk factor shall be incorporated by reference into, and replaces, the risk factor titled "Item 1A. Risk Factors—Risk Factors Related to Digital Assets—If a malicious actor or botnet obtains control of more than 50% of the validating power on the Ethereum Network, or otherwise obtains control over the Ethereum Network through its influence over core developers or otherwise, such actor or botnet could manipulate the Blockchain to adversely affect the value of the Shares or the ability of the Trust to operate," including all cross-references to such risk factor, in the Annual Report (with ~~strike-through~~ representing deletions and double underlining representing additions, where applicable):*

*"If a malicious actor or botnet obtains control of more than ~~50~~33% of the validating power on the Ethereum Network, or otherwise obtains control over the Ethereum Network through its influence over core developers or otherwise, such actor or botnet could manipulate the Blockchain to adversely affect the value of the Shares or the ability of the Trust to operate.*

All networked systems are vulnerable to various types of attacks. As with any computer network, the Ethereum Network could be attacked. For example, following the Merge and the switch to proof-of-stake validation, the Ethereum Network is currently vulnerable to several types of attacks, including:

- ">33% attack" where, if a malicious actor, validator, botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) or group of validators acting in concert were to gain control of more than 33% of the total staked Ether on the Ethereum Network, a malicious actor could temporarily impede or delay block confirmation or even cause a temporary fork in the blockchain. This is designed to be a temporary risk, as the Ethereum Network's inactivity leak would be expected to eventually penalize the attacker enough for the chain to finalize again (i.e., the honest majority would be expected to reclaim 2/3rd stake as the attacker's stake is penalized). Moreover, it is not believed that a 33% attack would allow a malicious actor to engage in double-spending or fraudulent block propagation. Even without 33% control, a malicious actor or botnet could create a flood of transactions in order to slow down the Ethereum Network.
- ">50% attack" where, if a malicious actor, validator, botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) or group of validators acting in concert were to gain control of more than 50% of the total staked Ether on the Ethereum Network, a malicious actor would be able to gain full control of the Ethereum Network and the ability to manipulate future transactions on the blockchain, including censoring transactions, double-spending and fraudulent block propagation, potentially for an extended period or even permanently. In theory, the minority non-attackers might reach social consensus to reject blocks proposed by the malicious majority attacker, reducing the attacker's ability to engage in malicious activity, but there can be no assurance this would happen or that non-attackers would be able to coordinate effectively. Although the malicious actor or botnet would not be able to generate new tokens or transactions using such control, it could "double-spend" its own tokens (i.e., spend the same tokens in more than one transaction) and prevent the confirmation of other users' transactions for so long as it maintained control (over 50%). To the extent that such malicious actor or botnet did not yield its control of the validating power on the Ethereum Network or the Ethereum community did not reject the fraudulent blocks as malicious, reversing any changes made to the Ethereum Blockchain may not be possible.
- ">66% attack" where, if a malicious actor, validator, botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) or group of validators acting in concert were to gain control of more than 66% of the total staked Ether on the Ethereum Network, a malicious actor could permanently and irreversibly manipulate the blockchain, including censorship, double-spending and fraudulent block propagation. The attacker could finalize their preferred chain without any consideration for the votes of other stakers and could also revert finalized blocks.

~~If a malicious actor or botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) obtains a majority of the validating power on the Ethereum Network, it may be able to alter the Ethereum Blockchain on which transactions in ETH rely by constructing fraudulent blocks or preventing~~

~~certain transactions from completing in a timely manner, or at all. The malicious actor or botnet could also control, exclude or modify the ordering of transactions. Although the malicious actor or botnet would not be able to generate new tokens or transactions using such control, it could “double-spend” its own tokens (i.e., spend the same tokens in more than one transaction) and prevent the confirmation of other users’ transactions for so long as it maintained control. To the extent that such malicious actor or botnet did not yield its control of the validating power on the Ethereum Network or the ETH community did not reject the fraudulent blocks as malicious, reversing any changes made to the Ethereum Blockchain may not be possible. Further, a malicious actor or botnet could create a flood of transactions in order to slow down the Ethereum Network.~~

For example, in August 2020, the Ethereum Classic Network, [a proof-of-work network](#), was the target of two double-spend attacks by an unknown actor or actors that gained more than 50% of the processing power of the Ethereum Classic Network. The attacks resulted in reorganizations of the Ethereum Classic Blockchain that allowed the attacker or attackers to reverse previously recorded transactions in excess of over \$5.0 million and \$1.0 million.

In addition, in May 2019, the Bitcoin Cash network, [a proof-of-work network](#), experienced a ~~51~~<sup>>50</sup>% attack when two large mining pools reversed a series of transactions in order to stop an unknown miner from taking advantage of a flaw in a recent Bitcoin Cash protocol upgrade. Although this particular attack was arguably benevolent, the fact that such coordinated activity was able to occur may negatively impact perceptions of the Bitcoin Cash network. Although the two attacks described above took place on proof-of-work-based networks, it is possible that a similar attack may occur on the Ethereum Network, which could negatively impact the value of [ETH Ether](#) and the value of the Shares.

Although there are no known reports of malicious control of the Ethereum Network, if groups of coordinating or connected [ETH Ether](#) holders that together have more than 50% of outstanding [ETH Ether](#) were to stake that [ETH Ether](#) and run validators, they could exert authority over the validation of [ETH Ether](#) transactions. This risk is heightened if over 50% of the validating power on the network falls within the jurisdiction of a single governmental authority and is significantly heightened if over 66% falls within such a jurisdiction. If network participants, including the core developers and the administrators of validating pools, do not act to ensure greater decentralization of [ETH Ether](#), the feasibility of a malicious actor obtaining control of the validating power on the Ethereum Network will increase, which may adversely affect the value of the Shares.

A malicious actor may also obtain control over the Ethereum Network through its influence over core developers by gaining direct control over a core developer or an otherwise influential programmer. ~~To the extent~~ The less that the [ETH Ethereum](#) ecosystem ~~does not~~ grows, the greater the possibility that a malicious actor may be able to maliciously influence the Ethereum Network in this manner ~~will remain heightened~~. Moreover, it is possible that a group of Ether holders that together control more than 50% of outstanding Ether are in fact part of the initial or current core developer group, or are otherwise influential members of the Ethereum community. To the extent that the initial or current core developer groups also control more than 50% of outstanding Ether, as some believe, the risk of this particular group of users causing the Ethereum Network to adopt updates to the core protocol that this particular group wants to be implemented will be even greater, and should this materialize, it may adversely affect the value of the Shares.

*The following risk factor shall be newly added and incorporated by reference into the section titled “Item 1A. Risk Factors—Risk Factors Related to the Trust and the Shares” in the Annual Report:*

*“The Trust is not permitted to engage in Staking, which could negatively affect the value of the Shares.*

At this time, none of the Trust, the Sponsor, the Custodian, nor any other person associated with the Trust may, directly or indirectly, engage in Staking of the Trust’s Ether on behalf of the Trust, meaning no action will be taken pursuant to which any portion of the Trust’s Ether becomes used in Ethereum proof-of-stake validation or is used to earn additional Ether or generate income or other earnings, and there can be no assurance that the Trust, the Sponsor, the Custodian or any other person associated with the Trust will ever be permitted to engage in Staking of the Trust’s Ether or such income generating activity in the future.

To the extent (i) the Trust were to amend its Trust Agreement to permit Staking of the Trust’s Ether and (ii) NYSE Arca were to seek and obtain a rule change permitting the listing of a spot Ether investment vehicle engaged in Staking, in the future the Trust may seek to establish a program to use its Ether in the proof-of-stake validation mechanism of the Ethereum Network to receive rewards comprising additional Ether in respect of a portion of its Ether holdings. However, as long as such conditions and requirements have not been satisfied, the Trust will not use its Ether in the proof-of-stake validation mechanism of the Ethereum Network to receive rewards comprising additional Ether in respect of its Ether holdings. The current inability of the Trust to use its Ether in Staking and receive such rewards could place the Shares at a comparative disadvantage relative to an investment in Ether directly or through a vehicle that is not subject to such a prohibition, which could negatively affect the value of the Shares.”

*Each of the following terms shall have the meaning set forth below and shall be incorporated by reference into, and supplement, the definitions in the “Glossary of Defined Terms” in the Annual Report:*

“**CME**”—The Chicago Mercantile Exchange.

“**DCM**”—A designated contract market, which is a board of trade (commonly referred to as an exchange) that operates under the regulatory oversight of the CFTC.

“**Ether**”—Ethereum tokens, which are a type of digital asset based on an open source cryptographic protocol existing on the Ethereum Network, comprising units that constitute the assets underlying the Trust’s Shares.

“**ISG**”—The Intermarket Surveillance Group.

“**Secondary Index**”—The Coin Metrics Real-Time Rate.

“**Secondary Index Price**”—The price set by Coin Metrics Real-Time Rate as of 4:00 p.m., New York time, on the valuation date. See “Business—Overview of the Ethereum Industry and Market—The Index and the Index Price—Determination of the Index Price When Index Price is Unavailable” for a description of how the Secondary Index Price is utilized when the Index Price is unavailable.

“**Secondary Index Provider**”—Coin Metrics Inc., a Delaware corporation that publishes the Secondary Index.

“**Staking**”—Using Ether, or permitting Ether to be used, directly or indirectly, through an agent or otherwise, in the Ethereum Network’s proof-of-stake validation protocol, in exchange for the receipt of consideration, including, but not limited to, staking rewards paid in fiat currency or paid in kind.