



Ernst & Young LLP
5 Times Square
New York, NY 10036

Tel: +1 212 773 3000
ey.com

Received
CFTC

2019 MAY 13 PM 12:21

Office of the
Secretary

Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre, 1155 21st Street, NW
Washington, DC 20581

8 May 2019

**Re: Request for Input on Crypto-Asset Mechanics and Markets
(Federal Register/Vol. 83, No. 241)**

Dear Mr. Kirkpatrick:

Ernst & Young LLP (EY US) is pleased to provide comments to the Commodity Futures Trading Commission on its Request for Input on ether and the Ethereum network. EY US is part of the global EY network, a global leader in assurance, tax, transaction and advisory services. The insights and services we deliver help build trust and confidence in the capital markets and in economies the world over. EY has developed a deep understanding of distributed ledger technology and the crypto-asset ecosystem to serve our clients that hold and transact in ether and/or are building solutions on the Ethereum network.

In this letter, we address two key differences between ether and bitcoin functionality and some accounting and auditing considerations related to both.

We appreciate the Commission's efforts to better understand the Ethereum network and encourage the Commission to continue to involve the cryptocurrency and developer community in its rulemaking process.

The establishment of LabCFTC along with the innovative and collaborative approach the Commission has taken on this subject is especially commendable. LabCFTC demonstrates that when regulators and industry participants work together, better questions can be answered. We look forward to continuing to collaborate with regulators to solve the complex issues facing the cryptocurrency industry and the greater FinTech ecosystem.

Functionality

Like bitcoin, ether functions as a cryptocurrency for enterprises to either hold as an investment or use as a medium of exchange. For brevity, we have assumed a basic understanding of how blockchain protocols, consensus algorithms, and public and private keys function.

Transactions in both ether and bitcoin are initiated by participants, validated by miners and recorded within their respective blockchains. Two key differences between ether and bitcoin relate to how balances are tracked on the network and whether logical commands can be processed on the network.

Tracking balances

The Bitcoin and Ethereum networks employ different means of tracking balances. When one user sends a coin to another user, protocols for both Bitcoin and Ethereum must account for the transactions and prevent the same cryptocurrency from being sent to another user. Bitcoin uses the unspent transaction output (UTXO) model to accomplish this, and Ethereum uses the account balance model.

A user who receives bitcoin receives an unspent transaction output, meaning that a user who "owns" bitcoin really controls access to the unspent transaction outputs that have been assigned to the public address of his or her wallet in previous transactions. When a user sends bitcoin, he or she uses transaction inputs that are transaction outputs from previous bitcoin transactions associated with that same public address. When the inputs used exceed the amount sent, the sender receives a new output equal to the difference that can be used in a future transaction. Inputs to a new transaction can only use unspent outputs from previous transactions, preventing the same bitcoin from being spent twice.

In contrast, the Ethereum blockchain tracks account balances for each address. When one party wants to send ether to another party, the transaction is assigned a number, known as an account nonce. Each transaction number in the account nonce sequence for an address can be committed to the network once, and only a transaction assigned the next nonce in the sequence can be committed to the blockchain.

As a result, a new transaction attempting to use a previously used nonce will not be processed because it is considered an invalid attempt to double spend by the network. The network also verifies that an account contains enough ether to spend the amount specified. After an ether transaction is executed, both users' accounts are updated to reflect the new balances.

Processing capabilities

Bitcoin transactions are validated by using a scripting language called "Script." Script provides only the computational power to validate and commit bitcoin transactions to the blockchain. The creator(s) of bitcoin limited its power to these functions because the main goal outlined in the Bitcoin whitepaper is to have bitcoin function as an electronic currency.¹

The Ethereum founders sought to process logical commands and therefore enable more complex computations on ether's blockchain.² Participants can insert logic into a special "data" field that can be included in transactions broadcast to the network. This logic can be committed to the blockchain, creating what is known as a "smart contract." Smart contracts can be self-executing or require a user on the network to invoke the logic of the smart contract by sending a transaction with the appropriate parameters to the smart contract's address.

¹ <https://bitcoin.org/bitcoin.pdf>

² <https://github.com/ethereum/wiki/wiki/White-Paper#bitcoin-as-a-state-transition-system>

Any type of data input can be included in an ether transaction's data field, and developers can use this capability to construct complex networks of interlocking contracts. The result resembles modern-day application infrastructure, but it is underpinned by a decentralized blockchain rather than a centralized database and ERP system.

Smart contracts can perform simple functions such as disbursing funds at a specified date to specified recipients and using funds deposited into the contract at the time it was written. They can also be used to handle more complicated transactions such as the processing of insurance claims. For example, if an insurance claim meets a set of criteria specified by the contract, the policy holder will automatically receive a disbursement. This could dramatically reduce costs for an insurance company and make the claims process simpler and faster for policyholders.

Smart contracts also create additional risks. In particular, poorly constructed smart contracts may not be executed by the Ethereum network as intended or may allow those attempting to do harm by exploiting a vulnerability in the smart contract to manipulate the expected outputs. EY and other service providers advise companies on the construction of effective, secure smart contracts prior to deployment.

Accounting under existing US GAAP

In the absence of standard setting that specifically addresses the accounting for cryptocurrencies, entities that invest in these assets must apply existing accounting standards. We believe that ether and bitcoin held by entities other than investment companies meet the definition of indefinite-lived intangible assets, and holders of ether and bitcoin must account for them at historical cost less impairment, applying the guidance in Accounting Standards Codification (ASC) 350, *Intangibles – Goodwill and Other*.

Investment companies in the scope of ASC 946, *Financial Services – Investment Companies*, should account for their investments in ether and bitcoin as "other investments" and should measure these investments initially at cost and subsequently at fair value through earnings. In determining the fair value of ether or bitcoin, an entity needs to identify its principal market. The market for ether or bitcoin with the greatest volume and level of activity to which an entity has access generally will be the entity's principal market. If the entity's principal market is an active market, the fair value of ether or bitcoin would be calculated as the quoted price for identical assets multiplied by the quantity held by the entity. This is referred to as a Level 1 fair value measurement.

Entities that receive crypto-assets in events known as hard forks (when a new cryptocurrency is created because a change in the software of an existing blockchain network is not adopted by all nodes) and airdrops (when additional crypto-assets are sent to holders of a cryptocurrency) will need to apply significant judgment to determine whether, when and how to recognize new crypto-assets they receive or have a right to receive. In these situations, a holder may receive access to new crypto-assets without his or her knowledge or permission and may need to take explicit action to obtain control. We note that the smart contract functionality of the Ethereum network has supported the development of many new crypto-assets by allowing them to be distributed to holders of other crypto-assets in airdrops.

We encourage the Commission to review EY's accounting analysis of cryptocurrencies in our Technical Line publication, *A holder's accounting for cryptocurrencies*.³ This publication provides an in-depth analysis of technical accounting questions about decentralized cryptocurrencies.

Auditing deposits

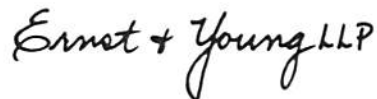
In a financial statement audit of direct holdings of ether and bitcoin, auditors typically test whether balances in the entity's books and records agree with balances on the public blockchain. Therefore, the blockchain data often represents an important source of audit evidence. Unlike audit evidence obtained from a trusted third party such as a bank, evidence is maintained by many participants (nodes) on the network. Auditors are required to assess the relevance and reliability of the evidence on which they rely. Assessing evidence from a blockchain requires a deep technical understanding of the underlying blockchain technology. Additional challenges may exist when ether or bitcoin is held in an account at a crypto exchange (rather than held directly by the entity) because exchanges may combine customer balances into pooled digital wallets, making it difficult to reconcile the entity's books and records directly to the blockchain.

To avoid using and relying on third-party block explorers such as Etherscan to obtain evidence from the blockchain, EY teams developed the EY Blockchain Analyzer to independently obtain transaction information from the blockchain.⁴ The Blockchain Analyzer is designed to enable audit teams to analyze the entire set of transactions associated with specified addresses and reconcile and identify transactions that are outliers in an efficient manner.

In addition to testing whether an address's transactions and balances agree with the underlying blockchain, auditors must perform additional procedures to test whether an entity controls the cryptocurrency associated with a public address. One way that an entity can demonstrate that it controls a public address is by authorizing a transaction for a specific amount.

We appreciate this opportunity for dialogue and would be pleased to discuss our comments with the Commission or its staff at your convenience.

Yours sincerely,



³ [http://www.ey.com/Publication/vwLUAssetsAL/TechnicalLine_04623-181US_Cryptocurrency_18October2018/\\$FILE/TechnicalLine_04623-181US_Cryptocurrency_18October2018.pdf](http://www.ey.com/Publication/vwLUAssetsAL/TechnicalLine_04623-181US_Cryptocurrency_18October2018/$FILE/TechnicalLine_04623-181US_Cryptocurrency_18October2018.pdf)

⁴ https://www.ey.com/en_gl/news/2018/04/ey-announces-blockchain-audit-technology