

Response to CFTC Request for Input on Crypto-asset Mechanics and Markets

February 15th, 2019

Dear Sirs,

I am contacting you in my capacity as Business Development Manager at Coinfirm in response to the CFTC (‘the Commission’) Request for Input (“RFI”) released on December 11th 2018 with the intention to collect public comment and feedback to support Commission’s work to gain a sound understanding of the technology, mechanics, and markets for Ethereum and its use on the Ethereum Network.

As recognized global RegTech provider for blockchain, Coinfirm serves as a foundation for the safe adoption and use of blockchain. The Coinfirm AML/CTF Platform uses proprietary algorithms and big data analysis to provide structured, actionable data that solves compliance and transaction risk issues in blockchain and cryptocurrencies. The blockchain agnostic platform is currently used by anyone ranging from major financial institutions to exchanges.

Given that a large portion of provided questions was already addressed by various market players, our intention in this response letter is to focus only on selected aspects. We would be interested, however, to have a wider discussion to help the Commission to identify Ethereum related inherent risks and propose and develop monitoring and risk mitigation tools and practices to ensure a smooth and regulatory compliant development of blockchain related investments and trading products.

We believe that the Commission’s efforts will help to drive the development of the blockchain related ecosystem in the right direction. In order to make this ecosystem safe and reliable, we think that disruptive RegTech and FinTech technology will play a major role in regulated markets and economies.

Coinfirm’s mission is to provide technology for regulatory compliance, bringing new levels of transparency and trust to the world of digital currencies. Our aim is to serve as a foundation for the safe adoption of blockchain by all actors in the economy, including traditional financial institutions, governments, regulators as well as ordinary citizens. We do that by applying blockchain technology to deliver solutions for various compliance challenges.

We embrace this opportunity to participate in the RFI. For further information, please contact me at: jt@coinfirm.com

Jacek Trzmiel
Business Development Manager

Our Response to CFTC Request for Input

21. What other factors could impact the Commission's ability to properly oversee or monitor trading in derivative

The Ethereum project is still in beta phase. Each technological change or update has a big impact on the value of underlying ETH cryptocurrency.

Each major event, whether a press release of new version roll-out, or an article, describing core developers discussions, has a correlation with the price. \

The major risk with ETH based derivatives is Illiquidity of the Ethereum underlying asset. Original purpose of ETH -- is to pay network fee. When an actor want to send a transaction, he has to pay network fee. The speculative side of ETH is a 'fiction', the market is thin, and price is fluctuating and it is almost impossible to control. But on the other hand the Ethereum serves as a public distributed infrastructure to build custom digital assets. So rather than introducing ETH derivative market, we/you/people should find out the way how to build a market with Ethereum based assets.

All assets (tokens) or data stored on public Ethereum mainnet, also is correlated with the ETH price. So if a new Ethereum based token will be introduced, with big value capacity, the value of ETH potentially will be changed.

Ethereum consensus model change (PoW --> PoC) is another risk. The proof of concept has never been tested in production environment (on mainnet), which can implicate the unknown behavior of the network, or new risks which were not foreseen;

Private transactions is a risk. There are few options how to create private transactions:

- zk-SNARK, stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge", would allow confidential transactions to occur across the Ethereum network;
The idea of zk-SNARKs is that they allow verification of the correctness of computations, without a verifier having to execute those computations, or even learn what was actually executed;
- State channels, is a private sequence of transactions which are used between closed party. After channel is closed, the batch transaction is sent to Ethereum public network to change the state, to represent data according to changes which occurred within the channel. It is possible to extrapolate private transactions from closed state channel, based on the state after channel is closed, but this operation is not always feasible;

-
- Parity private transactions;

22. Are there any emerging best practices for monitoring the Ethereum Network and public blockchains more broadly?

Coinfirm AML monitoring tools for Ethereum and all ERC20 tokens (as well as many other blockchain ledgers) are in the position to perform automated AML-assessments, both when onboarding clients and when monitoring transactions in real-time. Coinfirm provides AML-risk reports and actionable results within seconds. The risk assessment model allows to automatically decide which transfers on Ethereum and/or smart contracts can be deemed as low risk and which should be deemed as high risk.

Coinfirm can help the regulators to create safe, automated and data driven mechanisms to facilitate safe adoption of crypto and virtual currencies. We can do so by mitigating the risk associated with the adoption of cryptocurrencies in the broader economy. Our platform makes it possible to apply AML/CTF standard that is much higher than what can be achieved in the traditional economy.

Coinfirm's monitoring tools provide real-time monitoring of AML risk of ICO's smart contracts, cryptocurrency exchanges, wallets, payment processors as well as individual user private wallets. Coinfirm's panel is easily accessible through any browser.

By providing a smart contract, address user will be able to run fully automated AML risk assessment of contributors during on boarding, as well as at any point in time during ICO or on ongoing basis in day-to-day business activities. Based on unique scoring model user can decide which Ethereum / ERC20 transactions pose increased risk or are above certain thresholds.