COIN CENTER

Comments to the Commodity Futures Trading Commission on the Proposed Interpretation on Virtual Currency “Actual Delivery” in Retail Transactions

Peter Van Valkenburgh
March 19, 2018

Introduction

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing digital currency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.[1] We thank the Commission for taking great care in crafting guidance related to these exciting new technologies and welcome this opportunity to comment.

We will begin by offering a complete but non-technical summary of decentralized digital currency (cryptocurrency) technologies and the ecosystem of businesses that support and interact with these technologies. Terminology will reflect common industry parlance and will be described with specificity so that relevant aspects of the technology and the ecosystem can be mapped, carefully and without confusion, to legal structures and requirements under U.S. commodities law. We will then offer suggested clarifications and alterations to the draft guidance, primarily with regard to vocabulary and technical specificity, that we believe would improve it. Finally we will highlight a policy question that we believe the CFTC intends to answer in the draft guidance, but that under the current language is somewhat ambiguous.

Characterizing with Precision Digital Currencies and the Associated Ecosystem of Businesses

Digital currencies, like Bitcoin and Ether, are scarce items that may have utility and value as money, investments, tools for settlement, and/or fuel[2] for the provision of computational

[1] *See* Coin Center, *Our Work*, https://coincenter.org/our-work.
[2] There is a temptation to think of all decentralized tokens as money for making payments even if the network also allows for the provision of other computing resources. One could say, “The network may provide storage or it may provide computation and the user of the network uses the token to ‘pay’ for that good or service.” This, however, does not accurately illustrate the full achievement of these networks. As designed, a decentralized computing service should be entirely automated and provided by thousands or even millions of indifferent participants whose connected computers follow the rules of the

resources and services. Rather than *digital currencies*, they may be more accurately referred to as *digital commodities*. Digital currencies, like scarce commodities such as gold or salt, exhibit some of the classical characteristics of money (*e.g.* store of value, unit of account, and medium of exchange) but they may not exhibit all of these characteristics and may exhibit additional characteristics such as usefulness when employed in productive activity (*e.g.* ethereum is a necessary input to power and obtain decentralized computation just as oil is a necessary input to run internal combustion engines). The term *digital currency* has, however, become prevalent, so we will stick with it and refrain from using other terminology throughout this comment. Thanks to open blockchain technology, digital currencies can be sent person-to-person over the Internet with no intermediary required to broker or record the transfer, just as tangible commodities can be handed from one person to another in the physical world.

All digital currencies exist thanks to three things: software, networks, and blockchains. Each digital currency has its own software (*e.g.* the Bitcoin client software or the Ethereum client software) and its own network of unaffiliated individuals and businesses who run that software on Internet-connected computers *(e.g.* the Ethereum network or the Bitcoin network). Computers running the software will, by default, authenticate and relay transactions denominated in the respective digital currency between members of the network. The network works together according to rules in the software (known as consensus rules[3]) in order to agree upon, compile, and store a ledger of all valid digital currency transfers amongst members of the network. The network may also work together to obtain other productive results, such as on -demand decentralized computation or file-storage. The ledger of transactions for each network describes the entire past and current distribution of the corresponding digital currency, and it is known as a blockchain (*e.g.* the Bitcoin blockchain[4] or the Zcash blockchain). Network participants who obey the consensus rules of the software and who perform verifiable work maintaining the blockchain and providing any additional functionality (*e.g.* computation or file storage) are automatically rewarded with new units of the digital currency and/or digital currency-denominated fees attached to transfers between users on the network.[5]

protocol and contribute resources to the network. As such, the token is better analogized to fuel for running an automated decentralized engine rather than money involved in a person to person exchange of goods and services. To make it clearer, money gets you things in the world through a voluntary exchange with a person, fuel gets you things in the world by powering a machine that doesn't have discretion. The tokens in decentralized computing systems, if operating as designed, should therefore be more like fuel than money.

[3] For a complete explanation of the open consensus mechanisms that power digital currency networks like Bitcoin and Ethereum, see Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet," *Coin Center*, December 2016, *available at* https://coincenter.org/entry/open-matters

[4] The bitcoin blockchain is broken up into blocks. Each block comprises the authoritative list of bitcoin transactions that settled in a given period that is, on average, 10 minutes long. For an up to date list of recent blocks and the transactions included within them, see https://blockchain.info/blocks.

[5] Participating in the process of verifying and updating the blockchain is known as mining. For a comprehensive explanation of the mining process Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies," Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

Blockchains do not include human readable names. Instead, a blockchain lists transaction histories and token distribution as between pseudonyms: random but unique numbers that are commonly referred to as addresses (*e.g.* a Bitcoin address or an Ethereum address). A person has possession of some amount of a digital currency because she (or her agents) is capable of producing a digital signature that corresponds mathematically to an address or series of addresses in the blockchain that has a positive balance. A person can generate an address and the associated cryptographic data necessary to create matching digital signatures (a private key) by running free and open source software specific to the digital currency she wishes to send and receive. The software is sometimes known as a "wallet" because it will keep track of all the addresses generated, as well as the matching private keys necessary to transact, storing all of this data on the computer or internet-connected device to which it was installed. Typically this data is encrypted with a password set by the user such that mere access to the device is insufficient to initiate transactions.

Note that there are several levels of security in this scheme: a transaction can only be made by signing a message with a private key that corresponds to a positive balance in an address on the blockchain; users will have several addresses and matching private keys to obtain a modest level of privacy with respect to their total transaction history; and all private keys are, together, stored in an encrypted, password-protected form on the user's device through a wallet. When one secures her own wallet on her own device, one is using a *software wallet* to store and transfer her digital currency. That software wallet may be an app on a smartphone or it may be software that runs on a desktop or laptop computer. It may even be a purpose-specific computer designed to do nothing but store and protect the wallet data (known generally as a *hardware wallet*).

Alternatively, persons who do not want to themselves store this data on their own device (and by extension personally secure their digital currencies) may elect to use an agent to safekeep their digital currency. In this case we still often refer to the products and services of the agent as a wallet even though this arrangement differs significantly from self-storage. When a person entrusts an agent to safekeep her digital currency then she is using a service provided by a company rather than software on her own computer. These services are often referred to as *hosted wallets* but sometimes, imprecisely, they are known simply as "wallets." For clarity, we will always use the term *hosted wallet* to describe such a service.

Hosted wallet providers tend also to provide exchange services and some may offer margin trading. Indeed, we are not aware of any firm that offers a hosted wallet service alone without also offering it in conjunction with exchange service. These providers are commonly known simply as *exchanges* or, more specifically, *custodial exchanges*. A custodial exchange will usually not have unique addresses, private keys, and wallets associated one-to-one with each of their customers. Instead, the hosted wallet provider will generally pool all customer digital currency

Coin Center (Jan. 2016) https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies.

in addresses secured within one omnibus wallet. Maintaining individual wallets for every customer is redundant, complicated, and increases the amount of vulnerable data (private keys, encrypted wallet passwords), and vulnerable processes (generating new wallets, encrypting them) involved in the service. This, as a cybersecurity expert might say, “broadens the attack surface” and increases the odds that some vulnerable data or process could be exposed to hackers and exploited. Rather than creating individual wallets for each customer, the provider will create one wallet for all customers, and then build internal controls to guarantee that customers who have received a given amount of a digital currency can always withdraw that amount of currency from the pooled wallet and can never withdraw more than that amount. These internal controls are still password and login based, but they are administered by the provider rather than by an individual encrypting her own wallet or by the decentralized network.

The above technical specifics hold for all decentralized digital currencies, regardless of which blockchain network is being discussed. Accuracy in terminology is essential whenever we wish to discuss in legal or in technical contexts the risks, benefits, obligations, or capabilities of various entities or arrangements in the digital currency ecosystem. Having addressed the need for care and specificity in terminology, we will now highlight the sections of the draft guidance that we believe lack specificity or clarity, and suggest possible modifications.

Areas of Ambiguity in the Draft Guidance

Throughout the guidance, the terms “counterparty seller,” “offeror,” “purchaser,” “depository,” “virtual currency platform,” “blockchain wallet,” and “customer” are often used. We acknowledge that some of these terms are terms of art in commodities law and therefore cannot and should not be replaced with terms familiar to customers and technicians in the virtual currency ecosystem. That said, we believe it is critical to set out early in the guidance a passage that maps or translates between commodities law and virtual currency terminologies. We suggest the following and believe it honestly reflects the goals of the CFTC’s guidance:

Counterparty Sellers. A counterparty seller is the person or company who sells virtual currency in a margined or leveraged trade and may be any of the following:

1. A person who personally secures her own virtual currency using a software wallet
2. A customer of a virtual currency exchange who owns virtual currency and secures that virtual currency using the exchange’s hosted wallet service
3. A virtual currency exchange that owns virtual currency on its own account apart from any virtual currency it secures for its customers.

Offerors. An offeror is the person or company who presents margined or leveraged trade offers to purchasers and may be any of the following:

1. The counterparty seller herself when she offers to sell in a margined or leveraged trade
2. A virtual currency exchange that allows its customers to trade virtual currency on margin and that presents these trade offers to their customers on behalf of their customers

Financers. A financer is a person acting in concert with the offeror or counterparty seller by providing financing or leverage for the trade, and may be any of the following:

1. A person who personally secures her own virtual currency using a software wallet
2. A customer of a virtual currency exchange who owns virtual currency and secures that virtual currency using the exchange's hosted wallet services
3. A virtual currency exchange that owns virtual currency on its own account apart from virtual currency it secures for its customers

Depositories. A depository is a person or company who secures virtual currency on behalf of a counterparty seller, purchaser, and/or third parties to a trade and may include:

1. A virtual currency hosted wallet provider
2. A virtual currency exchange that offers hosted wallet services to its customers

When both seller, offeror, and purchaser secure their own virtual currency using software wallets, no depository is involved in the trade.

Customers. A customer of a virtual currency exchange may be, alternatively:

1. A counterparty seller
2. A purchaser
3. An offeror
4. A financer

The term "virtual currency platform" does not add anything to the guidance that would not be accomplished by using the more commonly understood term *exchange*. The term "blockchain wallet" is not sufficiently precise and is not a term that is in any common use. The Commission should make explicit use of the terms *hosted wallet* and *software wallet,* where appropriate, to create clarity with respect to how two very different technologies interact with commodities law. For example, when guidance is offered with respect to exchanges it should be made clear that exchanges often provide "hosted wallet" services and that such provision of services would make the exchange a "depository" for one or more traders. The guidance should also describe the terms *hosted wallet* and *software wallet* as we have in the first section of this comment and then map them to terms such as *depository* and *offeror*, as we have done immediately above.

Policy Question: Exchanges that Play Multiple Roles

With terminology clarified, there is now a question of policy rather than mere terminology to which we have not been able to derive an answer based on the draft guidance alone. To clarify the question we must begin with a hypothetical: An exchange offers margin trading between its customers such that some customers are counterparty sellers, others are purchasers, and still other customers provide leverage or financing for the trade. The exchange also provides hosted wallet services for all of these persons. In no situation does the exchange act as a counterparty seller or a provider of financing for the trade. To our understanding, this exchange is an offeror, as well as a depository for virtual currency owned by the other parties.

Does the Commission believe it is permissible under its rules for an exchange to play these dual roles: offeror of margin trades to which it is neither a seller or financier *and* depository for both the counterparty seller and the purchaser?

Further, if it is permissible for an exchange to play these dual roles, then do trades achieve actual delivery when the exchange, acting as a depository, does the following:

1. Evidences a change in legal ownership over traded virtual currency from seller to purchaser such that "no liens (or other interests of the offeror, counterparty seller, or persons acting in concert with the offeror or counterparty seller on a similar basis) continue forward at the expiration of 28 days from the date of the transaction," *and*

2. Within 28 days, adjusts internal controls over virtual currency in the exchange's hosted wallet system such that neither the seller nor the financers' login and password can initiate a transfer of the traded virtual currency and such that the purchaser's login and password can now, exclusively amongst all of the exchange's customers, initiate a transfer of the traded virtual currency. This transfer may be to other customers of the exchange (as evidenced by further adjustment of internal controls) or to anyone else in the world (as evidenced by a validly signed transaction on the virtual currency blockchain).

Whatever determination the Commission makes, the answer to this policy question should: (a) be made clear in this guidance and use common terms and vocabulary that industry will be able to easily comprehend, and (b) have parity with how other commodities arrangements are treated.

By this we mean that if a company that is the offeror of leveraged gold trades on behalf of its customers, and is also the depository of the gold for both the seller and the purchaser, can make actual delivery by evidencing a change in title and adjusting the security on its premises such that sellers can no longer access their gold and purchasers can, then so too should the digital currency exchange described in the above hypothetical be able to make actual delivery by evidencing change in ownership and also adjusting internal controls over virtual currency held in their hosted wallet system.

Conclusion

We thank the commission for taking great care in crafting guidance related to these exciting new technologies. To ensure greater compliance and a level playing field for digital currency businesses, we urge the commission to clarify the existing guidance by using the common terms we have described herein, offering non-binding but illustrative definitions of those terms as the commission understands them, and then mapping those terms to terminology relevant to commodities regulation. Finally, we ask that the commission offer a clear answer to the hypothetical we posed in the final section: whether, under the specified conditions, an exchange’s leveraged trades can achieve actual delivery if the exchange acts both as offeror and also as depository to the counterparty seller and the purchaser.