Comments on the COIN ETF (SR-BatsBZX-2016-30)

Tim Swanson

November 17, 2016

Note: I neither own nor have any trading position on any cryptocurrency. The views expressed below are solely my own and do not necessarily represent the views of my employer or any organization I advise.

This paper originally began as a letter in response to the SEC letter dated October 12, 2016 regarding an open comment period for the Winklevoss Bitcoin ETF, commonly referred to as the COIN ETF.[1]

It is my opinion that the approval of the COIN ETF represents a qualitative risk that could impact – without recourse or due process – investors in the COIN ETF. It could also negatively impact certain regulatory frameworks and the financial industry both of whom are currently experimenting with a mixture of technology commonly referred to as blockchain technology.[2]

Some of the issues below have been previously described in the Winklevoss Bitcoin Trust S-1 (pages 8-11; 32-33), but due to circumstances over the past 6 months they are worth highlighting once again.[3]

As described below, in terms of volume and liquidity the cryptocurrency market is relatively small compared to traditional FX markets and as a result unknown and unregulated participants ("whales") regularly move the price. Consequently, the COIN ETF creates a *caveat emptor* environment, or rather investor beware. Retail investors do not understand the risks and implications of forking in the code, collusion and coordination by mining pools, and price manipulation due to a lack of financial controls.

This paper is split into six sections, each of which answers questions raised by the SEC. For reasons detailed below, I recommend that the SEC reject the proposed COIN ETF.

Note: all of the citations, references, and links are from independent sources and unaffiliated with myself or any of the organizations I advise or work for.

Section 1: Price Manipulation Risks

In the SEC's most recent letter, dated October 12, 2016, the SEC asked,[4]

[1] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf
[2] http://blogs.wsj.com/moneybeat/2016/06/29/winklevoss-twins-pick-bats-for-proposed-bitcoin-etf/
[3] https://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/d562329ds1.htm#tx562329_4
[4] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf

> What are commenters' views about the current stability, resilience, fairness, and efficiency of the markets on which bitcoin are traded? [...] What are commenters' views on the risk of loss via computer hacking posed by such an asset?

To better answer these question, we should first look at other existing marketplaces.

The foreign exchange (FX) market is the largest, most liquid market in the world, with reported total daily volumes around $5 trillion a day and around $2 trillion in spot FX.[5] Meanwhile, daily volumes (when "wash trade" volumes at certain exchanges are excluded) summed across all cryptocurrency exchanges ranged in October 2016 from $75 to $150 million.[6]

Relative to securities trading, at the time of this writing the "market cap" (available supply*price) of bitcoin is slightly above the market capitalization of Seagate (STX) at $10.2 billion. The average volume in terms of United States dollar amount traded daily is roughly equal between Seagate and bitcoin.[7] STX is more liquid, given that its quotes are in a regulated marketplace and its volumes are mostly confined to 6.5 hours of trading, while bitcoin volumes are diffused over 24 hours across several dozen unregulated and underregulated exchanges, some of which as described below, are basically "bucket shops."[8]

One response is that the comparison above may not be apples-to-apples, because both the FX and securities marketplaces are regulated (some more than others). For instance, in the United States, recent legislation by the NFA led Interactive Brokers, host of 7% of the American retail FX market, to stop offering the customers with less than $10 million the ability or option to leverage their positions.[9]

There are multiple cryptocurrency exchanges that provide leverage. Huobi, a cryptocurrency exchange based in Beijing, allows traders to trade with 10x leverage through its BitVC affiliate.[10] 796.com, a Shenzhen-based cryptocurrency exchange, allows traders to trade with 50x leverage.[11]

Neither of these exchanges are regulated nor are there proper financial controls in place. As a consequence, users and investors have suffered losses on both platforms. In November 2014, Huobi socialized $1.2 million in losses BitVC had across all of its traders to cover a "system loss."[12] In January 2015, 796.com "lost" 1,000 bitcoins which impacted the dividend to investors.[13]

And, these are not isolated incidents.

During the process of just drafting this paper:

- Bicurex, the largest Bitcoin exchange in Poland, was hacked and lost 2,300 bitcoins (worth ~$1.5 million)[14]

[5] http://www.bis.org/publ/rpfx13fx.pdf Results for the 2016 survey are not yet available.

[6] https://coinmarketcap.com On October 27, 2016 for example, the 24 hour volumes across cryptocurrency exchanges with fees were $94 million.

[7] On October 27, 2016, 24-hour volume of bitcoin was $94,087,300 vs. STX volume of shares of 5,271,296 * $34.24 (closing price) = $180,489,175. The market data varies daily, and will vary based on metrics, but based on "market cap" and longer-term volumes as well, Seagate is a relatively fair comparison.

[8] http://www.investopedia.com/terms/b/bucketshop.asp

[9] https://smnweekly.com/2016/08/15/interactive-brokers-restricts-us-leveraged-forex-trading-to-big-clients-only/

[10] http://bitcoindaily.org/okcoin-futures-exchange/

[11] https://796.com/connect?name=1

[12] http://www.coindesk.com/huobis-bitvc-takes-trader-profit-cover-1-million-loss/ and https://cointelegraph.com/news/-huobi-talks-about-lessons-learned-from-socialized-losses

[13] https://cointelegraph.com/news/chinese-exchange-suffers-1000-btc-loss-in-uncertain-service-compromise

[14] https://np.reddit.com/r/BitcoinMarkets/comments/59ncid/the_biggest_polish_exchange_got_hacked_2300_btc/

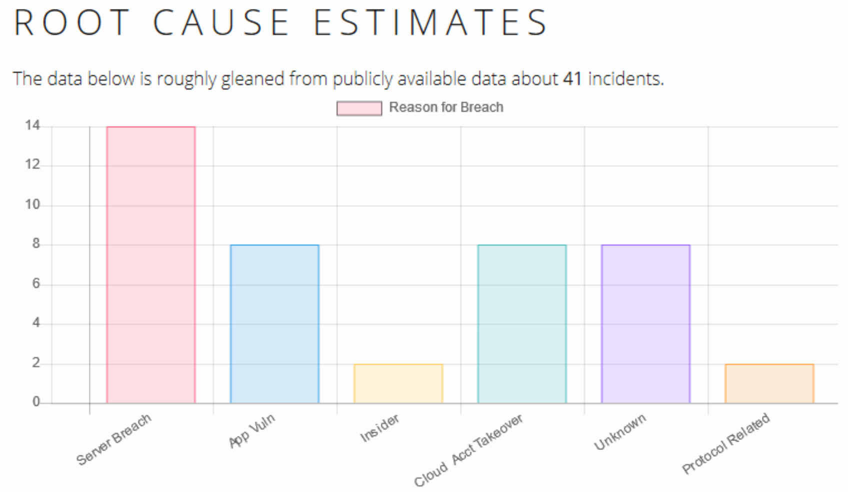
- Bitfinex, based in Hong Kong, announced yet another way to compensate its customers. Three months ago, Bitfinex seized funds of its customers after a large hack (it has been hacked twice in the past 18 months). It now plans to give equity of the parent company to its customers.[15]
- Cryptsy, once one of the largest altcoin exchanges prior to its bankruptcy, announced that the assets belonging to the wife of the CEO who fled to China, would now be liquidated to pay back the $5 million in customer losses.[16]
- Using the Shapeshift cryptocurrency exchange, The DAO attacker converted around 95,000 ether (ETC) it had taken from The DAO and changed it to 145 bitcoins; this is roughly equivalent to $100,000.[17] Separately, earlier this year Shapeshift was hacked for a total of around $230,000 in what is alleged to be at least partially an inside job.[18] The founder of ShapeShift also founded Satoshi Dice, an online gambling platform that was sued by and settled with the SEC in 2014 for offering unregistered securities.[19]
- Mike Murgio, father of Anthony Murgio, is a former Palm Beach County School Board member who pled guilty on October 27, 2016 in a bribery case for, "conspiring to bribe a bank official to conceal the financial activities of his son's [Anthony's] unlicensed Bitcoin exchange."[20] The exchange in question, Coin.mx, also laundered ransomware payouts through its system which classified them as "collectable memorabilia" and dubbed the business as the "Collectables Club."[21]

There appears to be a near direct correlation between the behavior of exchange operators and the level of regulation an exchange is required to comply with. One academic paper presented in April 2013 found that of 40 cryptocurrency exchanges surveyed, 18 had shut down and stolen customer funds.[22] In the three years since the paper was published, only a handful of the 40 still exist while others closed down. Of those that initially survived 2013 was Swedish exchange, Kapiton. Yet a year later, its founder died and due to operational problems, users were left unable to access their funds.[23]

Despite communal suggestions that users should remove their bitcoins to user-controlled cold wallets (air-gapped wallets), in practice, many users still leave bitcoins on cryptocurrency exchange creating large counterparty risks such as in the event an operator dies or steals assets. Another more recent example took place in May 2016, Gatecoin – a Hong Kong-based cryptocurrency exchange – announced that it had lost $2.1 million due to a hack which effected customer funds that were stored by the exchange operators.[24]

The former Director of Security at Coinbase has kept a catalogue of several dozen hacks, takeovers, and attacks and found that nearly all of them are preventable.[25] His list does not count “exit scams” such as what Moolah did with MintPal in 2014.[26] Ryan Kennedy, who went by the pseudonym Alex Green, used affinity fraud to move into the inner circles of Moopay, a cryptocurrency development company commonly known as Moolah.

[15] https://www.finextra.com/pressarticle/66851/bitfinex-offers-hacked-users-equity
[16] http://www.miaminewtimes.com/news/burned-users-of-south-floridas-cryptsy-bitcoin-exchange-may-get-1-million-settlement-8878531
[17] https://www.bokconsulting.com.au/blog/the-dao-hackers-booty-is-on-the-move/
[18] http://www.coindesk.com/digital-currency-exchange-shapeshift-says-lost-230k-3-separate-hacks/
[19] https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520
[20] http://extracredit.blog.palmbeachpost.com/2016/10/26/ex-school-board-member-mike-murgio-to-plead-guilty-in-bribery-case/
[21] https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/manhattan-u.s.-attorney-announces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange and http://www.theregister.co.uk/2016/10/28/coinmxs_murgio_pleads_guilty/
[22] http://fc13.ifca.ai/proc/1-2.pdf
[23] https://www.reddit.com/r/Bitcoin/comments/2tid9v/sebastian_manitski_creator_of_kapiton_has_left_us/
[24] http://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/
[25] https://magoo.github.io/Blockchain-Graveyard/
[26] https://motherboard.vice.com/read/darknet-slang-watch-exit-scam



Source: magoo.github.io/Blockchain-Graveyard

Kennedy used this cover and convinced the operator of the MintPal cryptocurrency exchange to let his team at Moolah rebuild the MintPal exchange platform. Several months later Kennedy disappeared with nearly $2 million in customer funds (around 3,700 bitcoins). He was later arrested and in August 2016 sentenced to 11 years of prison in the United Kingdom for unrelated crimes.[27] The exchange never relaunched and victims were not compensated.

A research paper published in January 2015 by SMU, "identified 41 scams occurring between 2011 and 2014, in which fraudulent sites stole Bitcoin from at least 13,000 victims."[28] Of the losses which they conservatively estimated at around $11 million (and likely millions more), only about $4 million was returned to victims.

In the SEC's most recent letter, dated October 12, 2016, the SEC asked:

> What are commenters' views on whether an ETP based on such an asset would be susceptible to manipulation?

Cryptocurrencies such as Bitcoin are inherently not a "safe asset" in any sense and are relatively easy to manipulate: both in terms of price and in terms of custody.[29]

But before going further, we should also include Question 5, where the SEC writes:

> A commenter notes that the Gemini Exchange has relatively low liquidity and trading volume in bitcoins and that there is a significant risk that the nominal ETP share price "will be manipulated, by relatively small trades that manipulate the bitcoin price at that exchange." What are commenters' views on the concerns expressed by this commenter?

The cryptocurrency exchange market is still very immature and largely based on self-reported volumes. There are no commonly accepted best practices surrounding pricing or transparency of price discovery.

[27] http://www.bristolpost.co.uk/bristol-man-who-got-kicks-from-dominating-partners-is-jailed-for-11-years-for-rape/story-29586393-detail/story.html

[28] http://blog.smu.edu/research/2015/01/27/bitcoin-scams-steal-at-least-11-million-in-virtual-deposits-from-unsuspecting-customers/

[29] There could be a comparison of cryptocurrencies such as Bitcoin with synthetic ETFs which are more common in Europe but controversial. Basically it is an ETF without the underlying asset. In the United States they are rare.

And, with respect to the United States marketplace, there is nothing equivalent to a national best bid and one best offer (NBBO) with cryptocurrency exchanges.[30]

Furthermore, as it is underdeveloped market structure it largely lacks reporting venues, reliable data feeds and fundamentally there is no transparency with respect to the interest parties as a whole or within specific cryptocurrency exchanges. Because there are few financial controls in place at most exchanges, both exchange operators and owners have material non-public information in terms of knowledge of hacks, large buy and sell orders, legal actions, and so forth. Lack of financial controls could lead to, among other risks, the ability to front-run customers.

Lacking financial controls poses a significant risk for investors because several of the cryptocurrency exchanges, which comprises the previously used Winklevoss Index (Winkdex), may not be financially sound and therefore it would have had adversely impact investors in the COIN ETF. The constituent parts of the Winkdex are discussed in Section 2.

In several jurisdictions, the COIN ETF may be effectively creating a financial product for which the underlying bitcoin may or may not be an actual asset. This is because there is no consensus on the legal nature of bitcoin in the jurisdictions through which the exchanges comprising the Winkdex.[31]

The COIN ETF may be legitimizing a "price" for which there is no regulated underlying basis; and the prior history of information asymmetry and manipulation throughout the cryptocurrency exchange industry is well documented.[32]

For instance, what if a court or regulator in a jurisdiction that includes an exchange comprising the Winkdex declares that bitcoin is not property? Or that bitcoins on these exchanges comprising the Winkdex themselves end up having different values due to these new laws or rulings?

In practice, we have seen that “virgin coins” trade for more than non-virgin coins.[33] Virgin coins are bitcoins freshly mined from a mining pool and typically yield a higher market premium as they lack provenance. Because they lack provenance. they are sometimes used in illicit activities on darknet markets which makes linkage via analytics more difficult.[34]

What if there is a new court order or ruling makes this price disparity more pronounced and stratified? What does this mean for retail investors; how are they expected to understand these risks?

In addition to virgin coins we have empirical cases where bitcoins are not viewed by the market as the same; within different markets there are different bitcoins.

This includes the most basic difference: on-blockchain and off-blockchain price discrepancy of coins that were held and traded during January and February of 2014 at Mt. Gox. Mt. Gox was a Tokyo-based bitcoin exchange that upon declaring bankruptcy claimed it had outstanding liabilities of 850,000

[30] With respect to the United States (not Europe), in some ways, the cryptocurrency market resembles the equity market of 40 years ago, before the Securities Act Amendments of 1975. Under the SEC’s Regulation NMS, today United States equity bids and offers are consolidated into one national best bid and one best offer (NBBO). This effectively holds the line on prices in one marketplace. The regulation does not allow participants to trade at a level higher than an offer or lower than a bid, without first filling all outstanding orders resting at a better marketable level. Conversely, with retail FX brokers and cryptocurrency exchanges, every exchange has its entirely own marketplace. There are no restrictions on the potential fills and the “best” bid and offer on every exchange is different. See: https://www.gpo.gov/fdsys/pkg/STATUTE-89/pdf/STATUTE-89-Pg97.pdf and https://www.sec.gov/rules/final/34-51808.pdf

[31] http://map.bitlegal.io/

[32] http://fc13.ifca.ai/proc/1-2.pdf and https://magoo.github.io/Blockchain-Graveyard/

[33] https://ihb.io/2015-07-30/news/virgin-bitcoins-8248

[34] https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces

bitcoins, worth roughly $450 million.[35] The Mt. Gox exchange was specifically singled out in the letter published by the SEC on October 12, 2016 (page 12).

Mt. Gox bitcoins did not trade at par due to perceived insolvency risk. What, if anything, drove the discrepancy between the price at Mt. Gox and other exchanges such Bitstamp during this time frame in early 2014? It appears that the different prices suggested solvency on the fiat side and/or the cryptocurrency side.

In the case of Mt. Gox, trying to remove or withdraw fiat became increasingly difficult the closer Mt. Gox came to going bankrupt. As a result, prices for frozen "Goxcoins" (similar to "Lehman dollars") dropped in proportion to this difficulty. As a consequence, during the first two months of 2014, an arbitrage service called Bitcoin Builder, became popular due to an arbitrage opportunity between non-ambulatory Goxcoins and other exchanges.[36]

While Mt. Gox may have been the largest bankruptcy – proceedings of which are still ongoing – other large hacks and loses have taken place including most recently Bitfinex (and its BFX token) which will be detailed later.[37]

And how can Gemini Trust Company assure investors of solvency of its exchange?

One letter the SEC received in July described a method for proving and guaranteeing 100% reserves held by the custodian's cold storage system.[38]

Currently neither retail nor institutional investors are provided public information to find out the solvency of any cryptocurrency exchange. To assess the credit worthiness of your bank, there exists a public call report.[39] But this type of service does not exist for cryptocurrency exchanges. Furthermore, since the Mt. Gox bankruptcy there have not been regular public audits of cryptocurrency exchanges comprising the Winkdex. In fact, several days before Mt. Gox collapsed, BTC-e – which was then a component of the Winkdex – publicly stated it would begin publicly publishing accounting statements certified by external auditors.[40] It has not.

This raises several questions. What are retail investors betting on in this largely unregulated marketplace? They are betting on the exchange rate as quoted by Bitfinex or Bitstamp. But what drives those prices? Investors appear to be betting on solvency in exchanges in general. However, what about material information behind the operations of those exchanges?

The principals involved in the COIN ETF are fundamentally unknown because all of the exchanges that comprise the Winkdex have not disclosed their role or the principals of their exchanges publicly.

We do not know the principals, the parties of interest at each of the exchange and what their direct participation is in the COIN ETF. Is it disclosable? With Mt. Gox, then-CEO Mark Karpeles had some serious material non-public information regarding its solvency. Yet Mark Karpeles' activity was not disclosed.[41]

[35] http://www.nytimes.com/2016/05/26/business/dealbook/mt-gox-creditors-seek-trillions-where-there-are-only-millions.html
[36] http://www.coindesk.com/has-company-found-workaround-mt-gox-withdrawals/
[37] BFX is the name of a virtual token that Bitfinex gave its customers. Some customers did not get the same level of haircut, see SynapsePay: https://www.reddit.com/r/Bitcoin/comments/4wrmne/my_haircut_only_227_usd_balance_untouched/
[38] https://www.sec.gov/comments/sr-batsbzx-2016-30/batsbzx201630-4.pdf
[39] https://cdr.ffiec.gov/public/
[40] https://btc-e.com/news/199
[41] https://www.amazon.com/Digital-Gold-Bitcoin-Millionaires-Reinvent/dp/006236250X

Will all of the counterparties involved in the Winkdex and COIN ETF provide their material information to the public? The operators of Bitfinex, which two months ago was hacked and lost $65 million in customer funds, may have some material non-public information regarding its solvency. Yet this information has not been released and troubling, Bitfinex is still listed as part of the Winkdex.

How would future hacks impact the COIN ETF and how do investors have recourse?

In addition, over the past two years, in any given quarter at least one "flash crash" occurs on a major cryptocurrency exchange that – if listed on a regulated stock exchange – would be likely investigated by a securities regulator.

For instance, Bitfinex alone has experienced a crash in 2014, 2015, and again in 2016.[42] And throughout 2014, multiple hoaxes, rumors, and fake stories were published in various media publications in China which led to sharp price declines.[43] In January 2016, a prominent Bitcoin developer announced that he was leaving the project and that the "original vision" failed.[44] Within several hours the price of bitcoin dropped 15% or more on many exchanges. How can the Winklevoss Bitcoin Trust protect investors in the event that influential developers make similar statements?

And more precisely, who are the large traders ("whales") on each exchange comprising the Gemini exchange and the exchanges constituting the Winkdex? What influence do these whales have on trading swings and movements? Consequently, because several of the exchanges that comprise the Winkdex typically do not comply with Know Your Customer (KYC) or Anti Money Laundering (AML) documentation requirements, it is difficult, if not impossible, to ascertain who is responsible for these movements.

There are fundamental differences between ETFs and the COIN ETF. In some ways, the COIN ETF would be akin to having a weather ETF, where the existence of deity or even a *force majeure* is known but not disclosed, but there is in fact a deity on the other side of the trade.

The counterparties listed as part of the Winkdex are opaque and these participants could be, as described below, manipulate the price. With previous ETFs, investors know what the potential underlying is in an ETF. They would know the nature and interest in the underlying of an ETF.

With gold, the market has a fairly accurate idea of many major holders of gold there are, but this is not the case with bitcoin.[45] Similarly, we have a pretty good idea due to volume of minerals dug who the biggest gold miners and suppliers are and consequently the price discovery process in gold is better than a cryptocurrency such as bitcoin.[46]

The theory of price manipulation is not far-fetched either as even regulated cryptocurrency operations in the United States have been fined for non-compliance.

- On September 24, 2015, the Commodity Futures Trading Commission announced a settlement and fine of TeraExchange, a regulated exchange which provided a provisionally registered Swap Execution Facility, for failure to prevent wash trading.[47]

[42] http://www.coindesk.com/margin-trading-crash-price-bitcoin/ and http://www.coindesk.com/bitcoin-price-falls-14-following-bitfinex-flash-crash/ and http://www.coindesk.com/bitcoin-drops-12-exchange-hack-amplifies-price-decline/
[43] http://www.coindesk.com/bitcoin-price-drops-new-chinese-bank-rumours/
[44] http://www.newsweek.com/bitcoin-price-crashes-cryptocurrency-branded-failed-experiment-416267
[45] http://www.bitcoinrichlist.com/top500
[46] https://en.wikipedia.org/wiki/Largest_gold_companies
[47] http://www.cftc.gov/PressRoom/PressReleases/pr7240-15

- On July 11, 2016, the SEC announced a settlement and fine of Bitcoin Investment Trust (BIT) and SecondMarket, which resulted in a Cease and Desist for not abiding by proper SEC redemption policies due to a violation of Regulation M.[48] BIT is referred to again in Section 6.

While the investigation is still ongoing, one of the purported explanations for the dramatic rise and fall of Mt. Gox, which collapsed in February 2014, and one that was initially part of the Winkdex[49] – is partially tied to an internal trading bot called "Willy" which allegedly manipulated the price of bitcoin. [50] Willy's efficacy was due largely to the fact that trading volume on Mt. Gox at the time represented between 50-80% of all global bitcoin trading.

Another exchange that is integral to the price discovery process of several cryptocurrencies including Bitcoin, is Hong Kong-based Bitfinex. On June 2, 2016, the Commodity Futures Trading Commission announced that it had fined and settled with Bitfinex for offering regulated products without having properly registered to do so.[51]

Currently the KYC and AML documentation requirements to deposit, trade and withdraw are minimal at Bitfinex, yet despite being hacked twice, it is the "finex" price which largely drives the market each day for Bitcoin.[52] Collectively, many of these exchanges listed above and below are not only accessible to potential attackers, but may lack safeguards in the event that an attack actually takes place.

To reflect upon the questions at the beginning of the section: empirically the markets that bitcoin has traded on are not stable, are not resilient, are not usually fair for traders. Furthermore, historically the risk of loss via computer hacking is relatively high. Thus to answer another question posed on page 12 of the SEC's questionnaire: bitcoin is not an appropriate underlying asset for a product that will be traded on a national securities exchange.[53]

Section 2: The Winkdex

This section will look at the evolution of the underlying pricing process for the COIN ETF including several amendments. For nearly three years it was proposed that the Winkdex would provide the underlying basis for pricing the Shares of the Trust. That all changed in the summer of 2016.

On June 29, 2016, Gemini Trust Company filed its sixth amendment for the COIN ETF, which replaced the Winkdex with the spot price of one single exchange: the Gemini exchange at 4:00 pm EST.[54] This was likely done in part because of the unreliability and potential for manipulation of the exchanges comprising the Winkdex which this section will explore later below.

On October 18, 2016, the Trust filed its seventh amendment, replacing the Gemini exchange spot price with a 4:00 pm EST auction price that also only takes place on the Gemini exchange.[55]

While there are only seven weeks of data for the Daily Auction, the results as measured in terms of participation and volume, have been underwhelming. As of this writing, in terms of bitcoin volume, the

[48] https://www.sec.gov/litigation/admin/2016/34-78282.pdf

[49] https://www.reddit.com/r/BitcoinMarkets/comments/1zi4ag/why_does_the_winkdex_still_list_mt_gox/

[50] http://www.coindesk.com/bot-named-willy-did-mt-goxs-automated-trading-pump-bitcoin-price/

[51] http://www.cftc.gov/PressRoom/PressReleases/pr7380-16

[52] Prior to the July 2016 hack on Bitfinex, the Bitfinex price constituted nearly a 50% weight on most major Bitcoin indices. See Tradeblock weighting: https://tradeblock.com/markets/index/

[53] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf

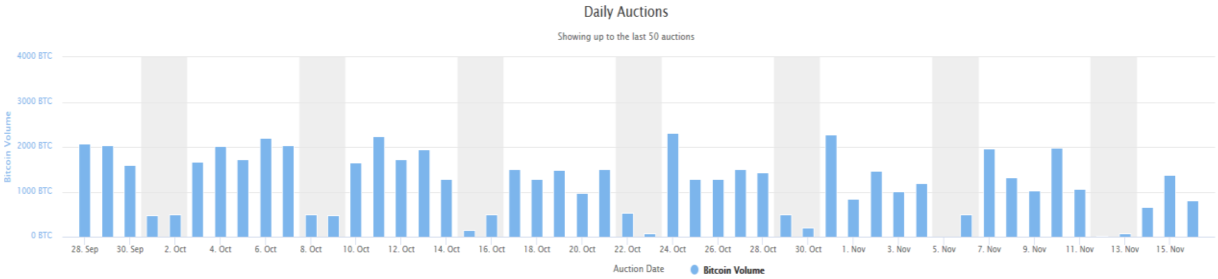
[54] https://www.sec.gov/Archives/edgar/data/1579346/000119312516636535/d68862ds1a.htm

[55] http://www.wsj.com/articles/winklevoss-brothers-choose-state-street-to-help-launch-bitcoin-etf-1476825213

largest Daily Auction was for 2,308 bitcoins and the smallest was 0 bitcoins.[56] On average, the Daily Auction is comprised of 1,230 bitcoins.

Based on the average past 3 days of trading, relative to other spot exchange, in terms of USD/BTC trading the Daily Auction would rank 11th, coincidentally just behind the actual Gemini spot exchange during the same time frame.[57]

In other words, the auction currently averages lower volume than most other exchanges do in a given day.



Source: http://geminiauctionhistory.bitballoon.com/

In fact, on certain days, specifically on weekends, the Daily Auction has not attracted many participants, falling to as little as zero volume on at least one occasion.

If this evolution and transition from a basket of exchanges to the Daily Auction was done to counter potential manipulation, there are still some unanswered questions. Who are the participants in the auction? Do these participants have any conflicts of interest? Are they affiliated with other exchanges or with mining farms or pools?

Perhaps the easiest illustration of this manipulation are exchanges based in East Asia, such as BTCC (formerly BTC China), OKCoin, and Huobi. All three are effectively unregulated and do not actively enforce KYC or AML documentation gathering requirements.

In addition, they each have zero-fee trading schemes, that is to say, traders are not charged based on trades. Instead, exchanges typically charge fees based on deposits and withdrawals of fiat currency. Zero-fee trading is sometimes coupled with in-house wash trading in order to inflate and overstate the volume and depth of an order book in order to create the perception that the exchange is popular.[58] This perception is helpful in a competitive market with very little product differentiation, as well as when attempting to raise external capital for continued growth.

For instance, prior to going on a road show, exchange operators may turn on exchange-owned and operated bots to trade with themselves. Because no other parties are involved, this effectively is a wash trade. Two years ago, Changpang Zhao, the former CTO of OKCoin, explained how OKCoin used bots that were "designed to pump up volumes" all with the approval of the CEO.[59]

There is also concern that internal staff can see the order books of the clients and know where the stop-loss limits are. They can relatively easily push the price towards the stop-loss levels creating a gain for

[56] https://gemini.com/auction-data/
[57] http://data.bitcoinity.org/markets/exchanges/USD/24h#volume_desc
[58] http://www.investopedia.com/terms/w/washtrading.asp
[59] https://www.reddit.com/r/Bitcoin/comments/37tm1b/czs_statement_regarding_the_dispute_between/ and https://www.reddit.com/r/BitcoinMarkets/comments/3lwnyn/the_state_of_trading_in_the_bitcoin_markets/

the exchange and a loss for the clients – this is in effect trading against the client in full view of the client pain points.

This is accomplished in part because as described above, most exchanges do not have adequate financial controls. In practice, most cryptocurrency exchanges acts as a depository, broker/dealer, a custodian, and also a clearinghouse. They do so without erecting internal barriers to prevent exchange operators from abusing asymmetric information.

This is not new to cryptocurrencies; indeed, it is a risk in global foreign exchange markets, but the low liquidity of cryptocurrency markets makes it easier for a single actor to manipulate the price.

How does this impact the COIN ETF?

On p. 13 of the SEC questionnaire:[60]

> According to the Exchange, the Gemini Exchange Spot Price is representative of the accurate price of a bitcoin because of the positive price - discovery attributes of the Gemini Exchange marketplace. What are commenters' views on the manner in which the Trust proposes to value its holdings?

While the question specifically asks about the spot price at the Gemini exchange, which will be looked at momentarily, it is instructive to see the reasons behind why this exchange eventually became the only exchange chosen for its role.

Since its announcement as an amendment in February 2013, the Winkdex price which underlies the price of the Commodity-Based Trust Shares, is currently culled from a pre-arranged group of five exchanges.[61] The Winkdex algorithm selects 3 out of 5 'qualified exchanges' and takes a weighted average every 2 hours.

Three years ago, the weighted price was based on three exchanges: Mt. Gox, Bitstamp, and BTC-e. A year later, with the launch of the Winkdex iOS app, the price data included: Bitstamp, Bitfinex, BTC-e, CampBX, and LocalBTC.[62]

In retrospect, while these exchanges may have had the volume to aid in price discovery, they each have had problems:

- LocalBTC: also known as LocalBitcoins, does not require its users to comply with any KYC or AML regulations and as a consequence is popularly used for money laundering and illicit money transfers into and out of fiat. Despite its growing volume, this should clearly not be included for regulatory compliance reasons.
- CampBX: is effectively dead. According to Bitcoinity.org, over the past 6 months CampBX has had a total of 319 bitcoins (BTC) traded on their platform.[63]
- BTC-e: nominally operates out of Bulgaria and also does not require its users to comply with any KYC or AML regulations and as a consequence is often used for mixing bitcoins with altcoins in order to remove lineage and provenance. Whereas some mixers will respond to subpoenas and provide information to law enforcement, BTC-e tries not to work with law enforcement. This altcoin <-> bitcoin volume not only distorts the true volume on the exchange

[60] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf
[61] https://www.sec.gov/Archives/edgar/data/1579346/000119312514058712/d562329ds1a.htm#tx562329_8
[62] https://www.producthunt.com/tech/winkdex-ios-app
[63] https://campbx.com/depthtable.php

but also likely facilitates money laundering and therefore should not be included as well. In August 2014 the exchange also experienced a "flash crash."[64]

- Bitfinex: once you remove the China-based exchanges due to artificially inflated volumes, Bitfinex is the largest exchange by volume globally. It has also been hacked twice in the past 18 months and socialized the losses of its second hack by seizing funds from customers to recapitalize itself.[65] It is currently raising $70 million in order to pay back its customers and is unregulated.[66] On the other hand, they do respond to subpoenas and we know who the founders are (some are in Taiwan, where the corporate bank accounts are also located).[67]
- Bitstamp: was hacked in January 2015 for $5 million in losses.[68] Unlike Bitfinex, it did not socialize the losses by seizing customer funds. It has since announced it has become the first nationally licensed bitcoin exchange in Europe in April 2016, although it is likely that Circle was actually the first.[69]
- Mt. Gox: as described earlier in Section 1, went bankrupt in February 2014 and lost several hundred million dollars' worth of bitcoins, the majority of which belonged to customers.[70] Previously it had suffered a very large hack in June 2011 resulting in the loss of thousands of bitcoins.[71]

One response will likely be that the Winkdex has changed its composition to include regulated exchanges. The Winkdex currently includes Bitfinex, Bitstamp, Gemini and itBit; two of which are domiciled and regulated in the United States. Let us look at the two additional exchanges it now uses as part of its weighting:

- itBit: obtained a banking charter license from the New York Department of Financial Services in 2015.[72] Over the past 6 months it has traded approximately 1.01 million bitcoins or about 5,627 BTC per day.[73] However, more than 10% of those trades are based on SGD. In terms of USD/BTC trades, itBit ranks 4th globally, just ahead of Bitstamp. While USD/BTC volume has seen an uptick over the past couple of months, as a whole, the relatively lower volume over several years of operations is one of the reasons it is allegedly trying to sell the exchange.[74]
- Gemini: launched in October 2015, it is owned and operated by the same management team that created the Winkdex and the Winklevoss Trust Company. But despite the publicity and having obtained a BitLicense from the New York Department of Financial Services, the exchange has floundered in terms of volume.[75] Over the past 6 months it ranks 9th in terms of USD/BTC trading globally, just ahead of Kraken which has raised a fraction of the total funding.[76]

  It has also had some operational problems. A month after its launch, on November 13, 2015, the Gemini exchange sent emails out to its users informing them that they would be reversing trades impacted due to what was called a "fat finger" error from one of its customers.[77]

[64] http://www.coindesk.com/price-bitcoin-drops-400-btc-e-flash-crash/
[65] https://www.bitfinex.com/posts/37
[66] https://www.reddit.com/r/Bitcoin/comments/5317nu/full_bitfinex_pitch_on_bnktothefuture/
[67] https://www.bitfinex.com/law_enforcement_requests_policy
[68] http://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/
[69] https://www.bitstamp.net/article/bitstamp-first-nationally-licensed-btc-exchange/
[70] http://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html
[71] http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm
[72] http://www.coindesk.com/in-itbit-we-trust/
[73] https://bitcoinity.org/markets/list?currency=USD&span=6m
[74] http://www.coindesk.com/itbit-exodus-populating-startups-blockchain-expertise/
[75] http://www.dfs.ny.gov/about/press/pr1510051.htm
[76] https://bitcoinity.org/markets/list?currency=USD&span=6m
[77] https://www.reddit.com/r/Bitcoin/comments/3ss945/just_got_this_email_from_gemini_about_the_2200/

At the time Arthur Hayes, CEO of BitMEX a Hong Kong-based cryptocurrency exchange, explained why this set a bad precedent:[78]

> "Gemini claims to be the exchange where professional investors will buy and sell Bitcoin. The exchange will possibly be used as the market for their planned ETF. However, if the SEC is still paying attention to Gemini, this incident has stalled the approval process further. Exchanges like the New York Stock exchange have clear procedures around Clearly Erroneous Executions.[79] In the linked document, the NYSE explains exactly under which circumstances a trade can be busted due to trader error. Gemini only specifies that during a system failure trades may be cancelled. Gemini presents no guidelines on how a trade due to customer error can be cancelled. However, the Gemini terms of service explicitly state that Gemini is not responsible for trader error while trading on their platform. These inconsistencies are why many traders took to Reddit, and flamed Gemini for their decision."

The Winkdex also currently provides two more alternatives including:

- LakeBTC: is another China-based exchange that allows for the same kind of gameable practices as its larger peers in China.
- Coinbase: has received the most external funding of any cryptocurrency exchange globally. As of this writing it still has not received a BitLicense, although it has applied for one. Coinbase rebranded its Coinbase Exchange to GDAX earlier this year and its USD/BTC volume is the largest for any exchange operating in the United States. However, it was sued last year for "allegedly making false and misleading statements relating to the regulatory status of its new bitcoin exchange in New York and California."[80] Just days prior to the public announcement of the Coinbase Exchange (GDAX), the price of Bitcoin rallied largely due to insider information and trading on the knowledge that Coinbase would be launching an exchange product, separate from its wallet product. Its Chief Compliance Officer also unexpectedly left last year due to what is believed to be messaging and communication problems with regulators, investors, and customers around an investor deck that highlighted how bitcoin can be used to bypass sanctions.[81] In addition, their executives have claimed that Coinbase holds close to 10% of all mined bitcoins making it a prime target for hackers and therefore potential risk to the Winkdex in the event that the market price of bitcoins substantially rise.[82]

  Consequently Coinbase has lost several key banking relationships over the past 2 years; it was debanked from Silicon Valley Bank in the United States and also lost its access in Canada via Vogogo.[83] In terms of stability, on June 7, 2016, the GDAX experienced a "flash crash" in which the bitcoin price dropped 20% in a matter of minutes because, "The sudden drop was cause by a large sell order, which triggered a series of large stop loss orders, resulting in significant amounts of slippage."[84] In August 2016, Coinbase lost approximately $40,000 from a replay attack following an Ethereum hard fork.[85]

[78] https://blog.bitmex.com/crypto-trader-digest-17-nov/
[79] https://www.nyse.com/publicdocs/nyse/markets/nyse-arca/NYSE%20Arca%20Rule%207.10.pdf
[80] https://www.finextra.com/news/fullstory.aspx?newsitemid=26952
[81] http://freebeacon.com/issues/coinbase-exec-resigns-as-company-faces-criticism/
[82] https://medium.com/the-coinbase-blog/how-coinbase-builds-secure-infrastructure-to-store-bitcoin-in-the-cloud-30a6504e40ba#.btcx851r3
[83] http://www.americanbanker.com/news/national-regional/pot-bitcoin-companies-pay-steep-fees-for-bank-access-1073710-1.html?zkPrintable=1&nopagination=1 and https://www.reddit.com/r/Bitcoin/comments/4rpyyf/coinbase_is_losing_the_ability_to_service/
[84] https://www.reddit.com/r/BitcoinMarkets/comments/4mzhsp/what_is_going_on_over_at_coinbase_exchange_gdax/d3zrr0f/
[85] https://twitter.com/brian_armstrong/status/761974232938983426?ref_src=twsrc%5Etfw

If the COIN ETF no longer uses the Winkdex, why are all of these numbers important?

They are important because there is an observable dichotomy between price discovery and regulatory oversight in the cryptocurrency industry.

On the one hand, market making and price discovery is observably strong on platforms located outside the US. But, there is little regulatory oversight or regulatory controls for most of the large exchanges that are critical to driving the price discovery process. In fact, one of the apparent reasons for why these platforms are typically popular is because of the very fact that they do not require KYC and AML documentation. Although users are legally obliged to declare taxes on earnings and capital gains from trades, it is unlikely that many do.[86]

On the other hand, regulated exchanges in the US, including itBit and Gemini, have created corporate structures that comply with a variety of regulations, but the lion share of trading volume continues to take place off of their platforms. As a consequence, neither of these exchanges is integral to the global price discovery of USD/BTC trading.

This is important because the Winkdex used three exchanges to price the Commodity-Based Trust Shares: so if there is any problem or manipulation taking place on other exchanges, only a couple of the exchanges can be held legally liable by United States laws. Yet for pricing the market value of bitcoins, the Winkdex may not be able to accurately reflect what the global market believes a bitcoin is worth, it may only be able to price a bitcoin based on USD as traded in the US.

The reason a multi-exchange basket of prices is useful is that enables price discovery in a relatively young market. However, because the cryptocurrency market as a whole is relatively illiquid and driven by sentiments such as large vocal investors on social media, the market price can be influenced much easier than the other commodity markets.

In short, the Gemini exchange is not very liquid so their price is less likely to be as accurate as other exchanges. For accurate prices of Bitcoin, the operators should use the most liquid exchanges for the Winkdex, of which the Gemini exchange is one data feed. Yet the characteristics of price discovery and legal compliance seem to be at continual odds.

Although there has been a transition to a Daily Auction, as noted above it remains to be seen how much trading volume this attracts and how prone to manipulation it is.[87] And using different indices such as the CME CF Bitcoin Reference Rate or NYXBT would probably not be useful at this time either as the underlying basis for these feeds are essentially the same kind of unreliable exchanges detailed earlier in this section.[88]

Despite the hundreds of millions of dollars invested in cryptocurrency exchanges by venture capitalists, there are important market infrastructure and practices that are still missing including: clear oversight and governance of exchanges, robust and secure clearing and settlement of exchange-based platforms, custody function being segregated from trading, reporting mechanisms for regulatory compliance, and more.

These do not exist yet for any cryptocurrency market, and retail investors are less protected as a result.

[86] http://www.coindesk.com/the-fbi-is-investigating-a-1-3-million-bitcoin-theft/

[87] http://www.bloomberg.com/news/articles/2016-09-21/bitcoin-to-get-first-ever-daily-auctions-on-winklevoss-s-gemini

[88] The CME CF Bitcoin Reference Rate pricing data comes from the following exchanges: Bitfinex, Bitstamp, GDAX, itBit, Kraken and OKCoin.com (HK). Several of these have been hacked and/or suffered flash crashes. See: http://www.cmegroup.com/trading/cf-bitcoin-reference-rate.html

In closing, on p. 14 of the SEC questionnaire, the question is asked:

> Do commenters' agree or disagree with the assertion that Authorized Participants and other market makers will be able to make efficient and liquid markets in the Shares at prices generally in line with the NAV?

To specifically address the SEC's question: no. Based on the evidence and citations above, it is unlikely that the Gemini exchange or Gemini Trust Company can make an efficient and liquid market based on the way the current unregulated cryptocurrency exchange marketplace behaves.

Section 3: Facilitators

Short of using a particle accelerator, it is physically impossible to duplicate a gold vein or to modify the characteristics of gold – but it is entirely possible to increase or decrease the money supply of Bitcoin by changing the software code mining pools use. And, if an organization that cannot be influenced by Gemini Trust Company or the SEC controls these mining pools, without legal recourse to United States law, then the question once again is: how to protect investors in the COIN ETF? More on that in this section.

As detailed above, the COIN ETF was originally priced based on the Winkdex, which is a weighted average of market prices based on several cryptocurrency exchanges, including Gemini, a regulated exchange run by the same parent company that manages the COIN ETF.

Despite the transition to an auction, the COIN ETF is directly tied to the physical mechanics and processes of the Bitcoin network. However, Bitcoin the network itself is secured by economic incentives which can be distorted or change over time.

To fully describe the technical mechanics would fill more than a couple of pages.

Logistically the block creation process on the Bitcoin blockchain is currently, relatively centralized. That is to say, in a given day, approximately 15 miners (colloquially referred to as "pools") package transactions into blocks that constitute the Bitcoin blockchain. According to Blocktrail, over the past 6 months the 15 largest mining pools accounted for creating 97.92% of all bocks during this time period.[89]

All of the operators of these mining pools – due to how they claim and sign the coinbase transaction (also known as a "block reward") – are effectively identifiable yet not legally accountable for their actions or inactions.

On p. 13 in the SEC questionnaire, the following question was asked:[90]

> According to several commenters, there is a need for the Exchange to provide additional information regarding "proof of control" auditing, multisig protocols, and insurance with respect to the bitcoin s held in custody on behalf of the Trust, in the interest of adequate security and investor confidence in bitcoin control. What are commenters' views on these recommendations regarding additional security, control, and insurance measures?

[89] https://www.blocktrail.com/BTC/pools?resolution=6m

[90] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf

One of the learnings from the most recent Bitfinex hack is that there are probably few, if any, independently insured cryptocurrency exchanges or wallets.[91] Circle may be one of a handful with this distinction.[92]

For example, during 2014 and 2015 several Bitcoin startups claimed to have partnered with or teamed with an insurance company.[93] Others, such as Xapo which provides a Bitcoin vault and custody service, self-insured by creating their own insurance company.[94] Following the Bitfinex hack, users learned that their deposits were not insured, only the exchange's fiat was. In addition, after the hack, BitGo, which provided a multi-signature service to Bitfinex, removed its webpage explaining their insurance policy, only to un-remove it days later after users on social media pointed out its disappearance.[95]

In the case of the Gemini exchange, only fiat deposits held at a New York State chartered bank are eligible for FDIC insurance.[96] How are retail investors expected to research and learn this information without having to become cryptocurrency experts themselves?

In many jurisdictions, a cryptocurrency user currently cannot be sure that they are the lawful owner of the cryptocurrencies such as bitcoin they control, unless they have mined them or did deep due diligence on their counterpart and the chain's history because otherwise they could take possession of stolen and encumbered property.[97]

In fact, anyone using an exchange has almost no ability to control anything. The exchange operators are entirely responsible for the generation of any transaction that transfers bitcoin ownership to a customer. There is nothing to stop an exchange operator from deliberately inserting tainted dust into every such transfer.

One such example, that has become increasingly popular over the past year, is data kidnapping, commonly referred to as ransomware. While ransomware itself predates cryptocurrencies, the fact that cryptocurrencies are designed to enable censorship resistance and pseudonymity has enabled a cottage industry of malware designers whom can and do "lock down" computers belonging to hospitals, schools, police departments and other public institutions, and do so with near impunity.[98] As a result, large enterprises and institutions "plan to hoard bitcoins to help them pay cyber ransoms."[99]

To remove the "lock" on these systems, victims pay ransoms typically denominated in bitcoins.[100] These bitcoins then become proceeds of crime and make their way through some of the exchanges previously mentioned above.[101]

This leads to questions such as, are the 145 bitcoins that were recently converted through ShapeShift by The DAO attacker considered encumbered?[102] If so, how does this impact the Gemini exchange or the other exchanges that comprise the Winkdex that may hold encumbered bitcoins?

[91] https://blog.bitmex.com/youve-been-buttfinessed/
[92] https://www.reddit.com/r/Bitcoin/comments/4g8t13/are_there_any_exchanges_with_insurance_in_case/
[93] http://www.coindesk.com/lloyds-back-bitcoin-insurance-deal-elliptic-vault/
[94] https://www.reddit.com/r/Bitcoin/comments/20dolm/psa_xapo_does_not_have_the_insurance_they_claim/
[95] https://www.reddit.com/r/Bitcoin/comments/4w3w46/why_did_bitgos_blog_post_about_insurance_disappear/
[96] https://gemini24.zendesk.com/hc/en-us/articles/205823016-Are-my-funds-FDIC-insured-
[97] http://www.bna.com/ucc-bitcoins-solution-n17179924871/
[98] S. V. Solms and D. Naccache. On blind signatures and perfect crimes. Computers Security, 11(6):581–583, 1992. See also the research of Adam Young and Moti Yung: Cryptovirology: Extortion-Based Security Threats and Countermeasures. IEEE Symposium on Security and Privacy 1996: 129-140.
[99] https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms
[100] http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf
[101] https://eprint.iacr.org/2016/358.pdf
[102] http://www.coindesk.com/dao-attack-hacker-trades-funds-bitcoin/

Similarly, the popularity of MMM Global – a Ponzi scheme – over the past year involved movement in and out of bitcoins, especially through exchanges in East Asia.[103] As a result, in January 2016 multiple Chinese governmental bodies issued warnings about MMM Global and other Ponzi schemes.[104] Are the cryptocurrencies used in these schemes encumbered, and if so, did any of them end up on the Gemini exchange or those exchanges comprising the Winkdex?

Fundamentally bitcoin is not a "safe asset" because there are information asymmetries about the coin's legal progeny. Because many jurisdictions do not currently classify it as cash, it typically does not qualify under the *nemo dat quod non habet* exemption that cash does.

Bitcoins are not fungible; this is a known issue that some technologists are trying to paint over with privacy-related techniques.[105] As a result, there is a new sub-industry using data analytics to build a service for tracking a coins provenance. This includes Chainalysis, Blockseer, Elliptic, Skry, and several others that work with law enforcement to effectively track down and prosecute participants of illicit activities.

One way to visualize the interrelated nature and counterparty risks of cryptocurrency exchanges would be for the SEC to request a volume-based chart showing all of the trades into and out of Gemini that originate or terminate at all other exchanges. The data analytic companies above could provide such a tool.

The tool can provide a color-coded breakdown of the trades from exchanges that have at one point been associated with the Winkdex.

And most importantly: it can require an additional breakdown of the trading activity of volume flows between, not just the exchanges comprising the Winkdex, but also the exchanges that tie into the Winkdex exchanges.

From there law enforcement, regulators, and potential investors could see percentage wise, how much illicit activity from darknet markets such as AlphaBay move into peripheral exchanges whose assets then move in and out of the Gemini exchange.[106]

According to an August 2016 report from the RAND Corporation:[107]

> The number of transactions of illicit drugs on the cryptomarkets has tripled, with revenues doubling, since Silk Road was shut down in 2013. This is despite various law enforcement interventions and exit scams by online marketplaces, which have led to declining levels of trust between buyers and vendors, and less confidence in cryptomarkets.

In the event that law enforcement and compliance teams begin to crack down on the exchanges benefiting from the proceeds of crime, some of which could be analogous to "blood diamonds," how will this impact the trading activity and price discovery process on the exchanges comprising the Winkdex, or a second-order effect, the trading activity on exchanges that tie into the exchanges comprising the Winkdex?[108]

Gemini Trust Company cannot directly control the impact encumbered bitcoins may have on other exchanges that constitute the Winkdex, it may even be difficult for them to control for the entire

[103] http://ftalphaville.ft.com/2015/11/09/2144388/im-no-crook-declares-mmm-scamster-while-claiming-credit-for-the-bitcoin-price-spike/
[104] http://english.caixin.com/2016-01-19/100901352.html
[105] http://www.coindesk.com/fungability-bitcoin-scaling-milan-one-bitcoin-not-like-others/
[106] http://www.coindesk.com/study-finds-bitcoin-has-a-new-top-dark-market/
[107] http://www.rand.org/pubs/research_briefs/RB9925.html
[108] The Kimberley Process Certification Scheme was instituted in 2003 to combat and prevent "conflict diamonds" from entering into the mainstream diamond market.

provenance of bitcoins that move onto the Gemini exchange itself. As the *Financial Times* put it, "there are probably more people with legitimate claims over bitcoins than there are bitcoins."[109]

As noted in Sections 1 and 2, over time there has probably been in aggregate hundreds of thousands of bitcoins that have been stolen and seized, if these are categorized property and are thereby encumbered, this could lead to potential challenges for all exchanges, including Gemini.

If for some reason a law enforcement agency outside the United States requires that all bitcoin transfers between miners, exchanges, customers, and the customer's customer must take into consideration the progeny of coins, this could not only impact the price discovery process but also the mining (custody) process. In 2012, a Bitcoin Core developer named Greg Maxwell, deliberately mixed untainted bitcoins with tainted bitcoins through a mixing process called CoinJoin, to force cash-like exemptions in order to achieve fungibility.[110]

This paper will not look further at these specific legal issues, instead it will look at mining pools which appear to have a facilitator relationship with bitcoins.

To better understand this role, it is worth looking at how key custody works. One of the letters the SEC received in July regarding the Winklevoss Bitcoin ETF briefly discussed the matter of key management, key custody, and multi-signature security.[111]

While the response below will not delve into the specifics, it is clear that "multi-signature security" in and of itself is not enough to protect digital or virtual assets. In the case of Bitfinex, while the details of the heist are still thin, the operators of the exchange setup their BitGo multi-signature implementation such that it was not different than a single signature or key implementation, thus resulting in a single point of failure that was exploited.[112]

As described in the July letter, private key holders are custodians.

Miners are facilitators of transactions, they are a type of processor. The analogue today would be that a bank custodies customer's money and SWIFT is the processor. While the processor has certain powers (such as cutting off access to sanctioned countries) it cannot do everything. In this case, a processor cannot initiate a transaction – only a custodian (private key holder) can do that.

What was left unsaid is that the processors of bitcoins are, at any given transaction interval, the mining pools. Without mining pools, no transactions would be packaged into blocks and built on top of each other. While a miner cannot directly take control of bitcoins they do not themselves control the private keys of, there is a real counterparty risk that mining pools could censor the transaction or reorganize the blocks that transactions are in.[113] While users could still send valid transactions to the collective memory pool and to nodes on the network, the transactions cannot be processed and added to the blockchain without a pool. In a phrase: without miners, there is no growth in the chain of blocks.

It is commonly marketed that anyone can contribute to the mining process, that mining is free and open to the public at large. But the reality is that not everyone can add blocks to the Bitcoin blockchain, if they could, there would be no canonical record as the blockchain would be continually reorganized. Instead, the Bitcoin network like many other cryptocurrency networks, effectively gates entry-to-edit by requiring those who want to change the block order to submit a proof-of-work. And by design, not everyone can

[109] http://ftalphaville.ft.com/2015/03/24/2122678/bitcoins-lien-problem/
[110] https://coinlab.com/blog/post/coinjoin/
[111] https://www.sec.gov/comments/sr-batsbzx-2016-30/batsbzx201630-4.pdf
[112] http://hackingdistributed.com/2016/08/03/how-bitfinex-heist-could-have-been-avoided/
[113] https://www.reddit.com/r/Bitcoin/comments/2ityg2/warning_bitcoin_address_blacklists_have_been/

generate a proof-of-work that enables them to do so – only one participant roughly every 10 minutes will be able to do so.[114]

Yet just creating a proof-of-work is insufficient. It has to be a proof-of-work that the bigger miners choose to accept. A large miner or group of miners can potentially mine an alternate chain to remove your proof, at which point it is just a proof of one potential history that in fact never occurred. In fact, it is a proof that is not even officially recorded anywhere. Because mining pools can censor transactions or order them in any manner they choose, this means they can also prioritize or de-prioritorize transactions. The BTCC pool actually sells this as a service: BlockPriority.[115]

As a consequence, because it does not operate a large mining pool, both the Gemini exchange and the Gemini Trust Company are beholden to parties it cannot hold responsible or accountable for such as transaction processors operating in other countries. And this can impact the investors in the COIN ETF.

Section 4: Out-of-band attacks

In the past, the SEC has treated bitcoins or operators of Bitcoin exchanges as if they were a 'security' in several cases (SEC v. Trendon Shavers; SEC v. Garza et al.; SEC v. Sand Hill Exchange).[116] This paper will *not* touch on any specific jurisdictional definition (e.g., SEC, IRS, CFTC, FinCEN).[117]

Instead, this paper will further illustrate that mining pools at the center of cryptocurrency networks like Bitcoin are prone to external influences that are beyond the control and accountability of both the Gemini Trust Company and the SEC.

One issue no one thus far has touched on in any response letter to the COIN ETF is the effect, if any, that accumulating a fund for the purchase and storage of bitcoin will have on the otherwise volatile price of bitcoin.

In an attempt to quantify extreme tail trail risk events, a new research paper used bitcoin pricing data from between September 2013 through September 2016. The researchers found that:[118]

> We see that the value-at-risk is about five times larger than the one for the G10 currencies, again showing the substantially higher risk of Bitcoin. You can expect to lose more than 5% in one day, about once every 20 days, when you are invested in Bitcoin.
>
> […]
>
> We see that the expected shortfall is about eight times larger than the one for the G10 currencies, again showing the substantially higher risk of Bitcoin. Provided you and yourself on one of those 1-in-20 days where you can expect to lose more than 5% in Bitcoin, you will actually end up losing more than 10% on that day.

[114] http://hashingit.com/analysis/32-the-gamblers-guide-to-bitcoin-mining

[115] http://www.coindesk.com/press-releases/btcc-launches-blockpriority-service/

[116] https://www.sec.gov/litigation/litreleases/2014/lr23090.htm and http://www.coindesk.com/sec-seeks-10-million-default-judgment-against-gaw-miners/ and https://www.sec.gov/litigation/admin/2015/33-9809.pdf

[117] For regulatory and compliance purposes, there is currently no consensus within the United States regulatory community as to what bitcoins are universally categorized as. For regulatory purposes, FinCEN deems it money such that certain operators need to register as money service businesses; the IRS classifies it as property; the CFTC classifies it as a commodity. And in a recent case currently being appealed, a county judge in Florida said that bitcoins are not money. See http://www.coindesk.com/florida-files-appeal-charges-bitcoin-seller-dismissed/

[118] "A statistical risk assessment of Bitcoin and its extreme tail behavior" by Jörg Osterrieder and Julian Lorenz, pp. 11-12 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2867339

In other words, the volatility of bitcoin is already between 6 to 7 times larger than one of the G10 currencies. How can the Winklevoss Bitcoin Trust protect investors from tail risk events discussed in this section that could contribute to these sharp shifts in pricing?

In other words, will getting investors to pool their resources to take bitcoins off the market drive up the price artificially, or will there be sufficient liquidity generated by those redeeming at the back end? Or is there so much bitcoin circulating generally that the COIN ETF, no matter how successful, would not have much impact?

On p. 14 of the SEC questionnaire, the following question was asked:[119]

> A commenter notes that the Gemini Exchange has relatively low liquidity and trading volume in bitcoin s and that there is a significant risk that the nominal ETP share price "will be manipulated, by relatively small trades that manipulate the bitcoin price at that exchange." What are commenters' views on the concerns expressed by this commenter? What are commenters' views regarding the susceptibility of the price of the Shares to manipulation, considering that the NAV would be based on the spot price of a single bitcoin exchange? What are commenters' views generally with respect to the liquidity and transparency of the bitcoin market, and thus the suitability of bitcoins as an underlying asset for an ETP?

In the past, ETFs are usually set up so that only authorized participants (brokers) can redeem the underlying commodity, which tends to keep bitcoin once acquired for an ETF out of general circulation. That is not necessarily a bad thing as long as there is already plenty of supply in circulation so that the ETF's hoarding effect will have no real pricing impact. Unless we know how the market is likely to work, retail investors can easily be caught up in a bitcoin bubble that could burst like has happened multiple times in the past. What kind of insurance or hedging mechanisms does the COIN ETF have in place to protect them?

In terms of exchange liquidity, as of this writing there is roughly a nominal $10 billion collective market value of all mined bitcoins, but there is probably nowhere near $10 billion in fiat to ensure liquidity. While there have been no scientific studies on the total amount of fiat liquidity surrounding the cryptocurrency ecosystem, on any given month a large trader (e.g., a whale) is able to significantly move the market by buying or selling less than $5 million in a cryptocurrency during a trading session.

In contrast with precious metals, with gold there is a market for jewelry and for use in industrial processes. What is the market for bitcoins if the liquidity leaves and how does a lack of liquidity impact investors in the COIN ETF in the event a percentage of them attempt to simultaneously liquidate their holdings? This potential liquidation event is real, as two principals of the Gemini exchange own more than 100,000 bitcoins themselves; what happens if they try to liquidate them on Gemini or other platforms?[120]

One of the current assumptions is that by approving a cryptocurrency-focused ETF this will lead to a large inflow of institutional capital; this was even cited in the Winklevoss Bitcoin ETF S-1 as a possibility (p.11). That an approved ETF in turn would markedly increase the market value of the underlying cryptocurrency. The precedence usually cited for this are gold-related ETFs introduced during the mid-2000s such as SPDR Gold Trust and iShares Gold Trust.

If this hypothetical market price increase occurs with the COIN ETF and other proposed cryptocurrency ETFs, this will likely increase mining activity in certain regions, regions that incidentally United States

[119] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf
[120] http://www.cnbc.com/id/100635418

regulators do not have direct oversight of: specifically, the People's Republic of China and the Republic of Georgia.

Historically as the price of bitcoins increases, so does the network hashrate. However, this has decoupled a little in an era of advanced ASICs. Instead the bitcoin price impact on mining revenues is the real driver; and ultimately proof-of-work effectively is simply converting useful energy into heat and venting it into the atmosphere.[121]

For example, if the COIN ETF is approved and the market price of bitcoin increases and even surpasses its previous all-time high, this will lead to increased capital expenditures by mining farms.

And because of the recent the block reward halving, consolidation of mining activity has continued in regions where the economic conditions provide profitable incentives to set up a pool or a farm. This includes regions in China that have subsidized hydroelectricity such as Sichuan.[122] Bitcoin mining in China is dependent upon electricity subsidies and if that policy was affected for any reason, it could impact the security and price of bitcoin. Typically, the gray market for this electricity exists because there is overcapacity at a specific plant and the extra electricity is sold off, allowing local stakeholders to profit. However, if there is a crackdown, price changes in the market, or modifications to the power grid, large amounts of hashing power could go offline.

This set of economic conditions is important for providing transparency and protections for investors in the COIN ETF.

In the event that miners coordinate changes to the software code to their own benefit, such as changing the rules around the money supply, this could impact other exchanges, including those that are part of the Winkdex. What are the potential regulatory risks if large scale miners are subject to legal actions in their own country?

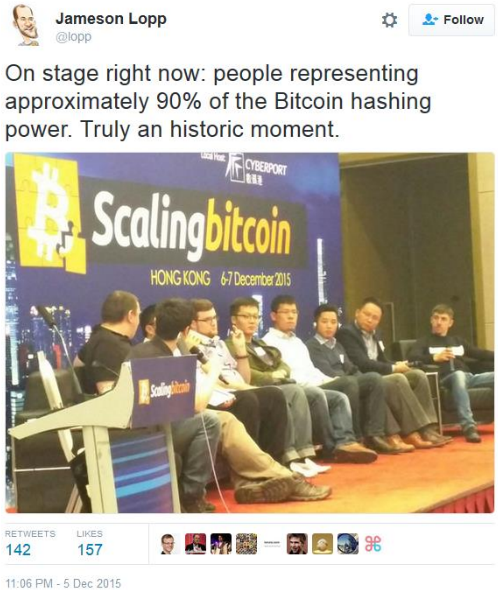
There is on-going precedence for this:

(1) Over the past year and a half, a governance and political fight has taken place within both the Bitcoin and larger cryptocurrency community over several proposed scaling solutions; this is commonly referred to as the "block size debate."[123] This involves arguing over the merits and demerits of different methods for increasing the transactional capacity of the Bitcoin network.
(2) This debate has split the Bitcoin community into at least two, maybe three discrete development groups, each of whom have lobbied the mining community, and specifically, the China-based mining community to implement or not implement certain scaling proposals.[124]
(3) There have been multiple known meetings involving large mining operators in the past:
    a. May 2014 in Shenzhen[125]
    b. December 2015 in Hong Kong[126]
    c. February 2016 in Hong Kong[127]

[121] As more countries begin to fulfill multilateral climate change pacts and agreements, the Bitcoin mining industry that exists in emerging markets may come under pressure as the proof-of-work process is environmentally unfriendly. How can the Winklevoss Trust protect investors in this edge case? See: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
[122] http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine/
[123] http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/
[124] This paper did not broach the contentious issues of active censorship and generally one-sided information streams in the cryptocurrency community. It is very hard to argue investors can be fully informed when all the primary forums and sites are systematically removing or ignoring potentially negative news. This is doubly so with the "research" that comes out of buy-side reports which is largely uncritical marketing material for various vendors and special interest groups.
[125] http://www.coindesk.com/private-china-meeting-bitcoin-mining-industry-leaders/
[126] https://news.bitcoin.com/scaling-bitcoin-workshop-hong-kong-wrap/
[127] https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff#.1ejrilfjf

d. July 2016 in California[128]
e. October 2016 in Chengdu[129]

Based on public records, neither Gemini Trust Company nor any United States regulatory body participated in these meetings, some of which were used to influence adoption roadmaps for the Bitcoin mining industry.



Jameson Lopp
@lopp

On stage right now: people representing approximately 90% of the Bitcoin hashing power. Truly an historic moment.

RETWEETS 142 LIKES 157

11:06 PM - 5 Dec 2015

Source: https://twitter.com/lopp/status/673398201307664384

As pictured above, at the December 2015 event, a now famous photo showed nine individuals on-stage that represented nearly all of the network hashrate. The majority of whom managed farms and pools operating in China.

And, at the October 2016 event, several speakers joked to the mining participants in the room, that they could successfully launch a 51% attack if they decided to.[130]

In the event of a continued governance crisis, in which one group is able to convince the mining community to support one policy versus another, how will Gemini Trust Company provide protections and guarantees to COIN ETF investors?[131] Does Gemini Trust Company have a “red phone” to contact the mining pools in the event that coordination is required to enable certain network upgrades or downgrades?

One response is that in the precious metals market it is unlikely that custody banks currently have a “red phone” to all the gold miners and all the shippers who move gold from country to country. But the key difference is that world trade could continue with or without “red phones” – cryptocurrencies such as Bitcoin are online-only.

[128] https://medium.com/@BlockByBlock/california-gathering-of-bitcoin-miners-and-devs-07-30-2016-highlights-by-tuur-demeester-9d85ec19c4e4#.wah5cuz9u
[129] https://www.reddit.com/r/btc/comments/58u8em/today_the_biggest_ever_conference_of_miners_in/
[130] http://www.coindesk.com/china-miners-big-blocks/
[131] https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

This is a critical difference in fact. Physical assets continue to exist if associated institutions fail. The cargo on cargo ships owned by Hanjin Shipping did not stop existing due to its bankruptcy in August.[132]

In the event of major network problems occur on the Bitcoin network then transactions can fail to be included. For instance, how much would a user pay to ensure that their transaction clears in the event of a hashrate halving and the price starting to decline?

This then also raises another problem: if Gemini Trust Company were able to maintain phone contact to these pools then it may be the case that other parties, including those that are not regulated by the SEC, can also influence the mining community. This includes other organizations and institutions that are not subject to United States laws.

If the price of Bitcoin does eclipse its previous all-time high due to the increase in institutional investors, governmental bodies in China may seek – as they have frequently done in peer-to-peer lending and other internet finance products – to regulate the cryptocurrency mining industry.[133] If they do, can this impact COIN ETF investors and can Gemini Trust Company provide protections to ETF shareholders?

This is not idle speculation as there is historical precedence for this. On December 17, 2013 the People's Bank of China informed domestic payment processors that they could no longer work with Bitcoin exchanges.[134] The immediate impact was the price on multiple exchanges in China dropped by 50%.[135] While enforcement of the directive loosened over the past three years, the precedence remains that governments can directly influence and impact the marketplace.

Similarly, on October 29, 2016, China UnionPay, the largest credit card provider in China, announced it would tighten regulations around how Chinese customers could buy insurance products in Hong Kong.[136] This was done as part of Chinese regulators efforts to reduce illegal capital outflows. It is naïve to think that future governmental intervention would not occur if Chinese or other authorities wanted to control capital flows, including those related to cryptocurrencies.

One response may be that governments will be unable to regulate mining because mining is supposedly decentralized and somewhat anonymous. But the reality is that since domestic energy generation in China is largely managed by entities like State Grid, third parties such as regulators are by default already keeping track of customer's identities.

In addition, many of the large professionalized miners in China have attended public events and on stage at conferences and in interviews they have told people what cities and towns their mining operations are located. Because Bitcoin mining is energy intensive, it could be relatively easy for utilities to identify who the large customers are in each city and town.

Similarly, Weixin, also known as WeChat, is a popular chat application that has over 700 million monthly active users and is actively monitored by governmental organizations and police departments.[137] If

[132] http://www.npr.org/sections/parallels/2016/09/08/493157924/container-ships-stranded-at-sea-after-south-korean-company-goes-bankrupt
[133] https://www.ft.com/content/5b179264-69e0-11e6-a0b1-d87a9fea034f
[134] http://www.forbes.com/sites/kashmirhill/2013/12/17/bitcoin-crashes-as-china-cracks-down-further-on-use/#42d017421876
[135] https://techcrunch.com/2013/12/18/bitcoin-drops-50-overnight-as-chinas-biggest-btc-exchange-stops-deposits-in-chinese-yuan/
[136] http://www.reuters.com/article/unionpay-regs-idUSL4N1CZ049
[137] http://www.techtimes.com/articles/70602/20150722/how-tight-is-internet-censorship-in-china-it-censors-wechat-even-for-harmless-rumors.htm

agencies at the national level agencies wanted to find out who, what, when, where, and how China-based miners operated, there are digital records that are retrievable by multiple authorities.[138]

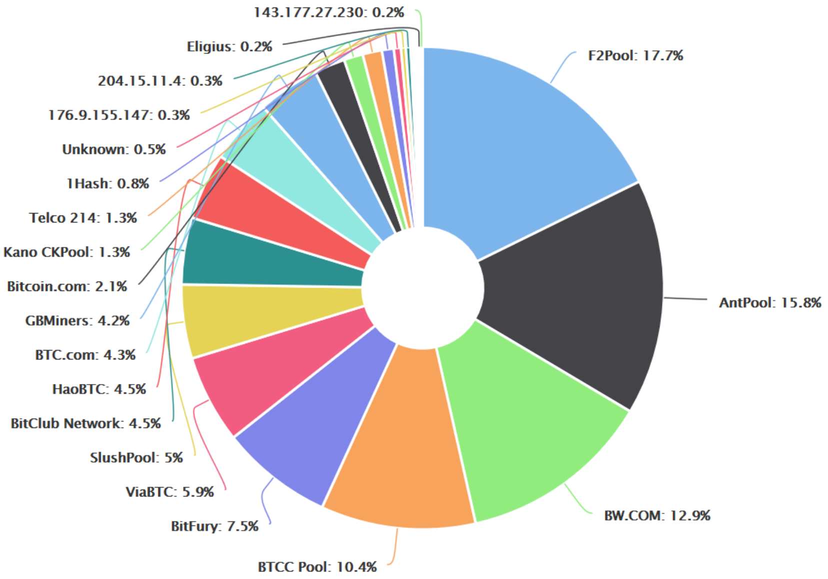
Why is this important?

Because for nearly two years, more than half of the network hashrate on the Bitcoin blockchain has originated from pools collectively based and operating in a country that the SEC has no jurisdiction over.

According to Blocktrail, for the past month, seven of the ten largest mining pools are China-based. These seven pools account for 70.93% of the network hashrate.[139] This includes F2Pool, AntPool, BTCC, BW Pool, ViaBTC, HaoBTC, and BTC.com.

It bears mentioning that just because there is potential for coordination (in this case based on geo-political identity), does not necessarily mean a fork or attack will take place. In fact, throughout the first half of 2014, GHash.io, a pool operating in Eastern Europe, accounted for more than 40% of the network hashrate – even dipping over the 50% market a couple times.[140] However, no known attack or fork took place.

Hashrate distribution by mining pool over the past 4 days



Source: Blockchain.info/pools

The *modus operandi* of miners is usually to just generate revenue. Until this past year most miners did not fund the underlying technology or seem to mind if illicit activity was taking place through their transaction processing system. Several did not publicly care about software development until their

[138] TechCrunch episode #2: "Mines and Miners" https://www.youtube.com/watch?time_continue=413&v=FtR06bIDxkE
[139] https://www.blocktrail.com/BTC/pools?resolution=1m
[140] http://www.coindesk.com/ghash-io-never-launch-51-attack/

revenue was threatened or future methods for generating revenue was potentially impacted due to the block size debate.[141]

And for the most part, this boils down to caring about the block reward itself, which currently represents about 94% of their overall revenue.[142] Note: this is another important, often overlooked issue as a recent research paper highlighted how the Bitcoin network becomes unstable without the block reward.[143]

In fact, some miners are bypassing capital controls and potentially money laundering. For instance, if you want to move money outside of any country, an operator simply needs to buy miners and invest in electrical infrastructure.

For example, in China an investor looking to bypass capital controls could:

(1) pay for miners and electricity in Chinese RMB;
(2) turn on the machines and then receive bitcoin; and
(3) then move bitcoins overseas to an exchange and reverse the process into local fiat

In this way, mining pools are – to use a phrase coined by Kenneth Rogoff – effectively partaking in reverse money laundering.[144] This is similar to the "virgin coin" idea mentioned in Section 1.

In the event that various law enforcement agencies in China decided to enforce new regulations, they have all of the necessary information to not only directly influence mining farms, but also the pools.

For instance, if the market value of bitcoins increased 10x to $6,500 due to the approval of the COIN ETF and 120,000 bitcoins were hacked and moved by an attacker as occurred with Bitfinex, what is to prevent governments globally from influencing pools to censor those movements? Or, to prevent transactions originating in the United States from being included into a block?

How can Gemini Trust Company protect COIN ETF investors in case government directed policies towards mining pools occurs? The same type of hypothetical scenario could be discussed with respect to other geographies such as the United States, not just China. There appears to be very few options and types of recourse that COIN ETF investors would have.

One of the oft mentioned use-cases for cryptocurrencies is cross-border payments and remittances. There are many articles written each year on how residents of emerging markets can utilize cryptocurrencies to bypass domestic capital controls – such as those in China – to move RMB (or in this case cryptocurrencies) across borders. At the time of this writing, aside from anecdotes, there has are no public studies that have detailed these specific payments.[145]

[141] On November 17, 2016, Bitmain and several other sponsors, announced they would jointly fund $1.2 million in software development: https://www.reddit.com/r/btc/comments/5dh14u/a_statement_from_members_of_the_bitcoin_community/

[142] https://blockchain.info/stats

[143] https://freedom-to-tinker.com/2016/10/21/bitcoin-is-unstable-without-the-block-reward/

[144] https://www.washingtonpost.com/opinions/is-it-time-to-do-away-with-cash/2016/09/21/459fa5b0-5f5a-11e6-af8e-54aa2e849447_story.html?utm_term=.bd8b0da81968

[145] Fake volume drives real volume. One way to look at this would be an analysis of the trend and the USD/RMB arbitrage value. The RMB price should be significantly higher than the USD price as BTC would be purchased in RMB and sold in USD. See also: https://www.saveonsend.com/blog/bitcoin-money-transfer/

Even if the price of Bitcoin does not increase due to the approval of a cryptocurrency-related ETF, if there is a measurable uptick in capital movement via cryptocurrencies, then Chinese regulatory authorities may act, as they have in the past when dealing with capital flows.[146]

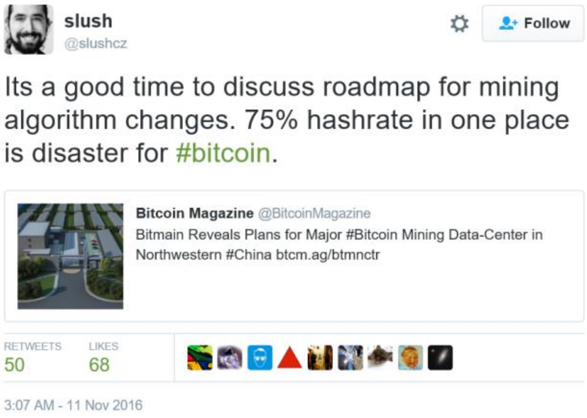
They can do this by directly influencing the operations of China and Hong Kong-based cryptocurrency exchanges one of which (Bitfinex) is listed in the Winkdex. Furthermore, the operators of LakeBTC – an alternative listed on Winkdex – are publicly known. The management teams of other popular China-based exchanges, such as OKCoin, Huobi, and BTCC are also publicly known and several have been stated that one of the use-cases for using cryptocurrencies is to bypass capital controls in China.

For all the discussion on how governments would be unable to influence or even shut down a cryptocurrency network, the evolution of China-based mining operations and exchanges has created a situation that directly impacts COIN ETF investors.

Dave Carlson, founder of MegaBigPower, one of the largest Bitcoin mining companies in the United States, recently told *TechCrunch*:[147]

> They [Chinese miners] essentially by having the majority of the mining power, they hold all the cards for whose transactions get included. That's another big one. Think about that. Think about the possibility that due to maybe a governmental ruling or something: no transactions originating in the US for bitcoin should be accepted to any of the blocks in China. That's a very scary scary concept. It should be extremely scary to the people who have invested in the businesses that are built on the Bitcoin blockchain.

While it has not been completed yet, on November 2, 2016, Bitmain announced its new Xinjiang-based 135,000 kW mining center.[148] Beijing-based Bitmain is the largest Bitcoin mining equipment manufacturer globally and will own a minority stake in the 45-room facility. When fully equipped it is estimated that this facility - based on current mining hashrate efficiencies - would account for 75% of the network hashrate. For comparison, 135,000 kW is roughly half the energy consumed by all of Google's data centers in 2011.[149]



slush
@slushcz

Its a good time to discuss roadmap for mining algorithm changes. 75% hashrate in one place is disaster for #bitcoin.

Bitcoin Magazine @BitcoinMagazine
Bitmain Reveals Plans for Major #Bitcoin Mining Data-Center in Northwestern #China btcm.ag/btmnctr

RETWEETS 50 LIKES 68

3:07 AM - 11 Nov 2016

Source: https://twitter.com/slushcz/status/797033019303464960

[146] http://www.bloomberg.com/news/articles/2016-08-17/china-crackdown-on-illegal-money-flows-sees-450-people-arrested
[147] https://www.youtube.com/watch?v=FtR06bIDxkE
[148] http://www.newsbtc.com/2016/11/04/bitmain-response-new-mining-center/
[149] http://www.nytimes.com/2011/09/09/technology/google-details-and-defends-its-use-of-electricity.html

Nine days after the announcement from Bitmain, Marek Palatinus ("slush") operator and eponym of slush's mining pool, posted the above message on Twitter. Operating from Prague, Slush's pool is the first public Bitcoin mining pool and currently hovers at around 7% of the network hashrate.[150]

If mining pools and pool software developers are able to change the type of mining (proof-of-work) algorithm used and deploy different ones, then so can well-organized and financed actors, including nation-states.

If law enforcement and regulators or those in countries where significant hashrate originates from decide to influence this market, how would this impact the COIN ETF and others that use other exchanges to provide pricing data for the Winkdex?

Section 5: Forks

The Bitcoin community continues to debate whether or not to proceed with a hard fork.[151] A fork is a change in one or more rules in the software used by miners. Those looking at a fork as potential fiduciaries – such as Bitcoin Core – believe a hard fork could negatively impact the price of bitcoins. A frequent response by groups disagreeing with the Bitcoin Core group state that developers should not act as fiduciaries; that a hard fork should be done to remove 'technical debt' even if the price declines.[152] At the time of this writing it is unclear if software developers designing and maintaining unregulated financial infrastructure such as Bitcoin are legally categorized as fiduciaries.

Another cryptocurrency called Ethereum, has had multiple hard forks over the past two years, some planned far ahead in the future, while others quickly coded and deployed in a matter of weeks.[153]

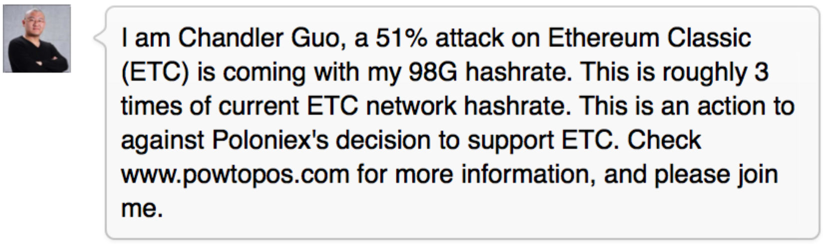
In point of fact, the Ethereum hard fork in July 2016 occurred to effectively negate the actions of a computer program called The DAO. Earlier that month an anonymous attacker, someone who is claimed to be a Byzantine actor, exploited a bug in the computer program.

During the summer, we saw different groups of Ethereum developers say 'we don't like that The DAO hacker found a bug in our system so we're going to choose to change the rules instead.' As a consequence, two Ethereum's – ETC and ETH – now co-exist side-by-side. Observationally the continued existence of ETC has reduced the value of ETH by about 10%. In addition, within a day of this fork, several exchanges such as Coinbase and Yunbi, lost thousands of dollars in ETC due to a replay attack.[154]

One of the reasons ETC gained value at all was due to cryptocurrency exchanges supporting both forks. For instance, in July 2016, Poloniex, a cryptocurrency exchange operating in Boston, announced its intention to support both forks.

As a consequence, at least one influential Ethereum miner promised to attack the fork:

[150] There were arguably "private" pools such as ArtForz.
[151] https://medium.com/@zhangsanbtc/ending-the-soft-hard-fork-debate-a-safe-hard-fork-is-the-same-as-a-soft-fork-c0e96eeb62d0#.pmu71h45s
[152] http://hackingdistributed.com/2016/04/05/how-software-gets-bloated/
[153] http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/
[154] https://yunbi.com/bulletins see July 27, 2016

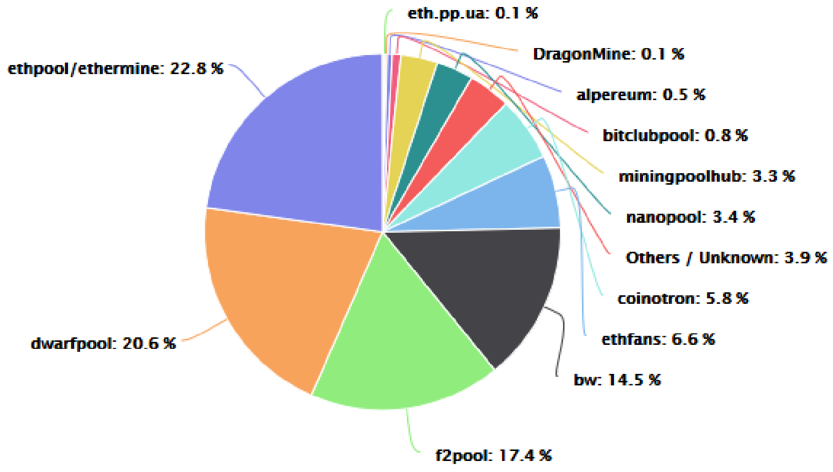


I am Chandler Guo, a 51% attack on Ethereum Classic (ETC) is coming with my 98G hashrate. This is roughly 3 times of current ETC network hashrate. This is an action to against Poloniex's decision to support ETC. Check www.powtopos.com for more information, and please join me.

Above is a public message posted on Weixin (WeChat) by Chandler Guo.[155] Guo is the co-founder of Bitbank which operates the BW Pool, currently the 3rd largest Bitcoin mining pool.[156] Bitbank also operates another BW Pool, for Ethereum, where it is currently the 4th largest. Both operate from China.

It is unclear if Chandler ever went through with the attack, as the parent company publicly distanced itself from his comments and he later began vocally supporting ETC.[157]

Hashrate distribution of Ethereum (ETH) mining pools over the past 24 hours



Source: https://etherchain.org/statistics/miners

Fundamentally, a hard fork is essentially the shortened name for '51% of the block creators producing work on what they perceive to be the valid chain.' The term "attack" is basically branding, to be more or less palatable to users. The reason why the word 'attack' cannot automatically be attached is because a malicious or Byzantine participant has just as much legitimacy to reorganize the chain as other block creators, because there are no contractual guarantees that the network will behave in a certain fashion.

That is to say, that whichever chain has the most work done on it (not necessarily the longest) is typically considered to be canonical. In fact, on November 14, 2016, ETC overtook the ETH chain to become the "longest chain" once again.[158]

[155] https://www.reddit.com/r/ethereum/comments/4ucgia/i_am_chandler_guo_a_51_attack_on_ethereum_classic/
[156] http://www.bbc.com/future/story/20160504-we-looked-inside-a-secret-chinese-bitcoin-mine
[157] http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/
[158] https://reddit.com/r/ethereum/comments/5d3kx2/etc_chain_now_longer_than_eth_congrats_etc_just/

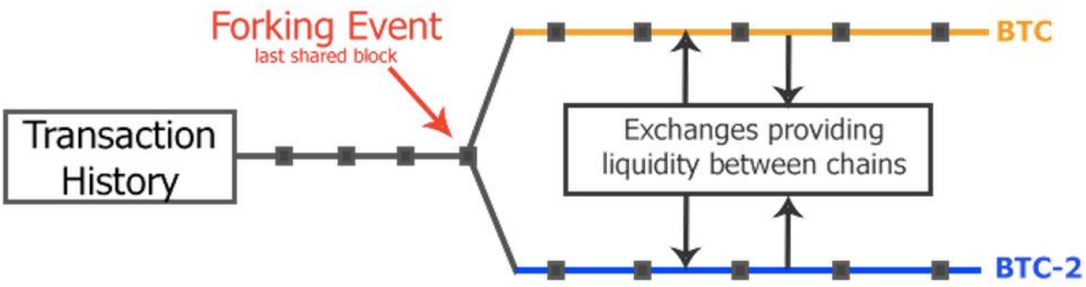
If more than 51% of the network hashrate switches and builds on top of a different chain, then the new chain deemed the canonical one due to "more work" (e.g., higher difficulty).[159] However, because there is no formal governance structure or on-chain terms of service, it is impossible to say which chain or chains is the *de jure*, legal one.[160]

What can the Gemini Trust Company and the SEC do in the case of a blockchain fork? This question is briefly discussed in the Winklevoss Bitcoin ETF S-1 on page 9.

Recently Michael Marquadt, a Bitcoin Core developer and moderator/owner of the Bitcoin subreddit, publicly suggested that:[161]

> My recommendation is that the ETF exactly specify the currency that they are going to consider Bitcoin, and be allowed to discard other currencies. Currently, the only sane way of defining a cryptocurrency is to point to specific full-node software. For example, the ETF could say that they recognize Bitcoin as the currency resulting from Bitcoin Core version 0.13.0 with SHA-256 hash [...]. Because the ETF exactly specifies the software version and hash, this does not delegate authority to the developers of this software, but it does exactly identify a unique currency. Redefining the currency may be necessary in the future and be supported by essentially the entire Bitcoin economy, so the ETF should also be able to change their software version of Bitcoin, perhaps with a 6-month advance notice to investors and possibly even an investor vote.

While he may or may not speak on behalf of Bitcoin Core itself, his remark is timely because of the actions of a mining pool based in China called ViaBTC. In the event of a fork, how will the Gemini Trust Company or SEC determine which fork is the legitimate or legal one? Is it the chain with the most work done? The chain with the backing of mining pools? The chain with the backing of Core?



The figure above, from TradeBlock, illustrates one hypothetical scenario that could play out in the event of a Bitcoin fork in which exchanges provide varying degrees of support to one fork versus the other. A similar event actually took place with the Ethereum hard fork in July 2016 and is still on-going.[162]

According to Blocktrail, over the past one month ViaBTC has generated 371 blocks, amounting to roughly 7.93% of the network hashrate.[163] The reason this number is important is because the operators of ViaBTC have publicly said they may block Segregated Witness (SegWit), a proposed change to the Bitcoin software by the Bitcoin Core group, which could be used by network participants.[164] In order for

[159] In practice a miner or group of miners would actually just need to control 33% of the hashrate to successfully attack the network and achieve what is called "selfish mining" https://arxiv.org/abs/1311.0243
[160] https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure
[161] https://np.reddit.com/r/Bitcoin/comments/57739e/bitcoin_hard_fork_poison_pill_via_etf_twitter/d8pjkr9
[162] https://tradeblock.com/blog/go-fork-yourself-life-after-a-bitcoin-hard-fork
[163] https://www.blocktrail.com/BTC/pools?resolution=1m
[164] http://www.coindesk.com/viabtc-mystery-miner-bitcoin-scaling-future/

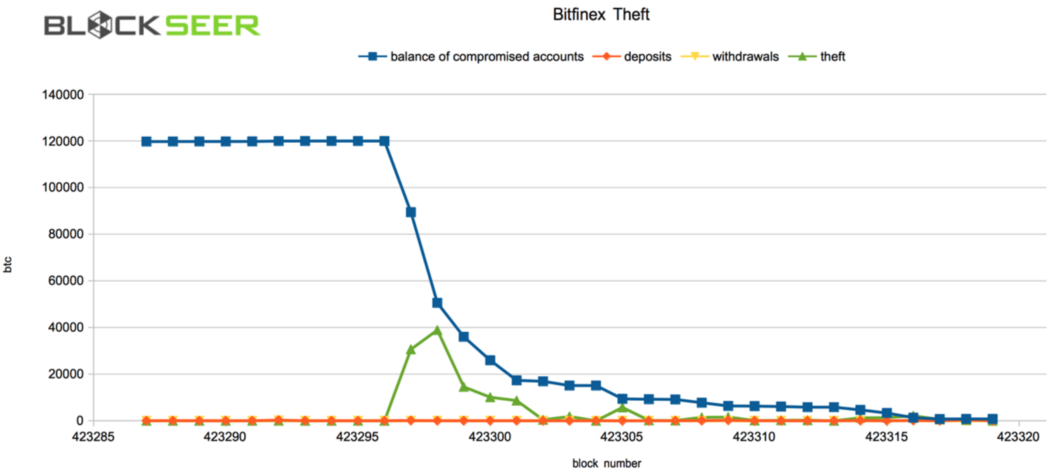
SegWit to activate, 95% of the network hashrate must adopt the proposal. Thus, in effect, with its current hashrate ViaBTC could potentially block this specific proposal.

Does this make ViaBTC legally liable in the event a fork does or does not occur?

Similarly, with the Bitfinex hack this past summer, another challenge around how to legally categorize and manage mining pools arose and how their actions or inactions could impact the investors of cryptocurrency-based ETFs.

On August 2, 2016, approximately 119,000 bitcoins (worth roughly $65 million) were removed from Bitfinex due to a hack.[165] As of this writing, the Bitfinex management team still has not disclosed how they got hacked and have published an open letter to try and negotiate with the hacker; asking to return the funds as part of an *ex post facto* "bug bounty."[166]

These Bitfinex bitcoins were, like all other transactions, sent to the network memory pool and then bundled into blocks by mining pools. They were then added to the Bitcoin blockchain. The first several pools that processed transactions containing these hacked bitcoins were (in chronological order): BTCC, AntPool, ViaBTC, AntPool, BTCC, and BW Pool.[167]



The commonality is that all four of these pools are located and operate in a country that is outside the jurisdiction of the SEC. In fact, the only non-China-based pool of the first 10 that processed bitcoins from the Bitfinex hack was Bitfury, which operates out of the Republic of Georgia.

If the COIN ETF were approved and the market value of bitcoins rises and surpasses the previous all-time high, it is conceivable that other regulators including those in China and the Republic of Georgia, begin to use data analytic tools from companies previously mentioned above, to have increased optics on network activity.

If this occurs, how does increased oversight and perhaps decision making by Chinese or Georgian regulators and law enforcement impact investors in the COIN ETF? If regulators in other countries begin to influence miners and pools like Bitcoin Core and other groups have, how could this impact investors in

[165] http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/
[166] http://www.coindesk.com/bitfinex-negotiate-hacker-stole-bitcoin-exchange/
[167] https://twitter.com/BlockSeer/status/761975450587402240

cryptocurrency-based ETFs who may not have any legal recourse or standing in the country where mining pools operate from?

One response may be that this is mere speculation, but in point of fact, in the past 4 months the cryptocurrency community has witnessed:

(1) The DAO attack[168]
(2) July Ethereum hard fork[169]
(3) August Bitfinex hack[170]
(4) ViaBTC mention it may block SegWit[171]
(5) October Ethereum hard fork[172]
(6) some of the proceeds of The DAO attack converted into bitcoin[173]
(7) November Ethereum hard fork[174]

Due to their key role coupled with the concentration of handful of global transaction processors, mining pools create a concentrated risk to all network participants. This is the reason why they are lobbied by many different parties to fork or not fork.

And in the event that miners split the network into two or more chains, this could leave the network difficulty relatively high such that no new blocks are able to be created due to the inability to generate a hash below the given target difficulty. This is a problem that has impacted alternative cryptocurrencies (altcoins) including Feathercoin before.[175] One solution proposed earlier this year by Luke-Jr, a Bitcoin Core developer, is to create a hard fork that lowers the difficult rating.[176]

This then leads to the question: if developers can directly influence how difficulty levels are adjusted, how large block sizes are, and what the money supply should be set at, then are they also a type of fiduciary?[177] Even if they are legally not categorized as fiduciaries they clearly are influential; does Gemini Trust Company plan to work with influential developers in order to protect their investors?

The takeaway is not that Chinese institutions or entrepreneurs are to blame but rather it is: organizations located outside the jurisdiction of the SEC can and will influence on cryptocurrency markets such as Bitcoin. Irrespective of the legal standing of mining pools in any jurisdiction, it is clear that the gravitational influences pools in general have on a cryptocurrency impacts all participants in an ecosystem, including investors.

Section 6: Confidence in Technology

[168] http://www.coindesk.com/understanding-dao-hack-journalists/
[169] http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/
[170] http://www.coindesk.com/bitfinex-most-user-funds-offline/
[171] https://www.reddit.com/r/btc/comments/5ddiqw/im_haipo_yang_founder_and_ceo_of_viabtc_ask_me/?compact=true
[172] http://www.coindesk.com/october-ethereum-hard-fork-network-spam-attacks/
[173] https://www.bokconsulting.com.au/blog/the-dao-hackers-booty-is-on-the-move/
[174] http://www.coindesk.com/ethereum-fourth-hard-fork-stop-blockchain-attacks/
[175] http://www.coindesk.com/feathercoin-hit-by-massive-attack/
[176] https://www.reddit.com/r/btc/comments/48nm9v/lukejr_is_proposing_an_emergency_hardfork_in_july/
[177] Influential developers such as those in the Bitcoin Core community which creates the software used by most mining pools, could impact the market value of bitcoins by modifying the money supply and/or modifying or not modifying the block size. Transitively, mining pool operators can choose which software to run and deploy, thus perhaps they too could be viewed as a type of fiduciary. Do the corporate sponsors and investors in developers and pools also have a fiduciary role? Andrew Hinkes, a lawyer at Berger Singerman, has argued that Bitcoin developers do have a fiduciary duty: http://www.coindesk.com/on-chain-scaling-bitcoin-blockchain-conference/

Another reason to reconsider approving the Winklevoss Bitcoin ETF has to do with external parties losing confidence, confidence in new, potentially transformative technology.

For example: earlier this summer The DAO -- a virtual-only, cloud-based investment fund, managing at its peak roughly $150 million -- was hacked and about $60 million of ether, the cryptocurrency which comprised both the fund and powered the Ethereum network on which it resides, was drained into a "child" fund that was controlled by the attacker.[178]

The Gemini exchange currently lists ether (ETH) in addition to bitcoin (BTC) as tradable assets. During the July Ethereum fork, the Gemini management team chose to only support the ETH branch instead of the ETC branch.[179] As future forks occur, what is the procedure that the Gemini exchange and Gemini Trust Company will follow to decide which fork to support? Will it support multiple forks? And how will it protect itself from future replay attacks that impacted its peers like Coinbase?[180]

This revelation and subsequent investigations of The DAO attack led to both a real and perceived crisis about the underlying technology: the secure transfer of digital assets via "smart contracts" on a blockchain.[181] At the time of this writing, the specific issues as it relates to Ethereum, have still not been resolved in that community as there have been multiple hard forks to fix some of the underlying problems.

A similar crisis of confidence could occur if the COIN ETF is approved and savvy attackers look at ways to exploit regulated products symbiotically tied to a largely unregulated cryptocurrency market that lacks financial controls and external auditability and accountability. And, it is the lack of controls that create an inherently risky environment for any financial product based on cryptocurrencies.

In theory, a savvy attacker could short shares of the COIN ETF and/or bitcoins held on the Gemini exchange and the exchanges constituting the Winkdex or even participate in an attack on the network; specifically an attack on a mining pool. This could come in the form of an out-of-band attack – such as the ones described above by governmental bodies – by disrupting the operating facilities and/or personnel (e.g., destroying routers, arson, kidnapping, denial of service).[182] This would be equivalent to the seizure or destruction of the crude oil pipelines and infrastructure in Cushing, Oklahoma.

The moment an attacker can extract large amounts of the fiat liquidity from the system via shorting then there is a major risk. There may be more subtle versions of the same approach that could be used to incrementally cause harm to other investors.

All of these out-of-band options are significantly cheaper than committing a direct attack on the network itself.[183] This is made possible due to the fact that these mining pool operators and many of the constituent mining farms themselves, are physically identifiable.

Similarly, zero-day exploits are usually reserved for very high value targets.[184] It is quite possible that a major increase in the market value of bitcoin could make it worthwhile for an attacker to use such an

[178] http://www.coindesk.com/leaderless-dao-put-test-following-reported-ethereum-vulnerability/

[179] https://gemini.com/blog/update-2-ether-classic-withdrawals/

[180] http://www.coindesk.com/rise-replay-attacks-ethereum-divide/

[181] http://www.kwm.com/en/knowledge/insights/smart-contracts-open-source-model-dna-digital-analogue-human-20160630

[182] http://ieeexplore.ieee.org/document/7509935/ and http://cryptohustle.com/51-attack-crew-extorts-and-hijacks-blockchains-for-ransom

[183] A direct attack is the 'classical' threat model that an attacker of a proof-of-work blockchain can and must attack via hashrate alone to overtake the chain. In reality, there are cheaper and easier ways to successfully disrupt and attack a proof-of-work chain that doesn't rely on expending much, if any, hashrate.

[184] Incidentally a common way to purchase zero-day exploits is via bitcoins: https://www.wired.com/2015/04/therealdeal-zero-day-exploits/

approach (or worse, several such approaches). Mining hardware is located on a connected network and as such just as vulnerable to attack as anything else as illustrated by the recent Mirai botnet attack.[185]

The subsequent disruption could cause a lack of confidence in the network security and reliability which could create a decline in the ETF price and/or the market price of bitcoins themselves. The attacker could then close his short and profit. The attacker could thus financially gain based on the asymmetric knowledge of when the timing of the attack(s).

In effect, the attacker could manipulate the price and there would be no legal recourse because in cryptocurrency networks such as Bitcoin and Ethereum, the miners which constitute their validation process inherently lack, by design, any terms and conditions or legal guarantees. By design, cryptocurrencies attempt to be extra-legal, sovereign entities and as such there is no insurance or customer protections in the mining process. And because there is no native KYC or AML natively integrated into the Bitcoin or Ethereum blockchains, savvy attackers could effectively launder the proceeds of the attack making recourse difficult.

If such an attack would occur, this could create a similar existential crisis for the Bitcoin community which could yet again spread to the larger blockchain technology ecosystem.

Due to the on-going education process, executives, decision makers, and stake holders at enterprises and institutions exploring blockchain technology may not fully understand the nuances of this emerging industry. As a result, they may believe the attacks on The DAO and on Bitfinex as being possible on other technology being developed by the blockchain engineering community. However, this is not the case for the companies and startups building blockchain technology that does not involve mining pools or cryptocurrencies at all.

But lacking this nuance, there could be a loss of confidence in the underlying technology at the top of institutions and organizations who have been open to experimentation thus far. If another Bitfinex hack or attack on another DAO occurs, this could make it difficult to explore the underlying technology further.

Experimentation and governance also ties into one final question that the SEC asked in its questionnaire on p. 13:[186]

> According to the Exchange, the Gemini Exchange is a Digital Asset exchange owned and operated by the Custodian and is an affiliate of the Sponsor. What are commenters' views regarding whether any potential conflict of interest or other issue might arise due to the relationship between entities such as the Sponsor, the Custodian, and the Gemini Exchange?

As noted in section 2, historically there has been a conflict of interest in cryptocurrency markets due to investors, owners, custodians, and exchange operator being all the same entity. In this case with the COIN ETF, the custodian should be a separate entity and be at least yearly independent audited to reduce conflict of interest and increase security especially since bitcoins can basically be stolen within seconds and gone forever in the worst case.

In addition, now that the Daily Auction takes place on the same exchange that the principals of the Gemini Trust Company own and control, *prima facie* it appears there could be a conflict of interest. It

[185] https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profita and https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn/
[186] https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf

should be recommended that the auction be moved to a neutral platform, or a regulated exchange in which the principals in Gemini Trust Company do not have a financial stake in.

This is not the first cryptocurrency exchange invested in by the principals of the Gemini exchange. Previously, through Winklevoss Capital, they had invested in BitInstant.[187] BitInstant was a New York-based bitcoin exchange whose CEO was later tried and pled guilty for aiding and abetting unlicensed money transmission.[188] The exchange subsequently shut down in 2013.[189]

Winklevoss Capital is also an investor in the Gemini exchange, as well as Xapo, a cold-storage provider which happens to be the official Custodian for the Bitcoin Investment Trust (GBTC).[190]As mentioned in Section 1, Bitcoin Investment Trust and its then-parent company, SecondMarket, settled with the SEC in July 2016 over a matter related to price manipulation.[191]

Managed by Greyscale, Bitcoin Investment Trust is commonly viewed as a semi-competitor to the COIN ETF. Greyscale is owned by the Digital Currency Group which has invested in multiple exchanges including several mentioned in this paper: Coinbase, Kraken, Circle, ShapeShift, and BTCC.[192] Does this interconnectedness between the two parent organizations constitute a conflict of interest?

Unless retail investors and regulators are actively researching and learning about this topic on a frequent basis, they may conflate the failures of Mt. Gox and BitInstant with the capabilities of the innovative technology as a whole.

Conclusion

For over twenty-five years, exchange-traded funds have been an innovative financial vehicle that has created and provided a new method for creating liquidity in previously less liquid markets and asset classes. Cryptocurrencies have some unique properties and utility and may one day become a legitimately discrete asset class. Yet mixing these two worlds, unregulated exchanges and unaccountable mining pools, could end up creating a new unknown, yet preventable risk that could have dramatic knock-on effects to the larger ecosystem.

While the Winklevoss Index has been replaced by the Daily Auction, the overall price of the underlying asset is still defined by a variety of precarious, unregulated businesses. This paper explored and detailed the fragility of the price of the underlying asset.

Because of its global nature, because exchanges and mining pools located outside of the United States directly determine and impact both the price of bitcoins and custody of bitcoins, the COIN ETF is also directly impacted by the decisions that are currently beyond the oversight of United States securities regulators. ETFs in practice are essentially retail instruments and as described above with respect to volume, we have a long way to go to build the right market infrastructure before we introduce and pair a popular retail instrument with a volatile cryptocurrency like Bitcoin.

[187] https://techcrunch.com/2013/05/17/with-1-5m-led-by-winklevoss-capital-bitinstant-aims-to-be-the-go-to-site-to-buy-and-sell-bitcoins/

[188] http://dealbook.nytimes.com/2014/09/04/charles-shrem-bitcoin-supporter-pleads-guilty-to-federal-charge

[189] This closure intersects with encumbrances. Tyler and Cameron Winklevoss acquired around 100,000 bitcoins during the 2012-2013 time frame. If they acquired them through BitInstant, and BitInstant was sourcing bitcoins partially through darknet markets such as Silk Road (BTCKing), are there any liens or encumbrances that transfer with the bitcoins that the Winklevoss twins now have? If these were co-mingled with the bitcoins at the Gemini exchange, how can investors be protected in the event that these encumbered assets must be untangled from untainted bitcoins?

[190] http://grayscale.co/bitcoin-investment-trust/

[191] https://www.sec.gov/litigation/admin/2016/34-78282.pdf

[192] https://angel.co/digitalcurrencygroup

Furthermore, there are no controls to hold the mining pools accountable for their decisions or disputes that may arise. Because mining pools act as the processor, validator, and clearer – their role in the ecosystem is fundamentally the most important; that is why many of the developer's lobby to influence their adoption roadmap.

Lacking transparency, auditability, and legal assurances likely conflicts with the mandate of providing a new financial product where the investor can be protected. In this case, there appears little that Gemini Trust Company can do to directly influence mining pools and farms, short of creating a regulated pool and regulated mining farm capable of generating non-negligible hashrate.

The COIN ETF attempts to create an asset class out of something that fundamentally changing and controlled by a distributed set of entities over which the SEC has no oversight. As a result, there are major risks for COIN ETF investors that need to be highlighted and addressed. If the goal is to manage risks and provide oversight, then I recommend that the COIN ETF be rejected at this time.

Acknowledgements: RB, RD, PE, DH, AL, KR, LS, JW, AW, and AY.