AOR 2014-02

MYL PAC
% Nick Staddon, Secretary
122 Pinecrest Rd.
Durham, NC 27705

Federal Election Commission
Office of General Counsel
999 E Street, N.W.
Washington, DC 20463

MYL PAC Advisory Opinion Request re. Bitcoin contributions

February 10, 2014

Dear Commiseioners:

Please accept this request on behalf of Make Your Laws PAC, Inc. (MYL PAC) for an advisory opinion from the Federal Election Commission (FEC or Commission), pursuant to 11 CFR 112.1(a) and 2 USC 437(f).

Background

In the Commission's recent open meetings about AO 2013-15 Conservative Action Fund, the Commission indicated informally that it believes that PACs may accept Bitcoins (BTC), but could not agree on *how* they may do so. Without such guidance, we are concerned that if we accept Bitcoin, we may inadvertently violate the FECA, as there is no safe harbor policy that we can currently follow to ensure compliance.

We[1] intend to solicit contributions using Bitcoin (as one of many payment methods for our contributors' convenience — e.g. PayPal, credit card, etc.), as well as to make payments for goods and services using Bitcoin. We ask for the Commission's approval of our framework below, which we believe strikes a good balance on the sensitive issues involved in this matter. Of course, other approaches might also satisfy the FECA; what we propose is only one.[2]

We request that, If the Commission approves this AOR, it do so with a sunset provision limiting

[1] "We", "us", and "our" in this document refers to MYL PAC.

[2] We understand that a formal rulemaking may also address this issue at some point; in the interim, we suggest that approving our proposed method would provide PACs with a basic "safe harbor" policy.

the validity of the AO until the December 31, 2015, so that we may all revisit these issues in the light of more information on its usage in practice as well as any advancements in Bitcoin's technical capabilities or regulatory regime.

A short technical primer on Bitcoin

Bitcoins are not actually a thing or number that is "transferred" from one computer to another; rather, Bitcoin uses a kind of universal account ledger. The Bitcoin system has *addresses* (which identify a public key[3]; anyone with access to the associated *private* key can control that address, much like a bank password); *transactions* (which authorize the transfer of Bitcoins to whoever can prove they control a given public key); and *blocks* (which form the public history of the Bitcoin network by authenticating the previous block, any other transactions its miner wants to, and one transaction of 'new' Bitcoins that the miner gets for creating the block).

Bitcoins originate from a Bitcoin miner, in an amount and rate given by the Bitcoin protocol (currently 25BTC / block and 1 block every ~10 min). Bitcoin users sign transactions, and miners include those transactions in the public blockchain, all using public key cryptography. The *transactions* are transferred among the peer-to-peer network of Bitcoin users.

Anything that is included in a block (i.e. all transactions and all public keys that have been designated as receiving Bitcoins) is public knowledge. A Bitcoin user's "wallet" stores the *private* keys of a set of Bitcoin addresses (and a ledger of its transactions & current "balance" for user convenience), thus enabling the user to control whatever amount of Bitcoins that the history of previous transactions have credited to the associated *public* key.

It is simply by tracing the *entire* transaction history from its very beginning (i.e. dead reckoning) that everyone knows how many Bitcoins every address "owns". And while Bitcoin *transactions* are public, the *transactors* are not identified by *anything* other than by a cryptographic public key. The various methods for laundering Bitcoins try to ensure that even the public transactions do

[3] http://en.wikipedia.org/wiki/Public-key_cryptography. Even more technically, a transaction can designate things other than a Bitcoin address as ways to prove that one is allowed to control the output of a transaction (and this is how future improvements on Bitcoin are built, that would eg designate a "refund" address or "contracts"), but currently, a Bitcoin address is the overwhelmingly most common mechanism.

not reveal *actual* underlying exchanges of ownership.

Bitcoins do not have serial numbers. A transaction can be for any increment of 0.00000001 Bitcoins. *Transactions* have ID numbers that are public.[4]

A Bitcoin user can control any arbitrary number of Bitcoin addresses. Many transactions transfer Bitcoins between multiple addresses simultaneously; there is no way to distinguish "which" address gave to which recipient. There is no easy way even to know reliably what set of Bitcoin addresses are controlled by a single person (without using sophisticated network traffic analysis — and even then, the conclusions are generally fuzzy at best).

Because transfers of Bitcoin are made based *only* on the authorization of the sender, not the receiver, it is not possible to "screen" or refuse an incoming transaction. Once the transaction to your Bitcoin address is signed by the sender and incorporated into the public blockchain, it is public knowledge that you own those Bitcoins, regardless of your consent.

Because the blockchain does not store IP addresses, and a computer *transmitting* a given transaction is not necessarily operated by the the user *initiating* that transaction, it is not possible to know the country of a Bitcoin user without doing sophisticated network traffic analysis.[5] Most Bitcoin clients have built-in support for the Tor anonymizing network,[6] which makes tracing the true source of a network request to its owner's IP more or less impossible.

Legal, policy, and technical issues with PAC use of Bitcoin

1. *Bitcoin's value in US dollars is easily determined by its trading price on major online markets at any time.*

Bitcoin is bought and sold using currency on several major online markets (e.g. MtGox, Bitstamp, BTC-e) as well as through various Bitcoin transaction intermediaries (e.g. Coinbase

[4] E.g. http://blockexplorer.com/t/6DxJkqkhnP

[5] See http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011 for an in-depth technical discussion by Dan Kaminsky, one of the leading experts in computer security. This is an evolving area, with techniques being developed on both sides. However, it cannot be reliably traced to a real human by an auditor of ordinary technical skill vs someone using even moderately good precautions for anonymity.

[6] https://www.torproject.org/about/overview.html.en

and BitPay), which typically use whichever high-volume market offers the best price.[7] Any sufficiently active market between Bitcoin and currency (such as US dollars) effectively determines the value of Bitcoin at any moment, just as with any other commodity market.

2. *Bitcoin transactions can be made untraceable, and attributing Bitcoin contributions is inherently problematic.*

Bitcoin transactions cannot easily be traced.[8] There are no centralized, authoritative records of who owns what Bitcoin address, as there are with a "Know Your Customer" compliant bank having a record of who owns every account. Knowing that a given Bitcoin transaction comes from a specific person depends primarily on asking them and just trusting their response.

The standard method that Bitcoin merchants use to attribute incoming Bitcoin transactions to a given user is to create a distinct Bitcoin receiving address owned by the merchant that is disclosed to that user (a "linked address"). When *anyone* sends Bitcoins to the linked address, the merchant credits the associated user's account. It is impossible to prevent third parties from anonymously sending Bitcoins to a linked address if they know what it is, and the user can easily disclose their linked address to third parties if they want. Furthermore, if it receives any Bitcoins, the linked address automatically becomes *public* knowledge by being published in the Bitcoin block chain.

For most merchants, this is not a problem; they don't care *who* pays them, so long as *someone* does. However, PACs have a duty to take reasonable steps to ensure that contributions they

[7] E.g. https://bitpay.com/bitcoin-exchange-rates

In 2013, 1 Bitcoin traded from a low of ~$13 to a high of ~$1242 on the MtGox USD exchange.

[8] The block chain is public, and in that sense, all transactions are publicly traceable. Bitcoin users can still remain extremely difficult to identify, using techniques specifically designed to *prevent* the nominally transparent public block chain from revealing real underlying transactions or ownership. (Bitcoin users are technically *pseudonymous*, not *anonymous*, but we use 'anonymous' in the FECA's legal sense.)

This is an evolving area of cryptography. There have been recent presentations within the security community about ways to counteract attempts at Bitcoin anonymity — e.g. by Kay Hamacher & Stefan Katzenbeisser: http://www.mdpi.com/1999-5903/5/2/237, http://youtube.com/watch?v=hlWyTqL1hFA.

Given the substantive national policy issues that are affected, we feel that the FEC should take a conservative approach to Bitcoin accounting — and that our approach does so.

receive originate from the person to whom they are attributed.

3. *Bitcoin requires special methods to fulfill 'best efforts' recording of transactions, contributor identities, etc.*

PACs are required to make a "best effort" to identify contributors, not to do so with absolute certainty. They are however *also* required to take reasonable precautions to deter unlawful activity, especially if they know something is liable to abuse. We believe that Bitcoin-specific means are needed to record transactions and provide some assurance of contributors' identities to fulfill this "best effort" standard. We detail such means in our proposed framework below.

We do not currently address or ask what we should do if we receive a Bitcoin contribution outside of our proposed framework, e.g. if we receive an anonymous Bitcoin contribution sent directly to a Bitcoin address we do not publish, or if we are the target of certain kinds of technically sophisticated malicious Bitcoin activity. We intend to ask the Commission for guidance on such matters when a specific scenario arises.

4. *It is de facto infeasible to transact in Bitcoin without paying anonymous Bitcoin miners (very small) transaction fees in Bitcoin.*

In order for any Bitcoin transaction to be effective (including, for example, a transfer of someone's own Bitcoins to a Bitcoin exchange like MtGox for conversion to USD), it must be included by a Bitcoin miner in a new block. Miners are anonymous. As a *de facto* matter, miners refuse to do this unless they are paid a small amount of Bitcoin, called a "transaction fee"[9] — typically on the order of 0.0001 Bitcoins. This fee is nominally optional, but in practice it is not; the size of the fee determines the priority with which a transaction will be finalized, and zero-fee transactions won't usually be processed.

In order for anyone to actually use Bitcoins, they *must* pay such Bitcoin-denominated fees to anonymous third parties. Therefore, the Commission should permit PACs to do so, so long as

[9] https://en.bitcoin.it/wiki/Transaction_fees

the transaction fee is paid at the standard rate. We also suggest that such transaction fees need be reported only in aggregate.

5. *Certain expenditures are more sensitive than others, which affects what medium of exchange may be appropriate for their use.*

Certain expenditures by a PAC, such as administrative / overhead expenses, employee salaries, and general goods & services (such as server costs, website design, food, and travel), are not particularly sensitive from a policy perspective. Although Bitcoin is significantly harder to trace than currency exchanges, we believe that such expenditures should be permitted to be made using Bitcoin, as doing so would encourage innovation and efficiency.

Other expenditures, such as independent expenditures, contributions to other committees, solicitation, advertising, polling, transfers, loans, candidate appearances, or political contributions, are more sensitive. Because of the very high public stake in the transparency and auditability of such expenditures, we believe that they should only be made using more traceable means of payment (such as US dollar denominated bank transfers, checks, etc).

MYL PAC's proposed framework for Bitcoin usage[10]

1. *MYL PAC's receipt of Bitcoins as contributions*
   a. MYL PAC will consider all contributions of Bitcoins to be in-kind contributions.
   b. MYL PAC will *only* accept Bitcoins through an online form designed specifically for the purpose, and will *not* accept "physical" Bitcoins.[11]
   c. MYL PAC will require *all* Bitcoin contributors, *regardless* of the proposed contribution amount, to provide their name, address, occupation, and employer.
   d. MYL PAC will require *all* Bitcoin contributors to explicitly affirm that every Bitcoin contribution attributed to them originates solely from Bitcoins owned by them (or jointly by the contributor and their spouse).
   e. When required by law, MYL PAC will refund Bitcoin contributions from fully identified contributors *only* in US dollars, based on the value at the time of contribution.
   f. MYL PAC will *only* accept Bitcoin contributions through a one-time-only linked address, which is only disclosed to the linked contributor *after* all information, affirmations, and consents that MYL PAC requires are obtained from them.
      i. MYL PAC will *not* publicly list any Bitcoin addresses it owns.[12]
   g. MYL PAC will not *directly* accept Bitcoins from any political committee, but may accept committee contributions of US dollars *derived from* liquidating Bitcoins.
   h. MYL PAC will *not* accept Bitcoins or Bitcoin-*derived* contributions from any 501(c)4.
   i. All of the above apply to *both* MYL PAC's contribution and non-contribution accounts.

2. *MYL PAC's direct buying and selling of Bitcoins*
   a. MYL PAC will not mine Bitcoins.
   b. MYL PAC will *only* buy or sell Bitcoins on an open, high-volume exchange (or a functional intermediary thereof, such as BitPay or Coinbase).
   c. MYL PAC will report its buying or selling of Bitcoins as a conversion of held assets to/from held currency. MYL PAC will *not* consider such trade at fair market value a contribution or disbursement, but only a transfer of assets from one form to another.

[10] This only states MYL PAC's own proposed policy for Bitcoin usage, and is not intended as a FEC "rule".

[11] See e.g. https://www.casascius.com or https://bitcoinpaperwallet.com

[12] However, it is technically inevitable that MYL PAC's Bitcoin addresses *will* be public knowledge to anyone with the technical skill to investigate the Bitcoin block chain, or if disclosed in a public FEC report.

d. MYL PAC will deposit proceeds from its Bitcoin sales into a depository account within 10 days of their liquidation to USD and availability for transfer.[13]

3. *MYL PAC's accounting of Bitcoin transactions*

a. MYL PAC will maintain a record of

  i. every Bitcoin address (including lihked addresses) it has owned

  ii. for all Bitcoin transactions MYL PAC is party to: the Bitcoin addresses involved, date/time, Bitcoin block chain transaction ID, and BTC-USD exchange value at the time

  iii. additionally, for all Bitcoin contributions made through the 1(f) linked address system: the linked address and identity of the contributor linked to it

MYL PAC will make the above information available to FEC auditors under the same conditions as would apply to an audit of any other records that could disclose contributors' private financial information.

b. MYL PAC will value Bitcoin:

  i. for Bitcoin-denomihated contributions and expenditures: at the trading price at the time closest to receipt / disbursement on MYL PAC's usual Bitcoin exchange

  ii. for purchase and sale: at the actual purchase or sale price in US Dollars

c. MYL PAC will separate its Bitcoin assets in the same way it separates any other assets, like bank accounts — e.g. contribution vs non-contribution, federal vs non-federal, etc.

d. MYL PAC will treat any appreciation or depreciation of value between acquiring and liquidating Bitcoin identically to the appreciation or depreciation of stock, bonds, or other investments.

  i. Appreciation or depreciation of value will not affect tne value assigned to a contribution or expenditure (which is valued at the time of that transaction, as above).

e. MYL PAC will pay Bitcoin miners normal transaction fees (in Bitcoin).[14]

[13] This may be delayed by circumstances outside of our control — e.g. if an exchange or intermediary has temporarily restricted MYL PAC's accounts, has a longer than 10 day transfer-to-bank sweep time, requires a minimum payout for settlement that is not yet met, etc.

[14] Currently, normal transaction fees are ~0.0001 BTC per transaction (worth ~$0.10), depending on the size of the transaction involved (in bytes, not amount of Bitcoin) and the number of transactions being processed.

f. To the extent that MYL PAC requires the cooperation of any Bitcoin transaction intermediaries it uses to comply with these policies, it will have some agreement with them to do so (either by contract or as part of their standard terms of service).

   i. MYL PAC may delegate some of the above accounting to intermediaries, just as it delegates the tracking of check transaction records to banks and credit card transactions to PCI-compliant credit card processors.

4. *MYL PAC's disbursement of Bitcoin for non-sensitive expenditures*

   a. MYL PAC will use Bitcoin directly to pay for administrative / overhead expenses, employee salaries, or general goods & services (such as server costs, website design, food, paper, and travel).

   b. In disbursing Bitcoins for goods or services, MYL PAC will accept any discount offered by the provider thereof on an equal basis to non-political entities.

5. *MYL PAC's disbursement of Bitcoin for all other expenditures*

   a. MYL PAC will *not* directly disburse Bitcoins for independent expenditures, contributions to other committees, solicitation, advertising, polling, transfers, loans, candidate appearances, political contributions, etc., and will instead first liquidate Bitcoins to US dollars before disbursement for such purposes.

Questions presented

Assuming that MYL PAC acts in accordance with our proposed framework above:

1. May MYL PAC receive Bitcoins as an in-kind contribution?

2. May MYL PAC purchase and sell Bitcoins?

3. May MYL PAC disburse Bitcoins?
    a. May it do so with Bitcoins it received as contributions as well as purchased Bitcoins?
    b. May it accept ordinary discounts offered by providers?

4. How should MYL PAC report all of the above?

Conclusion

After we received requests from multiple people interested in contributing to us via Bitcoin, we began discussing this matter with the Bitcoin Foundation, the Cryptocurrency Legal Advocacy Group[15], the Bitcoin community, state candidates accepting Bitcoin, and others over a year ago, to carefully assess the legal, policy, practical, and other issues involved in Bitcoin-based political contributions.

We believe that, in principle, Bitcoin *should* be permitted as a means of political contribution. Bitcoin is a useful and evolving new medium of exchange, and permitting its use would encourage technological innovation. We would like to accept Bitcoins so as to better serve our contributors, and we believe that technologically sophisticated approaches to campaign finance have the potential to be of great benefit to the public.

However, given the serious policy issues that must be considered and protected in the Commission's ruling on this matter, we believe a careful balance must be struck that protects those policy issues while permitting reasonable receipt and expenditure of Bitcoin.

Our proposal above is intended as a conservative safe harbor policy; it errs on the side of caution, providing as much auditability as is technically possible for Bitcoin while conforming as closely as possible to both the letter and spirit of existing FEC regulations, without requiring any new rulemaking. It leaves some questions open (such as how to handle unwanted anonymous Bitcoin contributions) that may be better addressed in the context of a specific situation.

If you have any questions or comments, please do not hesitate to contact me at sai@makeyourlaws.org or +1 (717) 469-5695.

I request the Commission's permission to appear at any meeting on this matter remotely, as I am unable to appear in person. I would prefer to appear via video conference if possible.

Sincerely,
/s/ Sai
President & Treasurer
Make Your Laws PAC, Inc. (MYL PAC)
FEC ID # C00529743

[15] http://theclag.org