FEDERAL ELECTION COMMISSION
Washington, DC 20463

MEMORANDUM

TO: The Commission

FROM: Commission Secretary's Office

DATE: November 20, 2013

SUBJECT: Comments on Draft AO 2013-15
(Conservative Action Fund)

Attached is a comment received from Jacob S. Farber and Ezra W. Reese on behalf of the Bitcoin Foundation. This matter is on the November 21, 2013 Open Meeting Agenda.

Attachment

Perkins Coie

Jacob S. Farber
Ezra W. Reese
PHONE: (202) 654-6268
FAX: (202) 654-9951
EMAIL: JFarber@perkinscoie.com

700 Thirteenth Street, N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.654.6200
FAX: 202.654.6211
www.perkinscoie.com

November 20, 2013

BY EMAIL: AO@FEC.GOV
BY FAX: (202) 208-3333 AND (202) 219-3923

Ms. Shawn Woodhead Werth
Office of the Commission Secretary
Federal Election Commission
999 E Street, N.W.
Washington, DC 20463

Re: Further Comments on Advisory Opinion Request 2013-15 (Conservative Action Fund PAC)

Dear Secretary Werth:

The Bitcoin Foundation submits these further comments ("Further Comments") regarding the Advisory Opinion Request (the "Request") filed by the Conservative Action Fund PAC ("CAF") on August 15, 2013 concerning the acceptance of bitcoins as federal political contributions. We respectfully request that the Commission to extend the deadline for their consideration. The Bitcoin Foundation previously filed comments on the Request on September 16, 2013 ("Bitcoin Foundation Comments"), and generally will not repeat the points made there. Instead, the Bitcoin Foundation is providing these Further Comments to address certain points raised during the Commission's discussion of the Request at its November 14, 2013 open meeting. The Bitcoin Foundation also wishes to reiterate its view that the Commission need not and should not categorize bitcoin contributions as either "money" or "in-kind" contributions, and therefore should adopt alternative Draft B or C as its Advisory Opinion.

The Bitcoin Foundation notes that during the open meeting, Chair Weintraub expressed interest in having an expert on Bitcoin provide the Commission with further input on the technical aspects of Bitcoin. The Bitcoin Foundation hopes that these Further Comments will assist toward that end. The Bitcoin Foundation is the leading association serving the business, technology, government relations, and public affairs needs of the Bitcoin community. The Foundation's members include many of the major companies and other entrepreneurs in the

Bitcoin space. Its staff and guiding committee members include Bitcoin core developers and prominent members of the Bitcoin community.

I. DISCUSSION OF THE TECHNICAL POINTS RAISED BY THE COMMISSION

A. *Bitcoin Transactions, Transparency and Privacy*

During the Commission's meeting, several Commissioners raised questions about the extent to which bitcoin contributions could be made anonymously. Those questions stemmed at least in part from the apparent tension between the Bitcoin Foundation's description of Bitcoin transactions as transparent and easily viewed and analyzed,[1] and the observation that Bitcoin users can choose whether to reveal their identity when conducting transactions.[2]

We explain below why those two characterizations of Bitcoin transactions are not in fact in opposition and are both true. In any case, Bitcoin contributions are no more or less anonymous than other forms of contributions. As with contributions made by text message, or in-kind contributions of goods or services, campaigns can control the terms on which they accept contributions made in bitcoins, and thereby avoid the receipt of prohibited contributions. Specifically, they can reject attempted contributions from donors who have not provided the necessary identifying information.

As the Commission itself noted in its draft opinions, its approach to donations by text message provides the model for its treatment of bitcoin contributions. In both cases, the only public information about the donor is an identifier—a phone number in the case of text messages, and a public address (referred to as a "public key") in the case of Bitcoins. Nothing inherent in the transaction ties that public identifier to a personal identity, yet the Commission did not regard that as a reason to disallow text message contributions. Instead, the Commission authorized donations up to specified levels without the provision of any identification information. Above those levels, the Commission required text message donors to provide the necessary personal information and attest to its authenticity. There is no reason why bitcoin contributions should not be treated in the same way. As with text messages, campaigns can require the provision of and attestation to personal information as a prerequisite for the acceptance of donations above the allowable limits for anonymous contributions.

Seen from this perspective, bitcoin contributions are really no different than other types of contributions in which the transfer mechanism does not inherently identify the donor. Consider a donor who wishes to donate $1,000 worth of gold nuggets. There is nothing inherent in the transaction that ties the gold nuggets to the identity of the donor. Yet a campaign may clearly

[1] *See* Bitcoin Foundation Comments at 5.
[2] *See* Bitcoin Foundation Comments at 6.

accept the donation, so long as it obtains and maintains the information from the donor necessary to ensure compliance with federal election law.

If anything, bitcoin contributions are preferable to other forms of contributions because they can in every case be immediately returned if necessary, by simply initiating a transaction sending the received bitcoins back to the donor's public key address. This is true even for donations made in amounts below the thresholds for the required provision of personal information. Unlike, for example, donations made by text message, where the sender's mobile number does not provide the campaign with the information necessary to return the contribution, every bitcoin contribution can always be returned.

Moreover, as discussed in the Bitcoin Foundation Comments, the block chain—the publicly viewable ledger collectively maintained by the computers on the Bitcoin network that contains every Bitcoin transaction ever made—records the public keys of both the sender and the recipient. The block chain thus enables anyone to trace the history of every bitcoin in existence from the present back to the date when it was first created.[3] (Or, more accurately put, since bitcoins exist only as entries in the block chain, the transaction history contained in the block chain for each bitcoin *is* the bitcoin.)

A simple example may help to illustrate the block chain mechanism. Assume that a particular miner is the first to verify a batch of Bitcoin transactions[4] and to add the transactions as a new "block" in the block chain. That miner receives a reward of a set number of bitcoins—currently 25—as the reward for having expended the computing power necessary to verify the block. That award of bitcoins is included as a transaction in the block, and is thus reflected in the block chain. That transaction record shows the new bitcoins as now belonging to the miner's public key. (Again, more accurately put, the record of the bitcoin value added to the miner's public key *constitutes* the new bitcoins.) The addition of the new transaction block to the block chain serves to confirm that the included transactions—including the transaction awarding 25 bitcoins to the miner—took place and, by virtue of the time-stamp included along with the block, when they took place.

Now assume that the miner wants to send 10 bitcoins to a friend. To do so, the miner would send a message to the other computers on the Bitcoin network announcing the transfer of 10 bitcoins from the miner's public key to the recipient's public key.[5] Once that transaction is verified and thus included in a new block added to the block chain, any user can see that 10

---

[3] New bitcoins are awarded to the Bitcoin users (called "miners") who verify Bitcoin transactions to incentivize them to perform that work. Thus, the so-called "mining" process functions both to verify Bitcoin transactions and as the mechanism by which new bitcoins come into circulation.

[4] The verification of the transactions is a perquisite to their being added to the block chain..

[5] This process is automated by the Bitcoin software. From the sending user's perspective, it generally requires no more than providing the public key of the recipient and the amount of bitcoins being sent.

bitcoins were transferred from the miner's public key to the recipient's public key. As a result, the recipient is now reflected as the owner of the 10 received bitcoins, and the miner is reflected as still owning the remaining 15 of the 25 bitcoins awarded to the miner.

Assume next that the Bitcoin user who received the 10 bitcoins from the miner wishes to purchase merchandise from an online seller that costs .5 bitcoins.[6] At checkout, the user would initiate a transaction on the Bitcoin network to transfer .5 bitcoins to the merchant. Once that transaction is verified and included in a block, the block chain will reflect the transfer of the .5 bitcoins to the merchant, and the sending user would continue to be reflected as the owner of the remaining 9.5 bitcoins. And, since every transaction recorded in the block chain contains a link back to its predecessor transaction, any Bitcoin user could see that the .5 bitcoins reflected as having been sent to the public key owned by the merchant were sent from the public key of a bitcoin user who had previously received 10 bitcoins from the public key belonging to the miner.

Thus, Bitcoin transactions are uniquely public and transparent. No other financial system includes a record of every transaction made that any member of the public can view and analyze. As explained in the Bitcoin Foundation Comments and discussed in Section I.B below, this makes bitcoins especially well-suited for making political contributions.

At the same time, Bitcoin transactions are also private in the sense that the block chain reflects only the public key addresses of bitcoin senders and recipients and does not reflect the private identity of the owners of those public keys. This is necessarily the case, as few users of any financial system would want their identity tied to a public record of every transaction they ever made. One of the fundamental innovations in the Bitcoin protocol is the separation of public key addresses from personal identities. The existence of public key addresses makes it possible to maintain a public transaction record and to thus enable the verification of transactions by users—which in turn is what allows the Bitcoin protocol to operate on a peer-to-peer basis without the middleman necessary in every other financial system to verify transactions. It is this elimination of the middleman, and the fact that users can transact directly with one another, that makes Bitcoin so revolutionary: it eliminates nearly all of the costs and friction inherent in other financial systems, making it possible for users anywhere to transact nearly instantaneously and at essentially no cost. This privacy is one of the key enabling features underlying the Bitcoin protocol.

Still, there is nothing in the Bitcoin protocol that prevents the disclosure of identifying information by Bitcoin users. Just as with any other financial system, Bitcoin users are free to identify themselves as the owner of their public key addresses to the extent they choose to do so. Senders (e.g. buyers or donors) can choose whether—and to what extent—to personally identify themselves. Some users opt to do so, and many users publish their public keys. In fact, unless a

[6] The Bitcoin protocol provides for the divisibility of bitcoins to 8 decimal places.

user reveals their public key, there is no way any other user could send bitcoins to them. Equally importantly, nothing requires a recipient to accept bitcoins from an unidentified sender. Instead, as with any other financial system, recipients (e.g. businesses or political campaigns) can determine how much identifying information to require from senders (whether buyers or donors) as a prerequisite to transacting in Bitcoins. For example, if an online merchant accepts bitcoins, it can opt to do so only from users who have created an account and provided their name and address and any other information deemed necessary by the merchant.

Political campaigns are no different in this regard. They can reject contributions from those who do not provide the personal information required by FECA. This is true regardless of how bitcoin contributions are received. If bitcoins are received through the mechanism contemplated by the Request, a third-party provider would accept the bitcoin contributions on the campaign's behalf via a web-based platform. That third-party provider would collect the necessary personal information and would provide that information to the campaign. If a potential donor refused to provide the information required by the campaign, the third-party provider would not accept the donation. A campaign could also operate such a web-based platform on its own behalf. Alternatively, a campaign could simply make public a bitcoin public key address for donations, and require the provision of accompanying personal information above the required thresholds. There are numerous mechanisms by which a campaign could accomplish this, including requiring potential donors to pre-register their public key(s). While nothing would prevent a Bitcoin sender from initiating a donation transaction without doing so, or in amounts in excess of permissible limits, the campaign would simply return all such contributions via a reverse transaction to the sender's public address.

Technologies are being developed that will make it even easier for campaigns to ensure that they comply with donation limits. For example, so-called deterministic public keys enable the creation of an essentially unlimited number of private addresses that in essence sit behind a single public key. The use of such keys would enable campaigns to allow the transparency inherent in receiving donations via a published address while enabling the use of separate addresses to track every individual donor, or even every donation.

B. *Auditing Bitcoin Contributions*

Questions were also raised at the open meeting about how the Commission could audit bitcoin contributions. As discussed above and explained in detail in the Bitcoin Foundation Comments, the block chain contains a record of every Bitcoin transaction ever made. The Commission—and for that matter, any user on the Bitcoin network—can see every donation made to each campaign. This provides an incredible public resource for tracking contributions. For example, the total amount of Bitcoin contributions reported by a campaign would be easily verifiable, as would the number of reported donors. While the identity of the donor is not necessarily discernible from the block chain itself, the Commission could easily tie the information available

in the block chain to the information reported and maintained by campaigns concerning donors in order to verify the campaign's reports.

Bitcoin is still in its infancy, and bitcoin contributions are likely to constitute a very low percentage of total donations, at least initially. As it has done with credit card contributions, the Commission can move forward now with the acceptance of bitcoin contributions, and develop and refine its auditing and verification requirements over time, as the volume of bitcoin contributions scales, and specific issues present themselves.

If the Commission believes that the Bitcoin Foundation can be of assistance in this regard, the Bitcoin Foundation would welcome the opportunity to provide input.

II. DISCUSSION OF DRAFTS A, B AND C

The Bitcoin Foundation notes that Drafts B and C released by the Commission differ from the initial draft Advisory Opinion circulated by the Commission in that they omit any finding that Bitcoin contributions do not meet the definition of "monetary" contributions, and therefore must be "in-kind" contributions. Instead, both Drafts B and C reach that same outcome by simply stating that Bitcoin contributions will be treated for practical reasons in the same manner as in-kind contributions.

The Bitcoin Foundation strongly urges the Commission to adopt Draft B or C rather than Draft A. As discussed in the Bitcoin Foundation Comments, the Bitcoin network and protocol enable transactions that have characteristics of both monetary and in-kind contributions. The Commission should therefore avoid defining Bitcoin contributions as one or the other. By instead simply treating Bitcoin contributions in the same manner as in-kind contributions, the Commission can defer making an unnecessary decision until the record warrants it and the need arises.

Taking this approach would avoid the possibility of prejudicing the ongoing consideration of the regulatory status of Bitcoin and digital currencies in general by other federal agencies. In addition to FinCEN, agencies such as the SEC and the Commodities Futures Trading Commission have either addressed Bitcoin-related questions or have said that they are considering whether they have jurisdiction over Bitcoin. Since the Commission need not rule on how bitcoins should be categorized, it should avoid the risk of muddying the consideration of Bitcoin by other federal agencies.

We appreciate the Commission's attention to these views.

Very truly yours,

Ezra W. Reese

Jacob S. Farber
Ezra W. Reese