Subject: File No. SR-CboeBZX-2019-004
From: SAM AHN

This is my eighth comment on bitcoin, and the previous ones are at the following links:

1st 08/13/18 https://www.sec.gov/comments/sr-cboebzx-2018-040/srcboebzx2018040-4206251-172835.htm
2nd 08/16/18 https://www.sec.gov/comments/sr-nysearca-2017-139/nysearca2017139-4221685-172898.htm
3rd 08/17/18 https://www.sec.gov/comments/sr-cboebzx-2018-001/cboebzx2018001-4226785-172988.htm
4th 08/21/18 https://www.sec.gov/comments/sr-nysearca-2018-02/nysearca201802-4240462-173003.pdf
5th 08/28/18 https://www.sec.gov/comments/sr-cboebzx-2018-040/srcboebzx2018040-4274529-173133.pdf
6th10/16/18 https://www.sec.gov/comments/sr-cboebzx-2018-040/srcboebzx2018040-4530331-176071.pdf
7th10/29/18 https://www.sec.gov/comments/sr-cboebzx-2018-001/cboebzx2018001-4581773-176242.pdf

All my comments, including this one, are somehow related to intrinsic value. The purpose of this one is to urge the SEC to ask a question to the applicant of SR-CboeBXX-2019-004.

First, I found SR-CboeBZX-2019-004 at the following link:

Link 8: https://cdn.cboe.com/resources/regulation/rule_filings/pending/2019/SR-CboeBZX-2019-004.pdf

Second, I boldface and underline three words in Quote 1 below:

(Quote 1)

SR-CboeBZX-2019-004
Page 52 of 132

Bitcoin miners do not need permission to participate in verifying transactions. Rather, miners compete to solve a prescribed and **complicated mathematical calculation** using computers dedicated to the task. Rounds of the competition repeat approximately every ten minutes. In any particular round of the competition, the first miner to find the solution to the mathematical calculation is the miner who gains the privilege of announcing the next block to be added to the blockchain. (Quote 1)

Third, the question: What is "**complicated mathematical calculation**" in Quote 1 like?

Fourth, why we need a good answer to the question

If this application gets approved by the SEC, some of us the public would consider investing in bitcoin-based securities. We would make decisions based on the belief that bitcoins were produced through complicated mathematical calculations. If the three words are true, there could be some value in bitcoins. For example, bitcoin miners may have expanded the horizon of mathematics and bitcoins are given in compensation for such a contribution to mathematics. If there is no complicated mathematical calculation, we would be making decisions based on wrong information.

Fifth, examples of acceptable answers:

The applicant's unequivocal statement that there is nothing that can be considered complicated mathematical calculation can be an acceptable answer. Withdrawal of this application itself can be one, too.

Sixth, an example of unacceptable answers:

The wording “complicated mathematical calculation” works like a moat around the castle of bitcoin mining, keeping us away from the reality of bitcoins. The applicant would most likely reinforce the moat, by saying “the answer is already given” and indicating a part of SR-CboeBZX-2019-004, e.g. something like Quote 2 below:

(Quote 2)

SR-CboeBZX-2019-004
Page 113 of 132

Bitcoin was first described in a white paper released in 2008 and published under the name “Satoshi Nakamoto”, and the protocol underlying bitcoin was subsequently released in 2009 as open source software. (Quote 2)

This the least acceptable.

Seventh, why the most likely answer is unacceptable:

I visited the “white paper” at the following link:

Link 9: https://bitcoin.org/bitcoin.pdf

And found something about the mining procedure, as Quote 3 below:

(Quote 3)
4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002. (Quote 3)

While quoting the above, I brought “Note 6” from the last page of the white paper onto the quoted text, for easier reading of my readers. In conclusion, it is all about hashing. If this “hashing” is what “complicated mathematical calculation” truly means, the three words phrase in question is a grand exaggeration and terrible misrepresentation.

We can find together the reason why I say it. Let’s look up hashing Technopedia at the following link:

Link 10: https://www.techopedia.com/definition/14316/hashing

Hashing is explained as Quote 4 below:

(Quote 4) Hashing is generating a value or values from a string of text **using a mathematical function**.

Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.

Hashing is also a method of sorting key values in a database table in an efficient manner. (Quote 4)

We do use a **mathematical function** during hashing, so the two words "mathematical function" remind us of **"complicated mathematical calculation"** in Page 1 of this letter. The problem, however, is that it is not the miners who use the mathematical function. There are no mathematical pains taken by the miners.

Let's find what it is to use the mathematical function while "hashing," by "hashing" it together.

Google "SHA-256," which is indicated in Quote 3 above.
And get into an SHA-256 algorithm such as the one at the following link:

Link 11: https://www.movable-type.co.uk/scripts/sha256.html

There are two boxes, one titled "Message" and the other "Hash." When you input something in the Message box, you get a 64-digit string, called hash, in Hash box. Now, input a1a1a1a1a1a1. Then, you will get the following hash:

Hash 1: 0dd8eb6c33ca722306c10073edfc2d9662ed0d3803f46cf26a174cb12ad4639e

In that specific tool, the same input will always produce the same hash. The miners repeat this, with different inputs, until they get a 64-digit hash starting with prescribed number of zeroes, which is about 16 zeros. The miners use huge computer facilities to input billions of Messages into the Message box, consuming huge amount of electricity, until they get a right hash. That is mining. It is neither complicated nor mathematical. The complicated mathematical algorithm is already given in the program running in the computer facility. What miners do is just waiting.

Now, it is a good time to evaluate the quality of the white paper. What Satoshi wrote in Quote 3 above, for the procedure of hashing shown above, is:

"scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits."

Here in this complicated sentence,

"Scanning" means searching for a right input that produces a new hash starting with many zeros.
"SHA-256" means the algorithm that produces a 64-digit hash each time you input something.
"a number of zero bits" means about 16 zeros at the beginning of a new hash.

Satoshi's sentence structure is unusual, the core technical terminology is extremely simplified, and the phrase "zero bit" is not a correct expression of what it really means.

Look at Hash 1 (redded) above. It starts with a zero. Satoshi called it “zero bit.” If the whole string of 64-digit is made up of zeroes and ones only, we would understand what a “zero bit” means. When one digit is expressed with one bit only, the bit can be valued either 1 or 0. The digit valued zero can be called a zero bit. However, have a look at this:

(Quote 5) A cryptographic hash (sometimes called ‘digest’) is a kind of ‘signature’ for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. (Quote 5)

Quote 5 is what is written at the top of Link 11 above. It says that one hash of 64-digits requires 256 bits. It means that one digit in the string of 64 digits is 4 bits. Calculation: 256 bits divided by 64 digits is 4 bits/digit. The term for 4 bits is a half byte or a nibble. A nibble can express, in a digit, one of 32 characters. Therefore, the first digit of Hash 1 is not a bit – not a “zero bit.”

Next, I quote the whole text of the white paper’s Abstract.

(Quote 6) Abstract.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. (Quote 6)

The abstract is all about transfer of bitcoins. Nothing is mentioned about mining. But Quote 3 above is about mining. The white paper is not an honorable document.

The white paper cannot teach how Bitcoin Network really works. The ones in the network learned how to mine bitcoins peer-to-peer, not through the white paper. I believe the white paper was created independently of the knowledge transfer process, perhaps for the purpose of pretending openness.

Besides the white paper, we know that one bitcoin is 100 million Satoshis. This indicates that the writer in the name of Satoshi followed Chinese traditional system of four-digit progression. A myriad(=ten thousand) is 萬 (pronounced ‘wahn’ in Chinese and same ‘mahn’ in Koean and in Japanese), and a myriad times of it is 億 (pronounced ‘ee’ in Chinese, ‘ehk’ in Korean and ‘oku’ in Japanese). Bitcoin-Satoshi system reveals that little efforts were exerted to make it easier for global use.

And the writer did not spend enough money to make the write paper understandable.

Eighth, how to find intrinsic value

Some bitcoin supporters say that bitcoin does have intrinsic value.

Link 12: https://hackernoon.com/money-the-debate-of-intrinsic-value-cd6ab8e4c4df

But some finds a way to equate bitcoin with US dollars in the "absence" of intrinsic value.

Link 13: https://www.wired.com/story/bitcoin-has-no-intrinsic-value-neither-does-a-dollar1-bill/

My argument about intrinsic value in the previous comments of mine, listed at the beginning of this one, can be summarized like the box below:

(My Argument 1) Assets can be classified into three kinds, according to the way intrinsic value is carried. (1) Gold, pot soil or the like carries its own intrinsic value with itself. (2) Something representing some another thing, such as a common stock certificate and a gold certificate, carries its intrinsic value in the one it represents. (3) A debt instrument's intrinsic value is carried in the "promise" written in the instrument. The risk level depends upon the reliability and financial soundness of the promiser.

Federal Reserve Act clearly states that a Federal Reserve note is a US government obligation, meaning it is a debt instrument. We have heard the Fed saying the same. Unfortunately, European Central Bank's website has a text meaning a paper Euro does not have intrinsic value. But it is the problem with the writer, not with the truth. Money does have intrinsic value, and the value deteriorates if the issuer is either not reliable or (promiser) not financially sound. We recognize intrinsic value in all things just because they can be exchanged for money. It is nonsensical to say that money does not have intrinsic value. (My Argument 1)

My Argument 1 refutes Link 13 above. Whether Link 12 above makes a little sense substantially depends upon how "complicated mathematical calculation" is explained. If the wording "complicated mathematical calculation" means nothing other than getting a new 64-digit "hash" staring with about 16 zeroes, then Link 12 above cannot stand.

(My Argument 2) The concept of intrinsic value can be better understood when bitcoin is compared with gold. Bitcoin is not a debt instrument. Bitcoin does not represent anything physical or productive. Therefore, bitcoin must carry its intrinsic value, if any, like gold does. And bitcoin supporters often compared bitcoin to gold.

Gold value varies depending on situations, but gold is gold for the number of electrons per atom. However, the same rule does not go with a string of 64-digits, with about 16 leading zeroes, like this:

Hash 2: 000000000000000000c10073edfc2d9662ed0d3803f46cf26a174cb12ad4639e

As Hash 2 has 18 zeroes, it could be a successful hash if hashed within the network of Bitcoin. When hashed outside of the network, or when not hashed but just written, it is nothing. Again, gold has its value, low or high, everywhere, only if there are 79 electrons in each atom. With as many as eighteen zeroes, Hash 2 is nothing because I wrote it outside of the network instead of hashing it inside the network. This is the stark difference between gold, which does have intrinsic value, and bitcoin, which does not. (My Argument 2)

Ninth, why intrinsic value is important

When it is made clear that bitcoins do not have any intrinsic value, as in My Argument 2 boxed at the end of Page 4, the last resort for this applicant might be an argument that currencies have no intrinsic values while the SEC has approved currency-based ETF's. That's why I had to write My Argument 1.

In general, the intrinsic value of something tangible is recognized for its the market prices. If the SEC has approved currency-based EFT's by utilizing this logic, it is not easy for the SEC to deny the same logic from utilized for bitcoin-based ETF's. Everything has its beginning and its end. It is a time for the SEC to start developing the concept of intrinsic value, for this decision and future decisions. My Argument 2 is my two cents

We the public has the right not to see something that represents pieces of "the blue sky" listed for trading in a prominent exchange. We are neither Canada nor Switzerland. We have the SEC, Securities Act of 1933, Securities Exchange Act of 1934, 18 USC 486, and US Constitution.