Subject: File No. SR-CboeBZX-2018-040
From: SAM AHN (3rd at this file number)

This is my sixth comment on bitcoin. The first one was put at SR-CboeBZX-2018-040 (right here) on 08/13/2018, the second at SR-NYSEArca-2017-139 on 08/16/2018, the third at SR-CboeBZX-2018-001 on 08/17/2018, the fourth at SR-NYSEArca-2018-02 on 08/21/2018, and the fifth right here again on 08/28/2018. All my writings including this revolve around intrinsic value.

Satoshi Nakamoto intended to create a new currency and a new payment system, but the new currency bitcoins are being traded like securities and the payment system Bitcoin Network has degenerated into a decentralized Ponzi scheme. While explaining it, this writing happened to be a long one. In fear of not being read at all, I enumerate some of what the readers can find herein, as below:

1. It is not stated in the bitcoin whitepaper that a new currency would be created.
2. A new currency was defined differently than it was illustrated, in the whitepaper.
3. Cryptocurrency was defined a chain of signatures, meaning blockchain, in the whitepaper.
4. Mining means attempting to get 64-digit codes beginning with 16 to 18 zeroes.
5. One success of mining was entitled to about 50 bitcoins for 4 years from 2009.
6. One success of mining will be entitled to about 6.25 bitcoins for 4 years from 2021.
7. The definition in 3 above is contradictory to the facts in 4 through 6 above.
8. Satoshi Nakamoto looked not knowing what "bit" means, within the whitepaper.
9. The math bitcoin advocates are proud of is just this: $S=a/(1-r)$, a high school formula.

SEC Release No. 34-84231 called for comments on 18 issue groups. This comment would belong to the 11th of them, reading:

> (Quote 1) 11. What are commenters' views on the cost and the efficiency of arbitrage across the various global markets for bitcoin? What are commenters' views generally with respect to the liquidity and transparency of the bitcoin market, the bitcoin markets' susceptibility to manipulation, and thus the suitability of bitcoin as an underlying asset for an ETP? (Quote 1)

Out of Quote 1, I pick the underlined part -- transparency problem that leads to price manipulation of the bitcoin market. Transparency in relation to price manipulation usually means information asymmetry involving insiders' hiding of some information from the public. In the case of bitcoin, the problem is difficulty of understanding what is already disclosed. Said problem can be called knowledge asymmetry. For example, the high school formula shown above is simple to money-related experts but unknown to most bitcoin advocates. The world of bitcoin is so full of murk, hiding numerous cases like that.

The arcaneness of Bitcoin Network and bitcoins can be best viewed in the original proposal of SR-CboeBZX-2018-040. Quote 2 below is what appears in SEC Release No. 34-83520 of 06/26/2018.

> (Quote 2) A bitcoin is (1) an asset that can be transferred among parties via the Internet, but without the use of a central administrator or clearing agency. The term "decentralized" is often used in descriptions of bitcoin, in reference to bitcoin's lack of necessity for administration by a central party. (2) The Bitcoin Network (i.e., the network of computers running the software protocol underlying bitcoin involved in maintaining the database of bitcoin ownership and facilitating the transfer of bitcoin among parties) and

the asset, bitcoin, are intrinsically linked and inseparable. Bitcoin was first described (3) 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)

I underlined and numbered three parts. The underlined (2) insinuates that a bitcoin is a security. The key word that makes a bitcoin a security is "inseparable." The Bitcoin Network does many things including limiting the total minable number of bitcoins to about 21 million. See "(7) Predetermined number of coins" under Quote 9 below, for the calculus. The 21 million bitcoins are 21 million shares of one integral system, as each bitcoin is "inseparable" from Bitcoin Network.

A Ponzi scheme is defined by the SEC as "an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors." Whether the Bitcoin Network is a Ponzi scheme depends on whether there is no other way for bitcoin investors to enjoy gains than inducing more investments into it.

The applicants of SR-CboeBZX-2018-040 suggested, as in Quote 2, Satoshi Nakamoto's bitcoin whitepaper at the underlined (3) above. In other words, Satoshi's whitepaper alone can show us another way mentioned in the preceding paragraph. Therefore, whether Bitcoin Network is a Ponzi scheme depends on what is written in the whitepaper.

Ideally, the bitcoin ETF applicants should have told us what is written in the whitepaper, as an alternative to inducing more investors into Bitcoin Network. They didn't do that, and defined bitcoin as in the underlined (1) above: "asset," the broadest term anybody can think of. Now the task of deciphering the whitepaper is left on the shoulders of the public. So be it.

Money creation in Satoshi Nakamoto's whitepaper

Satoshi Nakamoto's white paper is at this link: https://bitcoin.org/bitcoin.pdf. Quote 3 hereunder is the whole text of its Abstract.

(Quote 3) A purely peer-to-peer version of electronic cash (1) 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 (2) using a peer-to-peer network. The network timestamps transactions by hashing them into (3) an ongoing chain of hash-based proof-of-work (4), 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 (5) 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 3)

It took me a long time to comprehend the above. I want to share my understanding with the readers, on the five points I underlined and numbered.

The underlined (1) means cash transfer system, not just "cash." (2) means check bounces for NSF. (3) would be closer to its meaning when the whole underlined part is replaced with just one word "in."

The underlined (4) looks meaning blockchain in this Abstract, but it will mean confirmation of successful mining, too, later under subtitle of "Proof-of-work." I will show it in Quote 5 below. A successful mining means getting a 64-digit code with 16 to 18 zeros at the beginning. Mining is just wasteful, automated repetition of simple data entry. Human effort required for it is just clicking one button and waiting.

The underlined (5) "nodes" have now been split into "full node wallets" and "lightweight wallets." There are about 11 thousand full node wallets and over two million lightweight wallets in Bitcoin Network. The holders of lightweight wallets do not participate in the verification system of the network. They rely on the bitcoin "exchanges" for verification of bitcoin blocks. The bitcoin exchanges are now working as "trusted third party" in the third line of Quote 3 above. Weird.

With the advent of lightweight wallets and bitcoin exchanges has substantially compromised Satoshi's original intention for a peer to peer payment system. Bitcoins have been developed or degenerated into securities. The bitcoin advocates have almost forgotten the fact that bitcoin was created as a currency. They may need to forget it. The applicant of SR-CboeBZX-2018-040 did not assert that bitcoin was a currency.

Even Satoshi did not say in the Abstract that a currency was being created. We can find the first smack of a new currency later under "2 – transactions," reading:

(Quote 4) We define an electronic coin as a chain of digital signatures. (Quote 4)

This sentence looks attempting to define bitcoin, and we can rephrase it to "We define bitcoin as a currency made up of a chain of digital signatures." Satoshi was creating a new currency, without indicating it in the Abstract.

Satoshi meant in Quote 4 above that bitcoin was a chain of digital signatures. A chain of signatures, or a blockchain is, however, not bitcoins as assets but the payment system. In another part of the whitepaper, bitcoins can come into being with a success of mining. Satoshi starts "4. Proof-of-work" with explanation of mining, this time without the word mining or mine, as follows:

(Quote 5) 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. (1) The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. (2) (Quote 5)

As is throughout the whitepaper, Satoshi's wording in Quote 5 is difficult to understand. The underlined (1) had better be changed to "looking for an input value which SHA-256 hashes into a 64-digit code beginning with a number of zeroes," for everybody's understanding. What is truly meant by Quote 5 is that one batch of new bitcoins is recognized mined, when something like one of the two examples below is produced at a "hashing."

000000000000000000012494ddcfb91d3968b2ea4d2dd55e0d94b23c6eb1f11cf8
0000000000000000000f84021d63f8e21e9bcb5ac28b78b9e7ae292b726891896

The second example has one more zero than the first one. With these examples, we can understand the underlined (2), too. It means "becomes exponentially difficult if just one more zero is required. When the required number of zeroes is achieved, it can be verified by just one more hashing."

Hashing is a kind of code generation. A hashing engine called SHS-256 always generates 64-digit codes like the above, no matter what "nonce" is input. You can test it by googling with SHA-256 and entering an arbitrary word in the box. What you enter is called "nonce" in the world of bitcoin, to mean "a number that will be entered only once during mining. There are numerous successfully generated 64-digit codes at the link below:

https://block.bitbank.com/poolblocks/btc/1499356800

Digital signing is easy, but mining takes substantial waste of resources. If you invest in bitcoin, you are joining the waste party of mining. See who are major miners now, at the link below:

https://www.buybitcoinworldwide.com/mining/pools/

In Quote 5 above, we find the amazing fact that Satoshi Nakamoto did not know the meaning of "bit" in computer science. One bit can express one of just two things, typically zero and one. One digit in the world of bitcoin mining cannot be expressed with one bit. Usually, it is one byte that can express one digit of such a code. One byte, which is eight bits, can express one of 256 different numbers and characters. The name SHA-256 reminds that one byte can express 256 different things. Had this concept been clear to Satoshi, bitcoin would have been named Bytecoin instead.

We have found that Satoshi did not know, or pretended not knowing, the meaning of 'bit' in computer science. Then, did Satoshi have a good knowledge required for creating new currencies?

Satoshi first defined bitcoin as a chain of digital signatures. Considering the mining process, however, bitcoin is rather something that can be obtained through proof of a 64-digit code that has been newly hashed with SHA-256, with many zeros at the beginning digits, plus a chain of digital signatures, also hashed with SHA-256.

Three elements observed in new currency creation in history

We can retrieve from the history of money creation at least three elements, of which goodness determined soundness of the new currency. There may be other important elements, but the following three would be enough to criticize bitcoin as a new currency candidate.

(List 1) Elements of correct process of money creation
Element 1: Bearer of the burden to secure the value of the new currency
Element 2: Means of value maintenance
Element 3: Initial valuation (in terms of gold, other currency or some other reference)
(List 1)

For better understanding of the elements above, I am taking nine examples: Gold coins of 1792, State Bank Notes from 1836, Confederate States Dollars of 1861, Demand Notes of 1861, Legal Tender Notes of 1862, National Bank notes of 1863, Federal Reserve Note of 1913, Federal Reserve Note since 1971 and US copper coins.

Money creation example 1: Gold coins of 1792

Two months before Kentucky was admitted to the Union as the 15th state, Coinage Act of 1792 took effect with the following features:

Element 1. Bearer of the burden: US Mint
Element 2. Means of value maintenance: Redemption with gold
Element 3. Initial valuation: 10 dollars = 247.50 grains (about 16 grams) of pure gold

This system worked quite well, until gold fell short of demand.

Money creation example 2: State Bank Notes from 1836

Missouri, the 24th state, was established in 1921. There was no new state for the next 15 years. In 1936, the Battle of Alamo occurred and two new states (Arkansas and Michigan) were born. The year was a new start of incorporation of new states. The Union did not have enough gold to support ever-increasing demand for liquidity. The state-chartered banks started to issue bank notes, with the following features:

Element 1. Bearer of the burden: Issuing Banks.
Element 2. Means of value maintenance: Belief in the issuing bank.
Element 3. Initial valuation: Face value in US dollar.

It is said that some 1,600 state-chartered private banks issued paper money. But some issuing banks went bankrupt, weakening Elements 1 and 2 together. During the Civil War, the state bank notes disappeared, and two central governments started to issue paper money.

Money creation example 3: Confederate States Dollar (the Greyback) of 1861

Element 1. Bearer of the burden: Treasurer of the Confederate government
Element 2. Means of value maintenance: Winning the war and confiscating Union gold.
Element 3. Initial valuation: Face value in US dollar.

Element 2 is my reading of the issuer's mind. It evaporated together with the Confederate's loss of the war. The value of money deteriorated rapidly according to the growing prospect of defeat. At end of the war, Element 1 disappeared together with the Greyback.

Money creation example 4: Demand Note of 1861

Element 1. Bearer of the burden: The Treasury of the United States of America
Element 2. Means of value maintenance: Redemption with gold coin.
Element 3. Initial valuation: Face value in US dollar.

This was a perfect money. If the war had gone wrong, however, Element 1 could have disappeared. The Confederate could have confiscated all the gold, sending value of Demand Notes to zero.

Money creation example 5: Legal Tender Note (the Greenback) of 1862

Element 1. Bearer of the burden: The Treasury of the United States of America
Element 2. Means of value maintenance: Winning the war and confiscating Confederate gold.
Element 3. Initial valuation: Face value in US dollar.

Element 2 is my reading of the issuer's mind. The Union did confiscate Confederate gold various ways. But the Union did not directly use the gold to make the Greenback better. Under Gold Standard Act of 1900, the Greenback became as good as gold coins.

Money creation example 6: US National Bank notes of 1863

During the war time, the government needed more and more cash. Cash was linked to gold, and they were afraid of expansion of issuing the Greenback, which was not linked to gold then.

Borrowing money on interest was probably more comfortable under real bills doctrine, in that the bond buyer's assessment of the bond value looks like a real value of the bond. When the government wanted to sell the new bonds, however, the buyers did not have enough cash to pay for it. The solution was allowing national banks to issue bank notes up to 90% of the government bods they hold. Then, the government can receive that money for the price of the bonds and spend it for the war. The difference between the more Greenback issuance and this new method was more government debt, which is due to interest expenses on the bonds being issued, but this could be the price for the comfort of remaining under real bills doctrine.

Element 1. Bear of the burden: Issuing national banks and Office of the Comptroller of the Currency, which is a part of the Treasury.
Element 2. Means of value maintenance: The issuing banks' obligation to hold ample US debt instruments and some gold and/or lawful money.
Element 3. Initial valuation: Face value in US dollar.

Its value stayed good because, I think, the Union won the war.

Money creation example 7: Federal Reserve Note of 1913

Federal Reserve Notes were created as debt instruments under Section 16 of Federal Reserve Act in 1913. Said section is now sitting in the Federal Codes as 12 USC 411, as follows:

(Quote 6) Federal reserve notes, to be issued at the discretion of the Board of Governors of the Federal Reserve System for the purpose of making advances to Federal reserve banks through the Federal reserve agents as hereinafter set forth and for no other purpose, are authorized. The said notes (1) shall be obligations of the United States and (2) shall be receivable by all national and member banks and Federal reserve banks and for all taxes, customs, and other public dues. They (3) shall be redeemed in lawful money on demand at the Treasury Department of the United States, in the city of Washington, District of Columbia, or at any Federal Reserve bank. (Quote 6)

I numbered and underlined three parts, each of which matches each element of List 1 above in the same numerical order.

The word 'obligation' in the underlined (1) means indebtedness. If the reader has any doubt about this interpretation of mine, then read 18 USC 8:

(Quote 7) The term "obligation or other security of the United States" includes all bonds, certificates of indebtedness, national bank currency, Federal Reserve notes, Federal Reserve bank notes, coupons, United States notes, Treasury notes, gold certificates, silver certificates, fractional notes, certificates of deposit, bills, checks, or drafts for money, drawn by or upon authorized officers of the United States, stamps and other representatives of value, of whatever denomination, issued under any Act of Congress, and canceled United States stamps. (Quote 7)

Paper money in circulation is being recorded as a debt item in the book of the Fed. Compare this practice with how coins are accounted for in "Money creation example 9: US copper coins" below.

A note is the possessor's asset while the issuer's debt. The possessor gets the same amount of nominal value and intrinsic value. The government gets the same negative amount of nominal value and intrinsic value. Said asset and said debt offsets each other, and the sum of the two remains zero. The money creation did not add any intrinsic value to the economy and did not add any nominal value to the economy. As no difference between intrinsic value and nominal value has been created, money creation is fair and involves no bubbles. Paper money is not just a piece of paper but a debt instrument.

Elements with the creation of Federal Reserve Notes of 1913 were like this:

Element 1. Bearer of the burden: The Fed and the Treasury, per the underlined (1) of Quote 6.
Element 2. Means of value maintenance: Redemption in lawful money, per the underlined (3).
Element 3. Initial valuation: The face value in US dollar.

Underlined (2) in Quote 6 above is legal tender declaration with examples of debts that can be cleared with Federal Reserve Notes. This can be viewed as a complement to Elements 1 and 2. It can also be viewed as a fourth element.

Underlined (3) had in its initial version of 1913 "gold" in place of "lawful money." Gold Reserve Act of 1934 made the change, perhaps as a measure of limiting private possession of gold.

Three similar terminologies (lawful tender, legal tender, lawful money) were used in seven historical acts like below:

(List 2) Lawful Money and two similar terminologies
Coinage Act of 1792, Sec 16: (indicating coins) “a lawful tender in all payments”
Coinage Act of 1837, Sec 9: (coins) “legal tenders of payment”
Coinage Act of 1849, Sec 2: (coins) “a legal tender for twenty dollars”
Legal Tender Act of 1862: (the Greenback) “lawful money and a legal tender in payment”
Federal Reserve Act of 1913: (coins and the Greenbacks) “lawful money”
Gold Reserve Act of 1934: (United States notes, Treasury notes of 1890, gold certificates, silver certificates, Federal Reserve notes, and circulating notes of Federal Reserve banks and national banking associations) “legal tender” (None of gold, gold certificate or Federal Reserve notes) “lawful money”
Coinage Act of 1965: (all coins and currencies of the US) “legal tender for all debts” (List 2)

There is an assertion that a legal tender was called a lawful money when it was tied to gold. I don’t know. I could list my findings in List 2 above, because I could do that.

This system worked quite well until around the end of 1960’s, when the global economy demanded more dollars than the US could back them with gold. In this sense, this situation was similar to the one in “Money creation example 2: State Bank Notes from 1836” above.

Money creation example 8: Federal Reserve Note since 08/15/1971

From around the end of 1960’s, global demand for gold, together with the demand for US dollar, surged. The report at the following link may be a good explanation of such a situation of 1971.

https://www.nixonlibrary.gov/sites/default/files/2018-09/Gold.pdf

Nixon Shock of 08/15/1971 meant some change in Element 2. “Lawful money” in the underlined (2) in Quote 6 above meant in 1934 any of the previous US monies, all of which were tightly linked to gold. So-called Nixon Shock of 08/15/1971 severed the link between the lawful money and gold. For this severance, Nixon said:

(Quote 8) I have directed Secretary Connally to suspend temporarily the convertibility of the dollar into gold or other reserve assets, except in amounts and conditions determined to be in the interest of monetary stability and in the best interests of the United States. (Quote 8)

“The dollar” in the Quote 8 means all the monies including Federal Reserve Notes and lawful monies in Quote 6 above. Many economists of today lament over this event, but let me quantify what happened thereafter with the following table:

Table 1	Gold prices			CPI		Money value
	Price ($)	1971=100	Increase	1971=100	Increase	
Year	A	B	C	D	E	F (1/D)
1961	35.50	79.60		73.83		135.45
1962	35.35	79.26	-0.42%	74.57	1.00%	134.11
1963	35.25	79.04	-0.28%	75.56	1.32%	132.35
1964	35.35	79.26	0.28%	76.54	1.31%	130.65

1965	35.50	79.60	0.42%	77.78	.61%	128.57
1966	35.40	79.37	-0.28%	80.00	2.86%	125.00
1967	35.50	79.60	0.28%	82.47	3.09%	121.26
1968	43.50	97.53	22.54%	85.93	4.19%	116.38
1969	41.00	91.93	-5.75%	90.62	5.46%	110.35
1970	38.90	87.22	-5.12%	95.80	5.72%	104.38
1971	44.60	100.00	14.65%	100.00	4.38%	100.00
1972	63.84	143.14	43.14%	103.21	3.21%	96.89
1973	106.48	238.74	66.79%	109.63	6.22%	91.22
1974	183.77	412.04	72.59%	121.73	11.04%	82.15
1975	139.29	312.31	-24.20%	132.84	9.13%	75.28
1976	133.77	299.93	-3.96%	140.49	5.76%	71.18
1977	161.10	361.21	20.43%	149.63	6.50%	66.83
1978	208.10	466.59	29.17%	160.99	7.59%	62.12
1979	459.00	1,029.15	120.57%	179.26	11.35%	55.79
1980	594.90	1,333.86	29.61%	203.46	13.50%	49.15
1981	400.00	896.86	-32.76%	224.44	10.32%	44.55

Column A shows price change of gold. Column B is gold price index with 1971 figure as 100. Column C shows annual rate of increase. It tells that US government lost control of gold price in 1968. Column D is consumer price index with 1971 figure as 100. Column F is the reciprocal of D.

Column E shows annual prices increase, which is annual dollar value decrease. The speed after 1971 is faster than before 1971, but the difference was caused by not only Nixon Shock but also other factors such as the first oil crisis of 1973 and the second oil crisis of 1979. Tonkin Bay incident occurred in 1964. Paul Volcker's high interest policy started in 1979. These two events must have influenced prices, but I don't go deeper into them for now.

Considering various factors in the preceding paragraph, Nixon Shock's influence on "lawful money" in Quote 6 above does not look terrible. What was intended with Federal Reserve Act of 1913 has survived Nixon Shock for almost a half century.

Money creation example 9: US copper coins

A copper coin of 1792 can be viewed as a warehouse certificate money, because its face value was different from the value of copper in it. It was, in this view, a metal note secured by gold reserve in 1792. A copper coin after 1971 can be viewed as a note money. These two views are mine, and I don't know who else would share this with me.

Copper coins were always pegged to the main currency in its time, and their usefulness is indisputable. Because of its usefulness and its physical characteristics, in general, copper coins were always viewed as a commodity money.

There is a big difference in accounting between the two views in the preceding two paragraphs. If a copper coins of today is a note money, then all its production cost must be accounted for as expenses and no inventory value should be recognized in the book of the Fed.

As it is viewed as a commodity, the coin inventory in the Fed is recorded as an asset in its face value. US Mint sells the coin for its face value. The difference between the face value and production cost is recorded as seigniorage income in the books of US Mint. Seigniorage income is a little less than 50% of face value now. Considering its usefulness, this seigniorage is not unreasonable. Considering the weight of coins compared with all the monies in circulation, the seigniorage won't affect the value of dollar significantly.

Copper coins are auxiliary to the main currency. As to coins, we don't even think of the three elements discussed in the eight examples above. When creating a new currency, the creator's eyes should be focused on the main currency, not copper coins.

Interpretation and analysis of Part 6 (Incentive) of the whitepaper

We can find what bitcoin creators had in mind while creating bitcoin, by looking into Part 6 (Incentive) of Satoshi Nakamoto's whitepaper.

(Quote 9) 6. (1) Incentive

By (2) convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an (3) incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of (4) a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The (5) incentive can also be funded with transaction fees. (6) If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a (7) predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be (8) completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by (9) stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with (10) more new coins than everyone else combined, than to undermine the system and (11) the validity of his own wealth. (Quote 9)

The underlines and numbers preceding them are all my additions, made to interpret this important part of the whitepaper to a degree satisfactory of the purpose of this writing.

(1) Incentive (seigniorage)

Satoshi's incentive is equivalent to seigniorage. There are two seigniorages in the world of bitcoin: the underlined (3) and (5).

(2) Convention

Satoshi's thought in this word "convention" is with the process of issuing coins. Coins can be viewed as a commodity, but paper money and electronic money are not commodities. Non-coin monies are promissory notes as shown in numerous examples of money creation above.

Further, as the main currency is in the form of paper and electronic books, the process of issuing US coins is cannot be a reference to new currency creation. Satoshi did not have the ABC of money creation.

(3) Incentive 1

Satoshi's incentive at this part is analogous to the seigniorage on US coins explained in "Money creation example 9: US copper coins" above. The difference is that bitcoin miners do not spend bitcoin while mining, while US Mint spends US dollars while coining. This difference fails bitcoin to become a unit of account.

(4) Gold miners' expenses

Satoshi insinuated that the value of gold comes from the mining expenses. But expenses alone cannot make any value. We buy gold without knowing who spent how much for mining and refining it. We buy gold because we like it. We like gold because gold is not something like this:

000000000000000000012494ddcfb91d3968b2ea4d2dd55e0d94b23c6eb1f11cf8

Some economists in history did think that value comes from expense in terms of labor hours. But that kind of thought is long outdated. Especially, the Great Depression condemned this thought completely. FDR in his Fireside Chat # 2 said:

> (Quote 10) The people of this country have been erroneously encouraged to believe that they could keep on increasing the output of farm and factory indefinitely and that some magician would find ways and means for that increased output to be consumed with reasonable profit to the producer. (Quote 10)

The thought that expenses can create value is not just a different opinion. It cannot be considered an opinion any more. It is simply erroneous like a mathematical error.

(5) Incentive 2

This is about the second seigniorage, in the form of transaction fee, collected by the creator (the successful miner) of the block in the transaction. See Table 2 below for seigniorage comparison.

Table 2	Seigniorage		
	Collector	at issuance of the currency	while the currency is in use
bitcoins	Miner	See (3) above	See (5) above
US copper coins	US Mint	About 45% of face value	Null
Federal Reserve notes	FRB	Null	Interest on debt instruments owed to the Fed

US Mint sends all the net profit to the Treasury. FRB sends almost all (= minus tiny dividends paid to the shareholder banks) the net profit to the Treasury. Therefore, the ultimate collector of seigniorage of all US money is the Federal government.

(6) Input and output

The two words, input and output, are used in this Whitepaper very differently than in economics. Satoshi's input means inflow of bitcoins into a certain wallet, and Satoshi's output means outflow of bitcoins from the same wallet. If a specific block contained 10 bitcoins when it was flowing into a certain wallet, 8 of them were sold out of the wallet and 1.5 bitcoins remained as inventory, the wallet must have paid 0.5 bitcoins in the form of transaction fee. Satoshi did not mention inventory while explaining this seigniorage, leaving another confusion in the murk of bitcoin world.

(7) Predetermined number of coins

It is generally understood that the number of minable bitcoins is limited to 21 million. This number came from: (50 coins / new block for the first 4 years x average 6 new blocks / hour x 24 hours / day x 365 days / year x 4 years) x 2 = 21,024,000.

The 2 at the end means 1/(1-r) in the formula S=a/(1-r), where "a" is the whole thing in the parenthesis preceding it and r=1/2. The reward for a successful mining halves every 4 years.

The first 4 years (2009-2012): 50 coins per new block.
Next 4 years (2013-2016): 25 coins per new block.
The third 4 years (2017-2020): 12.5 coins per new block.
And so on.

What is in the parenthesis preceding "x 2" in the underlined formula means the number of all the bitcoins excavated in the first 4 years. Summation of an infinite geometric series is illustrated at the link below:

https://www.varsitytutors.com/hotmath/hotmath_help/topics/infinite-geometric-series

If you are not familiar with this calculation, tear a copy paper into equal two pieces. Write "50" on one of the two pieces and put it aside. Tear the other piece into two and put one of the two on the first piece you put aside. Tear the remaining one, which is one quarter of the original paper, and put a half on the stack put aside. Continue this process until you get bored of doing it. All the pieces on the stack put said is a little less than 100, which is 2 times 50.

The speed of mining is automatically controlled so that a new block can be produced about every ten minutes. If the mining happens too fast, the next mining success requires one more zero. If the new mining took too long, the next mining success requires one less zero. That's why the following two examples had different number of zeros. (There is a minor difference from the fact in this paragraph, but the reader can grasp the concept faster this way.)

000000000000000000012494ddcfb91d3968b2ea4d2dd55e0d94b23c6eb1f11cf8
00000000000000000f84021d63f8e21e9bcb5ac28b78b9e7ae292b726891896

(8) Inflation free

Satoshi thought that neither deflation nor money shortage is a problem. Deflation can come from money shortage, overproduction, advancement of technology. Deflation arising from money shortage is the worst kind of deflation. The typical case is as shown in "Money creation example 2: State Bank Notes from 1836" above.

(9) Stealing back his payments

The fundamental problem Satoshi found in the existing payment system is double payment. I wonder there really is such a case in electronic payments. Satoshi may have extrapolated the problem of checks bounced on NSF.

(10) More new coins than everyone else combined

Satoshi thought that one with the computing power enough to alter any past transaction could, using the same computing power, get more coins than all the existing coins. However, more than 17 million bitcoins have already mined. The remaining 3 million is not more than 17 million. Even before this stage of bitcoin history, this assertion can stand if there is only one block chain in the whole network of Bitcoin. However, isn't a new block containing new coins the start of new chain?

(11) The validity of his own wealth

It means that the wealth in terms of bitcoin can be kept only if the system is alive.

Bitcoin Network, a decentralized Ponzi Scheme.

A Ponzi scheme is defined by the SEC as "an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors." Whether Bitcoin Network is a Ponzi scheme depends on whether the only way for bitcoin investors to enjoy gains is inducing more investments into it. Whether inducing more investments is the only way depends upon whether there is another way.

The only source suggested by the applicants of SR-CboeBZX-2018-040 suggested, as in Quote 2 on Page 2 above, was Satoshi Nakamoto's bitcoin whitepaper.

What Satoshi attempted with the whitepaper was creating a new currency and a new payment system. However, Satoshi failed to design bitcoin so that it can function as a currency. There was no ground to guess that Satoshi had ever read the process of creating money in history. Satoshi had fundamental errors in understanding what money is. List 3 below enumerates some facts about money Satoshi did not know or pretended not knowing.

(List 3) What Satoshi Nakamoto did not know about money
A paper money is a debt instrument, not an object.
US copper coins are accounted for differently than Federal Reserve notes are.
Intrinsic value of a debt instrument is calculated differently than that of an object.
Working currencies were created with at least three elements in List 1 on Page 4 above.
Money shortage forces even the wealthy into bankruptcies. (List 3)

The last one in List 3 is well explained in FDR's Fireside Chat # 1, spoken about two months before Quote 10 above. The story of JP Morgan's rescue effort in 1907 is another example of the same.

Bitcoin's reality as to new currency creation is like this:

Element 1. Bearer of the burden: None.
Element 2. Means of value maintenance: Nothing.
Element 3: Initial valuation: Null.

As Satoshi failed to create bitcoin as a currency, the only way for bitcoin investors to enjoy gains is inducing more investors. Therefore, Bitcoin Network is a Ponzi scheme. As a pyramid structure, which is typical in a Ponzi scheme, is missing, Bitcoin Network can be called a decentralized Ponzi scheme. As a bitcoin is a share of about 21 million shares of Bitcoin Network, a single bitcoin is a security within the Ponzi scheme.

As most Ponzi schemes do, bitcoin has already caused suicides. Dropping from the 10th floor to the ground will kill. Dropping from the 20th floor to the 10th floor will kill, too. Dropping from 19k dollars per bitcoin to 6k dollars per bitcoin killed many people around the world. Bitcoin is a killer. The SEC's one approval would bring more suicides.