Virtual Currency RFI

Submission ICO, Commodities etc.

This is a response in generalized format to the Commodity Futures Trading Commission, request for input on crypto asset mechanics and markets. My name is Dr. Craig Wright and under the pseudonym of Satoshi Nakamoto I completed a project I started in 1997 that was filed with the Australian government in part under an AusIndustry project registered with the Dept. of Innovation as BlackNet.

The amount of misunderstanding and fallacious information that has been propagated concerning bitcoin and any derivative system based on a blockchain (such as and including Ethereum) has resulted in my choice to start to become more public. The system I created was designed in part to end fraud as best as that can be done with any technology. The lack of understanding about the functioning of blockchains has resulted in widespread misinformation and a dissemination of old scams. Many of the former USENET and web IPOs scams have been propagated with the re-badging as an ICO.

I plan to make myself available for questioning from the CFTC outside of the scope of this response. I note in particular that when I talk of bitcoin and other systems, I reference that which was defined in the original white paper and code release.

In any iteration of bitcoin and Ethereum, the nature of the system is of a competitive group of companies seeking payment in response for actively enforcing the rules. Note, when a system has been altered through a fork to introduce new rules the effect is of an airdrop to the prior holders of the digital asset. In this, the parties are generally issued an equivalent amount of the new asset. There has been a lot of fraudulent misrepresentation concerning the promotion of the term decentralized. Cryptocurrency's are only decentralized in the manner that any asset is decentralized. All assets including bitcoin are issued by a single party or group.

Miners do not act as issuers. The issue of a digital cryptocurrency such as bitcoin or Ethereum occurs when the product is launched. Any alteration in the rules of this system need be seen as the creation of a completely new system designed to mimic the original and to issue equivalent amounts of a token to the parties who originally hold that former asset. In the Ethereum network, fewer than 20 nodes control the entire system.

In this, I discuss the situation with a focus on Bitcoin as this is a protocol and when in competition, the existence of multiple protocols does not form a stable equilibrium.

Clearing & Settlement

Bitcoin (and Blockchain generally) alter the method on how trading is completed. The use of Bitcoin acts to remove the necessity of a middleman or intermediary. This intermediary system is the settlement and clearing function.

In the past, a transaction was typically concluded in two phases, the first phase involves the agreement to buy and sell. In Bitcoin, this is the peer to peer user aspect of the system. An individual or a company can deal with another individual or even an exchange. This allows for the seamless and integrated exchange of digital goods and even tokenised items including securities. This in no way differs from any existing financial or trading system. At present, sales over electronic brokers are conducted using the movement of digital tokens.

Bitcoin differs in that it solves issues with the second layer of this system; the clearing and settlement.

The existence of clearing houses is to ensure the peer exchange does not result in the "*double spending*" of a digital good (or token).

The aspect where bitcoin has solved a problem is in the settlement of an exchange. In the sale, Alice and Bob agree to swap 100 items of a particular digital good, say Alice wants to exchange a token that has value in USD for a share Bob holds.

This agreement is a reciprocal promise to deliver and pay.

This is where Bitcoin and the concept of ""Blockchain" comes in. This next phase which is termed settlement. A commercial exchange made at a bank or exchange are created from a combination of these two combined states. The parties make a contractual exchange and promise to deliver a valuable quantity of some tokenised item and they next executed (this is, the parties) the agreements that have been made.

Generally, we find intermediaries that facilitate and act to complete each phase. A peer transaction would include a direct sale or an OTC without an intermediary. With ICO based sales of tokens, this is no different. Sales of an ICO or other token are made either by an intermediary or as a direct exchange. Again, this execution is equivalent to the sales of any goods of commodity and is mirrored in the exchange of all securities and non-commodity money or note. A bank issuing a ""Letter of Credit"" and facilitate the later payment of beneficiary when the complying documents are submitted for redemption.

This applies to Futures commission merchants, share exchanges and any exchange that does not involve the direct barter of a commodity for another.

We can call these phases, the front-end where a market for the token (be it a share, bond or commodity is traded). The use of electronic ledgers and exchange is not new. At present, the dematerialisation of bonds and shares is effectively complete. These records on a computer database are tokens. At present, the use of tokens is widespread and dates to the move towards electronic trading as started in the 1980's. Markets are run over electronic trading platforms with floor traders having been replaced by electronic communication channels. The NYSE, CME and others, are markets that exchange tokens in a manner that is analogous to any "crypto" exchange.

Bitcoin (or any other "Blockchain") cannot and does not replace the front-end process. The execution of buy and sell orders is such a front-end process. Bitcoin (as with all "Blockchains") facilitates the remove of selected classes of "back-end" intermediaries.

Those orders that have been concluded in the back-end are moved into the next phase for ""settlement". This is the process that is controlled by "miners"" or nodes on a Blockchain. The miners act as a distributed clearing house and settlement function. For a digital asset, the actual transfer of assets can be concluded and settled. For commodities that have been securitised and are exchanged as a token, the settlement of transferred promises can be executed on a blockchain, but the final settlement of physical commodities still requires a back-end settlement function.

Where financial assets, shares and securities are exchanged, the blockchain acts to remove the need for a formal clearing house function.

This is the back-end, and the actual transfer of token or electronically designated assets is completed on a Blockchain in the same form as a clearing house in the existing exchange of tokenised financial assets (note all electronically offered assets are a token. This is a condition that has existed since the 1980's).

The function of the back-end intermediary is to ensure that the transfer of rights has been completed. The investor exchanging one asset with another investor for some agreed asset will be ensured to have received by both parties, that is, all exchanges and funds will have cleared and settled.

This back-end function is overlooked and is generally outside of the scope of notice for many/most in the general public.

The back-end function is to ensure that investors are issued with the rights they have acquired without concern for the quality, marketability, liquidity or risk of those assets. The back-end provides the mechanisms to equally exchange junk bonds or penny stocks equally with the exchange of AAA-rated sovereign bonds or S&P500 level company shares.

The blockchain, like the settlement intermediaries is a mere mechanism to ensure that the investors who have made a trade receive the rights to what they have exchanged.

Bitcoin, and in fact any Blockchain takes the role of a back-end intermediary.

The central securities depositories including the Depository Trust Company (DTC), Central Counterparties including the CME clearing house, the Large-Value Funds Transfer System (LVFTS) and the US Federal Reserve Banks are those entities that a Blockchain replaces.

None of those back-end entities operate a trading market place. They act to supply the plumbing that underlies the trades and take the trades executed in the front-end and ensure that these are settled, and the rights and/or assets are delivered between the parties in the trade.

Bitcoin does not replace the front-end function in any way. It acts to complement it allowing for a simpler, more cost effective and economically viable means to complete frond-end trades.

Bitcoin (and any blockchain) adds a layer of private as it streamlines the back-end process. The error made is that Bitcoin facilities the removal of All intermediaries, it does not and nor could a blockchain hope to deliver this aggrandised promise. The streamlining of the back-end and the ability to provide a seamless integrated global clearing and settlement function for all electronic rights is a more than significant innovation. The idea that this allows shares to be traded without rules or controls is simply a call by those seeking to engage in illegal "bucket shop" activities with a false and invalid promotion of the greater fool theory under the guise of "democratising finance". As noted, the clearing house acts without regards to the quality of the assets being traded. It is simply as N. Aubry (2008) stated the financial plumbing of Europe.

The introduction of a "blockchain" to any financial system does nothing to impact or mitigate, or for that point alleviate the need for regulations and controls of the ""front-end" function. In fact, bitcoin simplifies the regulation of all trade conducted over a financial market. The ability to add date defining the exchange allows the parties to simplify the compliance requirements and lowers the costs to the "front-end"" markets in providing services whilst simultaneously allowing the parties to an exchange to settle faster and with less costs. The result of which is the increased velocity of both national and global trade and exchange.

We can illustrate this process as follows. If we take a hypothetical exchange in USD for Apple share between Alice and Bob, we can have an agreement reached where Alice will buy 1,000 shares of Apple Corp from Bob at a price of USD $150 per share. This exchange is completed on the back-end after it has been agreed on the front-end. The front-end, the OTC facility or a share exchange does not change in any way as a result of the introduction of a blockchain. The process is faster, and the parties settle without delay, but the exchange process itself exists outside of Bitcoin (or any Blockchain).

In a traditional scenario, the clearing house and settlement functions will ensure that Alice deposits the required 150,000 USD and that BOB relinquishes his 1,000 Apple shares. The back-end will ensure that Alice has the funds available and that Bob has the shares deposited and holds the rights to those shares allowing the exchange to be completed.

Bitcoin simplifies this back-end process. It allows Alice to set her funds aside and be placed into a settlement function, either as a director or atomic swap and to have Bob's assets verified. The pseudonymous nature of the system means that Alice and Bob's identities are only known to each other and any parties related to the exchange and transaction. The identity of the parties can be immutably recorded on the blockchain and, any change in the value can be legally enforced allowing a share transaction to be noted if it violates statute or other regulations.

Bob and Alice simply settle in minutes and directly without the cost, overhead and added waste of a third party clearing house. This is the process introduced and enacted by Bitcoin and which is copied by other Blockchains.

Front and Back End

The front end of a financial exchange process differs greatly from that at the back-end. The front process involves the exchange of contracts to buy or sell securities or commodity

contracts. The back-end has traditionally been based on a pre-established closed-door relationship. This relationship exists in the form of an account which is maintained by the intermediary. This intermediary holds rights and duties that may not relate to any specific time and transaction circumscribed contract. The front end is thus a scenario incorporating a contract entered into between buyers and sellers.

The backend modifies a relationship between intermediary parties. For example, if Alice sold Apple shares using Morgan Stanley, and Morgan Stanley credits Bob's account with these stock certificates, the back-end exchange has been an account transfer where Morgan Stanley has credited Bob to the same amount it debited Alice's account. Alice has now a lower balance held at Morgan Stanley and Bob has an increased holding.

This is the same process that the blockchain replaces. Rather than the account function being completed and verified by Morgan Stanley in their internet clearing house, Bitcoin allows the ledger to be updated and maintained directly.

A smart contract or even simple template transaction is negotiated outside the blockchain and then is settled using the blockchain to ensure that the exchange is valid (verification occurs using the mining process) and that no "double spend" has occurred (such as a forger attempting to sell the same share certificate a second time).

Bitcoin acts as the back-end system that holds the certificate. The user has a record that is validated through the use of a cryptographically signed message which is recorded on the ledger.

Bitcoin is a write once, read many ledger. This mirrors many existing accounting databases. If an error occurs, the ledger can be modified but a reversal transaction must be written to note the error.

In the tokenised share offered by a company, if a court finds a particular share exchange to be invalid, such as being a sale to a restricted party, even on an immutable ledger, the company can rectify this.

The process is to issue a public reversal. The parties to the transaction remain pseudonymous to the greater world, but the company or group maintaining the ledger and records will issue a reversal transaction.

If for example, Alice sells Bob 100 shares in Apple, but a court deems that Bob's shares are ones he cannot hold by law, the transaction is reversed by invalidating the transaction.

If Bob will not sign the transaction to allow this to occur the company simply issues a revocation formally on the register and now, though Bob has a ""cryptographic ledger" entry, the entry is no longer associated with any rights. Bob cannot use this to redeem a commodity, he cannot sell this as any sale will also be invalid and the register will permanently note that not only Bob's entry but also any trees of transactions created from that are now invalid.

The blockchain allows for the introduction of a simple revocation table. If a certificate or transaction is revoked invalidly, this gives rise to an action by Alice against the company.

Although the records in a Blockchain are immutable, this acts as a WORM or write once read many account systems and does not leave the records to be unalterable.

Purpose and functionality

1. Ether and the related network we designed and developed due to a set of constraints being imposed by the bitcoin core developer group. Bitcoin was always designed with robust and thorough scripting capability involved. Bitcoin is in fact Turing complete and without the self-imposed limitations is capable of doing more than Ethereum computationally.
    a. Ethereum is a flawed concept based on bitcoin. The concept is that all nodes equally run and computer software making it “decentralized”. The reality is that this simply limits computation and stops scaling.
    b. The Ethereum network has already reached its computational limits. As it scales, every user needs to be replicated by every other user.
    c. Bitcoin conversely can leave simple verifications on chain allowing a system that scales globally and delivering a distributed computational method.
    d. The sole reason that bitcoin was set to no longer scale and to remain at a temporary 1 MB limit has been to force users away from the immutable ledger. The hijacking of bitcoin started with the failure of Silk Road. Since the collapse of these drug markets and the realization that are immutable blockchain allows law enforcement to better trace funds, the developers within bitcoin have sought alternative ways to force people off chain. This is led to the development of sidechains and lightning. These networks are designed to allow periodic settlement increasing anonymity through the deletion of records.
    e. A similar system is being developed for Ethereum and is called plasma.
    f. The sole purpose for taking these records off chain is to increase the ability to utilize cryptocurrency on dark websites such as drug markets.
    g. The issue of contracts on Ethereum is analogous to a group using an Amazon Cloud compute service and awaiting the results. The issue being that every client of Amazon would need to run all other clients code on a system simultaneously.
2. Ethereum is a poorly designed copy of bitcoin designed with the purpose of completing the promise of smart contracts and scripting that were delivered within bitcoin but which were hobbled by the core developers of bitcoin who sought to enable anonymous transactions to exist within the system.
3. This network has already hit its limit and is effectively only being used to raise capital using illegal bucket shops that are designed in such a way that they can deceive non-technical parties. No technology released within Ethereum for the provision of computation or ICOs has been created that did not exist prior and in a more effective manner before this network was launched.
4. Generally, most parties file to account for the currency arguing that it is difficult to record. This is misleading and false. All cryptocurrencies are incredibly simple to account.
5. This market is thinly traded and easily manipulated, and no data should be trusted.
6. -

Technology –

7. Ethereum is a copy of bitcoin with a virtual machine and high-level language built around it. It is a poor copy in that is unable to validate without having every single node run every single computation limiting the ability to scale and reducing its usefulness.
8. Ethereum cannot scale. If 10 people seek to run 10 applications all 10 nodes will have to run these applications. If 1 million people run 1 million applications all of 1 million nodes will simultaneously be required to run all applications. The effect is one global computer that is copied 1 million times. In bitcoin, the nodes are only required to validate the result and oracles can be set up allowing infinite scaling.
9. I tested the equivalent a proof of stake mechanisms between the years 2003 to 2007. All proof of stake mechanisms collapse into single-user control and allow alteration rather than the creation of an immutable record.
10. The economics of proof of stake are flawed and are based on an oligopoly game.
11. There is no working proof of stake model.
12. The only way that Ethereum can scale is reliant on altering the model to copy bitcoin. I have patented most of these techniques.

Governance

13. The governance model in Ethereum is controlled by one central group who uses misleading statements saying that they are decentralized to cover up the fraudulent creation of a digital security. All choices are made by one central group.
    a. The original version of bitcoin does not fork the protocol, this is set an unalterable other than major security vulnerabilities.
    b. The nature of any blockchain is of an immutable system and protocol.
    c. The bitcoin core (BTC) group has subverted this process in a vain effort to create an anonymous system allowing for dark market drug use and sale.
14. Blockchain's do not fork as the community tries to mislead regulators to believe. A complete and new copy is created on any split with an airdrop of coins being distributed to the new protocol.
    a. Blockchain's are protocols in the manner that the Internet and IP is a protocol compared to previous alternative such as NetBIOS and IPX.
    b. There is no distributed consensus model at work here, there is a new protocol such as with Ethereum Classic vs Ethereum where the creation of an entire new system that mirrored the original protocol with a few changes was launched.

Other

Bitcoin and all derivative systems solve one issue, clearinghouse and settlement of a digital asset using a competitive mining process that acts to settle the first seen transaction and holds this to be valid.

There is no such thing as a validating node nor for the concept of democratized decentralization. The myth of decentralization has been spread with the sole concept of enabling illegal markets to exist. The control of either bitcoin or Ethereum is limited to those who run nodes and these are people running at large data centers and not home networks.

Every contract and every exchange on any blockchain system was designed to be completely analogous to the existing financial and legal structure existing within the common-law market.

It is very simple to trace every single cryptocurrency and map every single sale on a system such as Ethereum. Those involved in promoting the systems seek to promote a misleading view of the functionality of a blockchain based system in order to circumvent existing law. In any blockchain system, all transactions are done between individuals in the same manner that an exchange is done between individuals when conducted in the Chicago futures markets. The sole innovation of bitcoin is the ability to ensure transactions are not reordered and cannot be altered without the need for a clearinghouse and settlement system.

Bitcoin does not distribute exchanges and it does not alter the process. No blockchain differs from this including Ethereum.

If anyone tells you separately the blockchain can work outside existing legislation, statutes and rules they are seeking to mislead and defraud for the sole purpose of avoiding regulation and creating unregulated bucket shops and dark web markets.

I am willing to testify under oath.

Regards,

Dr Craig S Wright, LLM, PhD