Testimony of Gregory Zerzan

Before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations

"Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains"

Introduction

Subcommittee Chair DeGette, Subcommittee Republican Leader Griffith, Mr. Chairman and Republican Leader Rodgers, thank you very much for allowing me to appear before the Committee today. My name is Gregory Zerzan and I am a shareholder at the law firm of Jordan Ramis PC. My practice focuses on financial services, natural resources and environmental regulation. Prior to my current position I served as Principal Deputy Solicitor in the U.S. Department of the Interior; I have also served as Deputy Assistant and Acting Assistant Secretary of the United States Treasury and as counsel to three different congressional committees, including this one. It is a privilege to be with you today.

Summary

Bitcoin and other cryptocurrencies have exploded in popularity in recent years. Cryptocurrencies are one aspect of a larger innovation, blockchain. Blockchain allows parties to exchange information across a transparent network without requiring the permission of third parties. Importantly this allows individuals to control their own information, thus potentially disintermediating large institutions that currently dominate the internet, like social network companies, search engines, virtual retailers and financial institutions.

There are different types of cryptocurrencies (also referred to as "digital tokens"). Bitcoin was designed to be an internet-based substitute for traditional forms of payment. Its appeal likely stems in part from the perception that national currencies have become less reliable as a store of value. Widespread government spending and central bank balance sheet expansion, particularly following the financial crisis of 2008-2009, doubtless fueled Bitcoin's popularity.[i] However, Bitcoin is only one, limited application of blockchain technology.

Apart from the Bitcoin use case, cryptocurrency serves an important role in the blockchain eco-system unrelated to its perceived substitutability for cash. Cryptocurrency can be thought of as an internal mechanism to incentivize participation in the blockchain. It facilitates the important role network participants play in allowing a blockchain to serve as a decentralized, distributed computing system. Cryptocurrencies exist to make blockchains run efficiently. They are not necessarily meant to be investments, or a substitute for cash, even if many have treated them as such. Rather than thinking of cryptocurrency as money, a more apt analogy may be to think of it as the oil that greases the gears of the blockchain.

Concerns have been raised about the energy consumption required to perform the computational tasks required by some blockchain networks. However, alternative means to validate transactions and achieve consensus exist. These other methods consume significantly less energy than does Bitcoin mining. As the technology evolves it should be expected that the systems will become more energy efficient. In addition, as technology advances it is likely that less carbon intensive sources of energy will become a greater part of the overall U.S. energy portfolio.

Blockchain technology holds the promise of creating a new type of internet, one where information is controlled by the users of the system. Blockchain can ensure that ownership of data stays with individuals, rather than in siloed servers owned by a few large corporations. However, regulatory uncertainty, or overly restrictive new laws and regulation, could prevent this technology from reaching its full potential in the United States and drive innovation offshore.

In summary, there are four main points I hope to convey in my testimony:

1. Bitcoin is only one application of the broader blockchain technology;
2. Blockchain can empower consumers and give individuals greater control over their information;
3. Concerns about energy usage will likely be alleviated as the technologies for both blockchain and energy production advance; and
4. Blockchain faces regulatory uncertainty in the US which could discourage the growth of this technology. This could be resolved through legislation clarifying that digital tokens are not financial products unless they are intended to be and are marketed as such.

Background

Blockchain is a relatively new solution to an age-old problem: how to securely store and share information. Blockchain operates as a distributed ledger, meaning that transactions that occur on the blockchain are shared with all other participants in the network who can affirm the validity of transactions. This validation occurs through encryption and mining, incentivized by rewards in the form of digital tokens.

Parties on the network control their own information, which they can exchange with others. Each participant has an address (a place to store contents) and a "private key," which is in effect a password that allows a participant to access his or her account. A participant also has a "public key," which is a numerical representation of the address. To exchange information a person uses the private key to "sign" a message to the other party. Using the receiving party's public key a message is created which can only be opened by the recipient using his or her own private key.

This "public key" encryption method relies on large numbers which must be computed correctly in order to validate the transaction, using cryptographic tools like prime factorization. Prime factorization relies on the fact that any number can be created by multiplying prime numbers; however, it is extremely difficult to reduce a very large number to its prime factors. This "one-way" mathematical problem means that persons who lack access to one of the factors (in this case, a private key) have little hope in cracking the code, since the computational power to do so exceeds any reasonably available resources.

Once the parties have authenticated their transaction it must be verified by the larger network to be added to the blockchain. "Nodes," or members of the network, compete to validate transactions in an effort to receive rewards in the form of digital tokens. "Miners" assemble transactions and "hash" the contents of a block- "hashing" being the process of taking one value and converting it into another using a specified mathematical function. The first miner to successfully compute a hash that meets certain conditions shares the answer with the rest of the network, which verifies that the answer is correct. Once a block of transactions is confirmed it is distributed to the entire network, ensuring each participant has a copy of the transaction. In this way, transaction by transaction and block by block, the entire network maintains an identical copy of each transaction in the same order (a "distributed

ledger”). It is this shared system that makes the blockchain both public and secure; in order to forge a transaction each and every other copy of the blockchain would need to be altered- a difficult task, and one (if even achievable) likely to be noticed.

One of the most familiar examples of the blockchain is the Bitcoin network. “Bitcoin: A Peer-to-Peer Electronic Cash System” was written by the pseudonymous Satoshi Nakamoto and released on October 31, 2008. The paper’s Abstract succinctly describes the concept:

> 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.

Bitcoin (BTC) transactions occur on a blockchain that is controlled by its members. To transact in BTC a party needs only an address and a private key, which can be housed on one’s own server. In this way BTC can be thought of as an alternative currency which is not issued at the discretion of a centralized authority (such as a central bank) nor transacted via centralized networks (payment systems of connected banks).[ii]

While BTC is the most well-known and widely circulated cryptocurrency in the world, thousands of other cryptocurrencies exist, many of which are not solely designed to serve as currencies. The second most widely held cryptocurrency, Ether (ETH), is the token used to reward validators on the Ethereum blockchain.

As described in his 2013 paper “A Next-Generation Smart Contract and Decentralized Application Platform,” Vitalik Buterin described the concept of using blockchain technology for a whole host of decentralized transactions beyond cash:

> Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or "intrinsic value" and no centralized issuer or controller. However, another, arguably more important, part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungible assets such as domain

> names ("Namecoin"), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ("smart contracts") or even blockchain-based "decentralized autonomous organizations" (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

One of the most well-known products of the Ethereum network are non-fungible tokens (NFTs). NFTs are data, such as an image or a video, with a unique and identifiable ownership record. NFTs can be sold or exchanged, with the blockchain recording the authenticity and transfer of ownership in each instance.

The Ethereum network described by Mr. Buterin, and other initiatives that have followed, seek not to create a new currency so much as to create a new internet, one where information is owned and controlled by its users and not large, centralized institutions.

Cryptocurrency as a Mechanism for a User-Run Network

The Ethereum network provides a computational framework, built on blockchain, that allows users to execute programs. In practical terms this means that the Ethereum network can act as a sort of decentralized virtual computer on which users can develop applications, store data and exchange information. Unlike the Bitcoin blockchain, which has a programming language consisting of true/false calculations amenable to spending transactions, the Ethereum blockchain is fully programmable. As described in "Mastering Ethereum" by Andreas M. Antonopoulos and Gavin Wood, two of Mr. Buterin's key collaborators in the creation of the Ethereum network:

> Ethereum is also a distributed state machine. But instead of tracking only the state of currency ownership, Ethereum tracks the state transitions of a general-purpose data store, i.e., a store that can hold any data expressible as a key–value tuple. A key–value data store holds arbitrary values, each referenced by some key; for example, the value "Mastering Ethereum" referenced by the key "Book Title". In some ways, this serves the same purpose as the data storage model of Random Access Memory (RAM) used by most general-purpose computers. Ethereum has memory that stores both code and data, and it uses the Ethereum blockchain to track how this memory changes over time. Like a general-purpose stored-program computer, Ethereum can load code into its state machine and run that code, storing the resulting state changes in its blockchain. Two of the critical differences from most general-purpose computers are that Ethereum state changes are governed by the rules of consensus and the state is distributed globally. Ethereum answers the question: "What if we could track any arbitrary state and program the state machine to create a world-wide computer operating under consensus?"

In this fully programmable version of blockchain the Ether token serves a broader purpose than does BTC. Bitcoin was created to serve the same function as a traditional currency. As Securities and Exchange Chairman Gary Gensler has observed, these functions are as a unit of account, a store of value and a means of exchange.[iii] Ether can also serve these functions, but its main purpose is to act as a

virtual lubricant for the operation of the Ethereum network. Users "pay" for the computational services of the network using Ether tokens. While outside users may (and have) chosen to hold ETH for investment purposes, its most important function is to act as a facilitator for the operation of the virtual, distributed machine.

The Ethereum network allows users to develop, own and exchange data through an open network controlled by all participants. This contrasts with the internet as it currently exists, where data often resides in silos controlled by a few large companies with the capacity to maintain massive server farms.[iv]

Cryptocurrency Mining and Energy Use

One criticism of some blockchain technologies is that the computational power required to mine cryptocurrency demands an extravagant use of energy. Further, the criticism holds that this energy use comes with high environmental costs in the form of increased greenhouse gas (GHG) emissions.

The reason the Bitcoin blockchain network requires energy is because, as described above, transactions are only added to the blockchain after they have been validated by "miners" competing to solve a cryptographic puzzle. This puzzle, the "nonce," is an algorithm-generated number that can only be computed by trial-and-error. Successful miners are rewarded for solving this puzzle correctly with newly minted tokens. In the case of the Bitcoin blockchain, the increasing value of BTC has attracted ever greater numbers of miners operating powerful computers capable of generating hundreds of quintillions of guesses a second. According to some estimates, Bitcoin mining composes .5% of all worldwide energy usage.

BTC mining has tended to cluster around areas with comparatively low energy costs. In the United States Texas, New York and Washington have attracted significant mining-related activity. Texas leads the nation in wind-produced energy, while Washington leads the U.S. in hydropower production. These carbon-free energy sources may alleviate some of the concerns over the GHG footprint of crypto mining.

In addition to the use of less carbon-intensive energy sources, another reduction in energy use comes from alternative means of achieving consensus besides the Proof of Work (PoW) method employed by Bitcoin. In the PoW method different nodes (participants) compete to solve a cryptographic problem, with the winning node gaining the right to add a block to the chain and receiving digital tokens as a reward. Later this year the Ethereum network is expected to shift to a Proof of Stake (PoS) consensus model. Under the PoS method the network's protocol will choose a node to validate a proposed block, based in part on how much cryptocurrency the node has bid, or "staked," for that right. If the validator's proposed block is accepted by the network the validator receives digital tokens, as in the case of the PoW system. However, if the validator attempts to submit a false result the validator is punished by forfeiting its staked currency.

PoS systems are less energy intensive than the PoW method because rather than requiring multiple parties to compete to find the correct answer, using vast quantities of computation, a limited number of validators are chosen to validate a less computationally intensive equation. Other consensus systems also exist that can lessen the energy needs of a blockchain consensus mechanism. For instance, the Ripple network allows a network of "trusted nodes" to validate transactions. However, some have noted this results in a degree of centralization that runs contrary to one of the most valued aspects of blockchain. Another network divides the tasks involved in reaching consensus among different validator

nodes, tasking some with computationally intensive "deterministic" tasks such as computing the results of transactions, and "non-deterministic" tasks such as the timing and order of transactions. Taken together these alternative consensus mechanisms provide the opportunity for more energy efficient blockchains.

Many mining companies have proved willing to enter into agreements with local utilities to facilitate fair pricing and ensure grid reliability. This in turn has created new market opportunities for the energy providers, while helping the United States to become the world leader in BTC mining.

It is also useful to compare data mining to other internet-related energy usage. According to some estimates non-BTC-mining related data centers consume 1% of total global energy. The use of energy (regardless of how it was created) is utilized identically. Kilowatt hours are converted to compute cycles, and those cycles are used in traditional datacenter infrastructure in the same way they are used to mine crypto. Many crypto miners have purposefully developed processors known as ASIC (application specific integrated circuits) which are optimized to mine/process crypto more efficiently than normal processors. Importantly, however, unlike dedicated data centers owned by or for the benefit of individual companies, crypto mining helps to facilitate a shared, distributed blockchain open to all participants.

Lastly, U.S. GHG emissions have generally trended downward for at least the last decade.[v] As demand increases for less carbon-intensive forms of energy it should be expected that technology will continue to evolve to accelerate this trend further.[vi]

Regulatory Uncertainty Surrounding Digital Assets

In the United States cryptocurrency and other digital assets suffer from uncertainty over whether regulators might impose regulations, or even find some assets illegal. The Securities and Exchange Commission has taken a mixed approach to cryptocurrency, with at least some officials at the agency stating publicly that BTC and ETH are not securities while at the same time taking enforcement action against Ripple Labs, issuer of one of the mostly widely traded cryptocurrencies, XRP. Officials at the Commodity Futures Trading Commission have publicly stated that cryptocurrencies are "digital commodities," and in some circumstances potentially subject to regulation by that agency. As recently as November 2021 the President's Working Group on Financial Markets announced that a particular type of digital asset known as "stablecoins"[vii] should be issued only by insured depository institutions (e.g., banks).

The regulatory uncertainty surrounding digital assets is troubling for several reasons. First, the lack of clarity and threat of enforcement may drive innovation in the blockchain away from the United States. For example, if an entrepreneur developed a blockchain enabled social network, one where all the personal data on the network belonged to each participant on the network and couldn't be monetized for advertising revenue by a single company, it would likely require some sort of digital token to allow the blockchain to function.[viii] Unfortunately, the threat that this token might be found to be an unregistered offering of a security in violation of U.S. securities laws could force this developer to locate outside the United States. Given the revolutionary potential the blockchain holds to return power to the users of the internet, this would be an undesirable result.

An additional problem is that currently digital asset regulation is a conversation largely occurring among the nation's financial regulators. But blockchain and digital assets[ix] are code that facilitate the performance of a computational task, not shares of ownership in a company (stock) or the promise of future delivery of a commodity (futures contract). Digital assets are a 21st century creation that do not fit well within the terminology and structure of financial services laws that were written in the last century and that in many ways describe products and practices dating back to the 17th century (or even earlier).[x]

While it is certainly possible to create products traditionally thought of as financial instruments such as securities and derivatives using blockchain (indeed, such efforts are well underway), there is nothing inherently financial about digital tokens themselves. Digital tokens should not be treated as financial products solely because people purchase them for uses other than to facilitate transactions on a particular blockchain. People routinely purchase and hold collectibles like baseball cards, stamps and cars in hopes that the items will increase in value, but this does not turn those items into financial products.

It is worth noting that excluding the bulk of digital assets from financial regulations does not mean they are unregulated. For instance, the Federal Trade Commission Act (FTCA) has protected Americans from "unfair or deceptive acts or practices in or affecting commerce" since 1914. The potential for fraud, misconduct and abuse certainly exists in the digital assets market, as in all markets. The FTCA's powerful consumer protection provisions, which clearly apply to internet-based transactions, afford a strong layer of protection for market participants.

It would be beneficial to establish a legal presumption (through law or regulation) that a digital asset such as a cryptocurrency is not a security or other financial product unless it is primarily designed to perform the role of a financial product and is sold or marketed as such. In all other cases a digital asset should be treated as a good, subject to the normal protections that apply to transactions in ordinary commerce.[xi] Policymakers can ensure the United States is a leader in blockchain technology by resolving the regulatory uncertainty that currently hangs over this still developing area.

Conclusion

Blockchain and the digital tokens it relies on are an important and potentially consumer-empowering innovation. Blockchain holds the promise of a new kind of internet, one where individuals have power over their own information. Meanwhile, cryptocurrencies have become an asset class that has provided smaller investors the opportunity to reap large rewards based on their own assessment of the risk and promise of any particular network, without the need of intermediaries such as financial institutions. Unfortunately, concern about this new technology threatens to drive innovation and opportunity in this area to foreign markets. Taken together cryptocurrencies are estimated to have a market value of more than $3 trillion. Although digital tokens are a highly speculative and volatile asset class, they also represent the promise of a more open, more widely shared internet. If policymakers take a cautious approach and foster a pro-innovation environment, the rewards for consumers, investors and all Americans are likely to be great.

[i] As I have written elsewhere, the appeal of cryptocurrency lies at least in part due to a lack of faith in fiat currencies. This lack of faith is surely impacted by steadily increasing budget deficits and national debt, as well as quantitative easing by central banks. Policymakers concerned about the rising appeal of cryptocurrencies might consider imposing limits on government spending, rather than additional regulation. See Zerzan, Gregory "Why Governments Hate Cryptocurrency,' RealClearPolitics.Com (October 20, 2021) https://www.realclearpolitics.com/articles/2021/10/20/why_governments_hate_cryptocurrency_146598.html

[ii] It is worth noting that a Bitcoin does not actually exist as a physical object, in either the non-electronic, material sense, nor in the sense of a unique line of computer code. There is no "BTC A" (01000001 in binary code), "BTC B" (01000010), "BTC C" (01000011), etc. Rather, the transfer and ownership of BTC and other cryptocurrencies is the record of inputs and outputs of digital addresses, or the record of the different states of a distributed computational system.

[iii] Gensler, Gary, "Remarks before the Aspen Security Forum," (August 3, 2021), https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03

[iv] In important ways Ethereum addresses the "Siren Server" problem identified by the technologist Jaron Lanier in his 2013 book "Who Owns the Future?" In that work Mr. Lanier proposed an alternative internet where individuals owned their own data and were compensated for it through a system of micropayments. ETH can be seen to fulfill that same function. *See* Lanier, Jaron "Who Owns the Future," Simon and Schuster (2013).

[v] *See* "Climate Change Indicators: U.S. Greenhouse Gas Emissions," U.S. Environmental Protection Agency, available at https://www.epa.gov/climate-indicators/climate-change-indicators-us-greenhouse-gas-emissions

[vi] According to the EPA, in 2019 the United States emitted less CO2 than in any year since 1992. This reduction, largely attributed to the technological innovation of hydraulic fracturing, or "fracking," is parularly notable given that 2019 was pre-pandemic and occurred even as the larger economy grew. https://www.epa.gov/sites/default/files/2021-04/documents/us-ghg-inventory-1990-2019-data-highlights.pdf

[vii] Stablecoins are a cryptocurrency issued by an organization that holds other assets in a trust that back the value of the digital token. For instance, US Dollar Coin (USDC) allows users to buy the coin on a dollar-for-dollar basis, with each coin putatively backed by an equal amount of dollars held in reserve. Stablecoin can in theory be backed by anything, such as oil, gold or other assets.

[viii] This is essentially the same example as described in the explanation of Ethereum, above.

[ix] With the caveat in endnote ii.

[x] The Dutch East India Company is generally attributed the distinction of having the first publicly traded stock, issued in 1602. Derivatives, like futures and options contracts, have been traced as far back as Ancient Greece.

[xi] For example, this approach could remove uncertainty in the context of the securities laws by resolving ambiguities created by the application of the ***Howey*** test to initial coin offerings (ICO). Using the proposed framework an ICO would be presumed not to be a security unless it was both designed primarily to be an investment and was marketed as an investment. Neither the fact that the ICO is intended to raise capital for its creator, nor that individuals might choose to purchase it for speculative purposes, would alone be enough to make a digital token a security. This framework, which combines elements of both the Howey and Reeves tests, would both promote blockchain development and ensure the securities laws fulfill their important role of protecting investors.