Spring 5-3-2024

From Cypherpunks to Congress: A Historical Analysis of the Development, Uses, and Regulatory Landscape of Cryptocurrencies

Andrew Moore

FROM CYPHERPUNKS TO CONGRESS: A HISTORICAL ANALYSIS OF THE DEVELOPMENT, USE, AND REGULATORY LANDSCAPE OF CRYPTOCURRENCIES

by

Andrew Michael Moore

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Oxford, MS

May, 2024

Approved By

_____

Advisor: Professor Josh Hendrickson

_____

Reader: Professor Jon Moen

_____

Reader: Professor Ken Cyree

ACKNOWLEDGEMENTS

I first want to thank my advisor, Josh Hendrickson, for the multitude of hours he has spent meeting with me and reading my drafts. His help in guiding me through this project has been incredibly valuable. It is truly a blessing to have someone with so much knowledge about this topic at Ole Miss. I also want to thank my other two readers, Jon Moen and Ken Cyree, for their efforts in reading this paper, I know it is long.

I want to thanks my parents for always believing in me and for instilling in me at a young age a high standard of academic rigor. Additionally, all the teachers that I have had throughout my life that helped develop my passion for learning. Finally, I want to thank my girlfriend, Jaiden, for putting up with me over the last year and all the times I talked about this project and cryptocurrencies to her.

ABSTRACT

FROM CYPHERPUNKS TO CONGRESS: A HISTORICAL ANALYSIS OF THE DEVELOPMENT, USES, AND REGULATORY LANDSCAPE OF CRYPTOCURRENCIES

As cryptocurrencies have begun to proliferate through the economy policymakers are asking questions of where they came from, how do they work, what they are used for and how should we regulate the market. Through a historical analysis, it can be seen that Bitcoin represented a legitimate innovation in money and provided significant improvements to earlier attempts at private commodity currency. Additionally, many of the criticisms lobbied against Bitcoin appear to be overstated, most notably the claim that it is a good tool for criminals. However, there has been a notable split in the market. The emerging crypto industry bears little resemblance to the promise of the Cypherpunks. The crypto industry has become rot with fraud and has shifted from activists attempting to build a better financial system, to something adjacent to Silicon Valley. The current approach by federal regulators to regulate the crypto market has been wholly inadequate and Congress must act to create a federal regulatory framework surrounding digital assets.

TABLE OF CONTENTS

PART I: BACKGROUND

CHAPTER I: INTRODUCTION

Fifteen years ago, the Bitcoin Whitepaper launched the crypto movement. Bitcoin was not a mistake, it was not a fad, but represented a real innovation that has ideological roots that can be traced back decades. The creator of Bitcoin Satoshi Nakamoto laid out why Bitcoin is a necessary innovation on money and finance:

> "I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. The root problem with conventional currency is all the trust that's required to make it work… . With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless" (Nakamoto, 2009).

The Bitcoin whitepaper laid out a protocol and design for a digital currency that solved the problems, primarily the issue of double spending, that the Cypherpunks and other ideological movements were attempting to solve. The product created a truly decentralized digital currency.

At the end of 2022, the then world's second largest cryptocurrency exchange, FTX, collapsed. FTX and its founder Sam Bankman-Fried (SBF) was exposed as nothing more than a total fraud. The collapse of FTX essentially exposed more broadly to the entire public a worrisome trend that has cropped up in the ever expanding and rapidly evolving crypto industry. Bitcoin represented a truly revolutionary innovation. Since its inception many innovators have attempted to build upon its promise and bring it worldwide. However, the cryptocurrency ecosystem no longer embodies the principles of the Cypherpunks and has been taken over by fraudsters, scams and Ponzi schemes.

The collapse of FTX highlights two things. One, is that it is quite evident that it is time to separate the crypto industry. Tokens such as Bitcoin and Ethereum, real innovations, created with a purpose by individuals who believe they are doing a good thing for the world should not be lumped into the same box as people like SBF (or any other fraudsters/scam discussed throughout), or with tokens like Dogecoin. These aredistinctly separate groups. One of these groups is built on sound technology and innovation and was the product of years of hard work. The other is nothing more than scammers attempting to get rich quick by hopping onto a trend.

The second point that FTX fully highlighted and perhaps to Congressional leaders for the first time, is that it is beyond time for Congress to finally step up and pass a regulatory framework surrounding digital assets and cryptocurrency. It is clear that existing security law is not enough and without action and guidance from Congress, enforcement actions from the SEC will not be enough to prevent another FTX, which is quite clear because it wasn't able to prevent the first FTX. Cryptocurrencies are not new, they have been around for fifteen years at this point and many countries around the world are passing comprehensive regulatory frameworks to update their laws to accommodate digital assets and it is time the United States join them.

Purpose of the Thesis

This thesis is designed to accomplish several primary purposes. One of which is to showcase the skills that I have learned throughout my time in the Lott Leadership Institute and the Economics program here at Ole Miss. This thesis should demonstrate my ability to research and analyze policy and serve as a considerable writing sample as I begin to apply for Fintech policy fellowships on Capitol Hill.

Another goal of this thesis is to address the considerable knowledge gap that currently exists amongst policymakers, specifically focused on the Federal level. Most policymakers lack an understanding of what cryptocurrency is, how it functions, where it came from, what its goals are, and the difference that exists between different digital assets. This thesis will also make the case for why Bitcoin is valuable, due to its various use cases and it being an economically sound form of currency. This thesis should help address this gap, by serving as an educational tool for policymakers as it will contain a history of cryptocurrency development and a section on the technology behind cryptocurrency.

Another aim of this paper will be analyzing and identifying the policy problems that cryptocurrency can cause and analyzing the current regulations in order to identify any gaps in the regulations and where the need for future federal regulations and clarity can come in.

This thesis will also be forward looking, examining a few of the most hotly debated cryptocurrency bills and regulations at the federal level and analyzing the impact on the cryptocurrency industry. Through this analysis the chief purpose of this thesis and final product will be to propose a federal regulatory framework for the cryptocurrency market.

CHAPTER II: WHAT IS CRYPTO?

Cryptocurrency

Cryptocurrency is a digital form of currency that employs cryptography for secure and decentralized transactions. Typically, cryptocurrencies are decentralized, like Bitcoin, or not controlled by a central authority, as most currencies throughout the world are. Fundamentally, cryptocurrency is based on technology that was developed over decades, blockchain, cryptography and consensus protocols. The chief goals of most well-known cryptocurrencies are to remove the middlemen in traditional finance, facilitate quicker global transfers, lower fees, remove government control of the money supply, and protect privacy (Ashford, 2023).

Cryptocurrency is part of the broader category of digital assets. The IRS defines Digital Assets “as any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary" (IRS, 2024). The IRS classifies assets such as stablecoins and Non-fungible tokens (NFTs) as digital assets alongside traditional cryptocurrency.

Non-Fungible Tokens (NFTs) are digital assets that resemble some art form. Examples include paintings, videos, or music. NFTs are based on the same underlying technology as cryptocurrencies and blockchain but do not function the same. This is because they are “non-fungible” meaning that each unit of the asset is unique and cannot be exchanged on a one-to-one basis with another unit of the same asset. NFTs have been around since 2014 but underwent a meteoric rise and hype period in 2021. Essentially,

NFTs are digital art or any form of traditional collector's items (i.e., baseball cards). (Conti, 2023).

Bitcoin

Bitcoin is the most widely recognized and used cryptocurrency in the world. Bitcoin began in January 2009 when the first genesis block was mined only a few months following the publication of the Bitcoin Whitepaper under the pseudonym Satoshi Nakamoto in October 2008. Bitcoin was the invention of blockchain technology and the first truly decentralized peer-to-peer electronic cash that allowed for the transfer of funds between users without an intermediary and whose issuance is not centrally controlled. Bitcoin enables secure and transparent financial transactions without the need for intermediaries like banks. Bitcoin transactions are recorded on a public ledger that is maintained by a network of computers, known as miners, who validate and secure the network. The total supply of Bitcoin is capped at 21 million, making it a deflationary digital asset (Pritzker, 2019).

Blockchain

The invention of blockchain technology began with Bitcoin. Blockchain is the fundamental building block and technology of digital assets. Blockchain is not a complex technology; it is "a digital ledger that allows parties to transact without the use of a central authority to validate those transactions" (Jaikaran, 2018). In a blockchain, each individual block is linked together to create a chain that establishes a singular linear history (Pritzker, 2019). Since the original invention of blockchain there has been a series of various innovations over the years, including Ethereum smart contracts and web 3 technology.

Nodes

Nodes are the foundation that supports a blockchain. Each node in a blockchain network is typically a single computer on the network. By having a network of computers or nodes, blockchain networks can be decentralized. Nodes are the pieces of blockchain that are responsible for storing all information in the ledger and are also the mechanism for verifying the accuracy of the ledger and transactions. Having the information on the network spread throughout numerous nodes makes blockchains extremely resistant to hacker attacks (Aswal, 2024).

Ethereum

Ethereum is a decentralized blockchain platform and cryptocurrency that Vitalik Buterin proposed in late 2013. Its development began in early 2014, with the network going live on July 30, 2015. While Ethereum shares some similarities with Bitcoin, its primary distinction lies in its versatility and programmability. Ethereum introduced the concept of smart contracts, self-executing contracts with the terms of the agreement directly written into code. This feature allows developers to create decentralized applications (DApps) on the Ethereum blockchain, enabling a wide range of use cases beyond simple peer-to-peer transactions. Ether (ETH) is the native cryptocurrency of the Ethereum platform and is used to facilitate transactions and pay for computational services on the network. Ethereum has undergone significant upgrades, with the ongoing transition from a Proof of Work (PoW) to a Proof of Stake (PoS) consensus mechanism, known as Ethereum 2.0, aiming to address scalability and environmental concerns while maintaining its position as a leading platform for decentralized applications and smart contracts (Buterin, 2014).

Proof of Work VS Proof of Stake

Proof of Work (PoW) and Proof of Stake (PoS) are two distinct consensus mechanisms in blockchain networks. In a PoW system, participants, known as miners, compete to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. In contrast, PoS operates on the principle of validators who are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Validators are selected in a deterministic or pseudo-random manner, and their likelihood of being chosen is proportional to the amount of cryptocurrency staked. Each of these systems has unique advantages and disadvantages, and adopting either system requires tradeoffs. For example, the computational power required for PoW requires high amounts of energy usage. This has led to concerns over the impact of PoW systems on the environment. On the other hand, there are many criticisms that PoS does not increase decentralization and is more centralized than PoW as it potentially concentrates power on a few wealthy investors (Quigley & Gilbert, 2024).

Altcoins

"Altcoins," or alternative coins, are the generalized terms for all cryptocurrencies that are not Bitcoin or the original cryptocurrency. The definition of an alt coin has shifted over time as different coins have entered the market that are intended to have different purposes than to serve as a traditional currency or to be decentralized money (i.e., stablecoins). Altcoins can also have other purposes than what the goal of Bitcoin is, which is to be a decentralized medium of exchange; for example, Ethereum is designed to be much more than just a coin, such as the application of smart contracts on top of the

blockchain (Hicks, 2023). By far, the world's leading altcoin is Ethereum ($223 billion), whose innovative blockchain is responsible for a plethora of other altcoins. Other Major altcoins include Binance Coin ($37.4 billion), CRP ($36.2 billion), Solana ($9.4 billion), and Litecoin ($6.4 billion), one of the first alternatives to Bitcoin (Whittaker, 2023).

One type of altcoins are meme coins, essentially joke crypto coins that are created for no practical purpose and whose price is driven through their popularity on social media. The most prominent of these meme coins is DogeCoin, which, in 2021, experienced a massive social media phenomenon that saw a skyrocketing price. There are over 200 meme coins in circulation (Hicks, 2023).

Stablecoins

Stablecoins are a form of utility tokens that are designed to have their price pegged to a specific asset; most commonly, this is seen as being tied to the price of the dollar. If functioning as designed, the price of a stablecoin should always be at $1. The purpose of stablecoins is to grant the benefits of crypto, such as faster payments or increased privacy, while limiting or removing the volatility seen in the crypto market more broadly.

There are two types of stablecoins. One is collateralized stablecoins, which gather a pool of reserves used to back the coin's value. The most prominent example of this stablecoin design is Circle's USD Coin. The second type of stablecoins are algorithmic stablecoins. The mechanism that maintains the price of the coin is through an algorithm that controls the supply of the coin to keep it $1. Currently, the largest algorithmic stablecoin is a tether. Algorithmic stablecoins are much more controversial, and one of the largest scandals in crypto came from the collapse of Terra (Ashmore, 2022).

Utility Tokens

Utility tokens are designed with a specific purpose in mind that is outside of the scope of being a medium exchange. This service is performed through the blockchain network of the token allowing for specific actions to be done or for various applications to be run. The most prominent example is Ethereum with the smart contracts application on the blockchain (Hicks, 2023).

Security Tokens

Security tokens represent the ownership of an asset similar to traditional securities. Typically security tokens have been used by companies as a way to raise capital funds through the sale of coins (ICOs). These tokens fall within the jurisdiction of the SEC. These board definitions of tokens are not mutually exclusive. Binance Coin (BNB) is both a utility token, as it can be utilized to pay fees on the Binance exchange, but it has also been considered a security by the SEC and is currently undergoing a criminal investigation. BNB is also not decentralized (Hicks, 2023).

Wallets

Crypto wallets is the term used to refer to some mechanism that stores private crypto keys that are necessary to be used to access one's crypto coins on a blockchain. Keys are a required mechanism to prove digital asset ownership and can not be recovered. Various types of wallets function differently. First is a paper wallet; a cryptocurrency owner can write down all of their keys on a hard copy that they can use when they wish to access their coins; this is a relatively simple but impractical way of storage. The second is hardware wallets, which store the keys on an external thumb drive only inserted into the computer when an individual wishes to access their assets. This is a

more convenient method of storage and is still safe for users. Finally, online wallets store keys through an app or software typically administered by a third-party company, such as Coinbase. This is the easiest way to access crypto, which allows a user to store, manage, sell/receive, and shop. However, there is a risk of hacking as it is online (Hicks, 2023).

Exchanges

Crypto exchanges allow for the purchase of cryptocurrencies with fiat currency (i.e. dollars). Crypto exchanges operate like traditional stock exchanges, allowing people to make transactions by matching sellers and buyers in return for a fee. Before the emergence of crypto, acquiring cryptocurrencies could only be done through the mining process or by organizing transactions directly with the owner of a coin. There has been an explosion of exchanges, coming a long way from the origins of Bitcoin (Maheshwari, 2023). The most prominent exchange in the US is Coinbase. Internationally, the largest in Binance. Coinbase and Binance are locked into legal battles with the Securities and Exchange Commission, with the SEC claiming they are listing unregistered securities for sale on their exchanges. The most infamous is FTX, which collapsed in shame along with its founder, Sam Bankman-Fried (SBF), in November 2022 (Napolitano, 2023).

CHAPTER III: HISTORY AND DEVELOPMENT

History of Money

The history of money is a fascinating journey that spans millennia, reflecting the evolution of human societies and their economic systems. It began with commodity money, where items with intrinsic value, such as shells, salt, or precious metals, were utilized as mediums of exchange. The transition to metallic coins marked a crucial advancement, providing standardized units of value. Ancient civilizations like the Greeks and Romans adopted this form of money. Paper money emerged in China during the Tang Dynasty, facilitating trade and reducing the need for heavy metal coins. The modern era witnessed the establishment of fiat currencies, which were not directly tied to physical commodities but backed by the trust and authority of governments. In the 20th century, electronic forms of money, such as credit cards and digital transactions, became increasingly prevalent (White, 2023).

The concept and institution of private commodity money is steeped in the tradition of the United States. During the 1500s to 1700s, the concept of private money in what would become the United States was marked by a lack of a standardized currency and various forms of private and foreign money circulated in the American colonies. Barter and trade were prevalent, and the scarcity of official government-issued currency led to a reliance on foreign coins, such as Spanish pieces of eight, Dutch guilders, and English shillings. Local communities and colonies attempted to address the shortage of currency by utilizing commodities as a medium of exchange. For example, in the

Massachusetts Bay Colony, wampum (beads made from shells) was used as money. In other areas, commodities like tobacco in Virginia and rice in South Carolina were used for trade. Private individuals, businesses, and even local governments began issuing their own forms of paper money, known as colonial scrip, to facilitate trade. The Massachusetts Bay Colony issued the first paper money in the 17th century, setting a precedent for other colonies. The Continental Congress introduced the Continental Currency during the American Revolution, facing challenges such as hyperinflation. The U.S. Constitution granted Congress the power to coin money, leading to the establishment of the U.S. Mint in 1792. The Coinage Act of 1792 standardized the American monetary system, and various forms of commodity-backed money, including gold and silver certificates, circulated throughout the 19th century (Studenski & Krooss, 2003).

The First Bank of the United States was the brainchild of Alexander Hamilton and was the first federally-chartered bank in the US. The bank was established by Congress in 1791 and was approved for a twenty year charter. The bank in some ways can be viewed as a prelude to central banking, although it was very different from modern central banks. The bank served as fiscal agent for the federal government by providing loans to the government and collecting tax revenue. The bank also issued notes which were the closest thing to a standard national currency at the time and were the only acceptable payments for taxes. However, private banks were still allowed to issue their own notes. Throughout its existence there was constant debate over the power and influence of the bank and after expiration in 1811 the charter for the bank was not renewed.

The United States would once again set up a national bank in 1816 when The Second Bank of the United States was chartered for another twenty years. This bank operated in a very similar fashion to the first bank. However, the second bank had additional authority in monitoring the issuance of state bank notes.

Following a political battle with President Andrew Jackson, the charter for the Second Bank of the United States was not renewed and in 1836 America returned to private money. The Free Banking Era in the United States refers to the period from the 1830s to the Civil War (1861-1865) when state-chartered banks were allowed to issue their own currency without strict federal regulations. During this time, various states enacted laws that permitted the establishment of banks without a federal charter, leading to a proliferation of state-chartered banks issuing their own banknotes. This decentralized and less regulated system was known as "free banking" (Studenski & Krooss, 2003).

The free banking era saw the number of banks and the amount of paper currency issued increase dramatically. It allowed for free entry into the banking system and overall a lower level of regulations. Customers were able to choose which issuer they trusted or which one provided them the greatest benefit. The bank notes of individual banks would circulate at a greater discount the farther they got from the location of issuance and the information on individual notes could be found in weekly publications from note reporters. Some states attempted to construct insurance systems such as the New York Safety Fund. Additionally, one of the most robust insurance systems, the Suffolk Banking System, developed privately (Studenski & Krooss, 2003).

There has been a lot of talk that free banking was inherently unstable and led to failures across the banking sector. However, bank failures were not evenly distributed

across the country, showing that certain state laws were better or worse, not that free banking was inherently flawed. It also appears that bank failures were closely associated with the general business cycle (Studenski & Krooss, 2023). Free banking was wrongly tied to the phenomenon known as “wild cat banking.” This was when a bad actor would start a bank, lie about it, collect deposits, and then leave town. However, this was incredibly rare (Rockoff, 1974). Additionally, the failure rates for banks was virtually the same that was experienced in all other businesses, 48%. Even when a bank did close only a small percentage of them did not fully redeem all currency at face value. The stories of “wild cat” banking and massive losses in value were largely overstated (Rolnick & Weber, 1983). The National Bank Acts of the 1860s brought the free banking era to an end and set forth a standard for a national currency. However, state issued bank notes remained in circulation for years following the acts (Studenski & Krooss, 2003).

The 20th century witnessed a shift to central banking with the creation of the Federal Reserve in 1913. The United States entirely abandoned the gold standard in 1971 under President Richard Nixon. The move by Nixon to suspend the convertibility of the US dollar into gold has become known as the Nixon Shock and it effectively ended the Bretton Woods System which had governed the international monetary system. The US dollar became a fiat currency, meaning it was no longer backed by a physical commodity but rather by the trust and confidence of the public in the government.Today, the U.S. dollar serves as the world's primary reserve currency, and the digital era continues to shape the landscape of American monetary transactions.

This telling of the history of money, both throughout the totality of human history and in US history, illustrates several key points:

1. The notion that the institution of money is one that has to be controlled by state actors is not a given; much of the development in making money a better medium of exchange came from the private sector.

2. Money has been changing, developing, and evolving throughout all of human history, and this is not a straight line. In the US, there was private money, then notes issued by colonies and eventually the federal government, but then there was a return to the private issuance of currency during the Free Banking Era. It is unclear and fails to stand up to the body of evidence that the peak of money is fiat paper money in the form of the US Dollar or that the next logical progression must be the digitalization of the US Dollar by the Central Bank.

3. The concept of fiat currency is a modern idea in human history.

The debate over which monetary system is the best has yet to be settled amongst monetary economists, and the foundations of something like Bitcoin are present throughout the literature. Milton Friedman had a complex view of monetary theory. He critiqued the gold standard in believing that the money supply needed to be expanded when necessary. However, he also acknowledged the advantages of commodities and was fearful of central banks mismanaging the money supply. In "*In Search of a Monetary Constitution"*, Friedman wrote, "Money is too important to be left to the central bankers." (Friedman, 1962). He proposed a system controlled by computers rather than humans to make the monetary supply stable, predictable, and insulated from bad influence on monetary policy. The technology is now present for cryptocurrencies to take a similar approach. In the 1970s two economists, Benjamin Klein with his paper "Competitive Supply of Money" and F.A. Hayek in "Denationalisation of Money" challenged the centralization in the issuance of currency by the government of central bank controlled fiat currencies. They argued for the benefits of a monetary system with competing private currencies.

Cryptography

The fundamental basis for all cryptocurrencies is cryptography. Encryption is the method through which cryptocurrencies verify transactions. There is a distinction between cryptography and encryption. Cryptography studies methods to disguise messages in secret, and encryption is the process of actually coding messages. "Encryption is a method for taking some data and obscuring it, so that only someone who has the key can read the original message by decrypting it" (Pritzker, 2019). A form of encryption has been around for thousands of years of human history, dating back to 600 BC in Ancient Sparta (Thales, 2023). These early forms of encryption were symmetric or only used one key to code and decipher the message (Pritzker, 2019). Modern cryptography is based on computer-based encryption, which a group at IBM designed in the early 1970s. They designed a block cipher known as the Data Encryption Standard, which was adopted by the US in 1973 as the national standard. A fundamental change occurred in 1976 when a paper published by Whitfield Diffie and Martin Hellman, Diffie-Hellman key exchange, for the first time made a state where the code key was not determined beforehand but rather based on a pair of mathematically linked keys, one public and one private (Diffie & Hellman, 1976). The public/private key is the technology incorporated into cryptocurrencies.

Cypherpunk Movement

The ideological underpinnings of what became Bitcoin were housed in a group of individuals chiefly interested in the spread of cryptography and other privacy technologies due to their concern over individual privacy in an increasingly digital world. The starting point for the movement was when Dr. David Chaum, widely viewed as the father of digital currency, began writing on the topics in the 1980s, most well

encapsulated in his paper “Security without Identification: Transactions Systems to Make Big Brother Obsolete.” Hal Finney, a prominent Cypherpunk, had this to say about the contributions of David Chaum and the potential of public cryptography:

"Here we are faced with the problems of loss of privacy, creeping computerization, massive databases, more centralization, and Chaum offers a completely different direction to go in, one which puts power into the hands of individuals rather than governments and corporations. The computer can be used as a tool to liberate and protect people, rather than to control the” (Finney, 1992).

In the early 1990s, the movement had become more organized, and Eric Hughes, a prominent member of the group, published “A Cypherpunk’s Manifesto.” Other members of the group included Timothy May, John Gimore, Julian Assange, Jacob Appelbaum, Dr. Adam Back, and Bram Cohen. In the manifesto, Hughes expressed his chief concerns: “Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know. Privacy is the power to selectively reveal oneself to the world” (Hughes, 1992). Hughes makes the distinction between privacy and secrecy which is important to make. Frequently, governments have employed the “nothing to hide” argument in order to advance surveillance measures.

Furthermore, Hughes laid out the need to spread the use of cryptography throughout society in order to build anonymous systems. Hughes laid the groundwork for what would follow on the digital cash front:

“We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do. We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money (Hughes, 1992).

The Cypherpunks wanted a form of private commodity money that was free of government control because the Cypherpunks believed that we could not rely on the government to grant us the privacy that is necessary. Through the study of the Cypherpunks and early attempts at digital currency, it is clear that the creation of Bitcoin was not a random accident but rather the product of decades of philosophical thought, progress, and work on the economics and computer science fronts.

Early Attempts

Bitcoin was not the first attempt at digital currency, but rather the first successful one that could answer the problems of its predecessors. Dr. Chaum first thought of an idea for electronic money in 1983, which he called ecash. Many of these ideas were later implemented in Digicash, which was created in 1989. Digicash used encrypted keys to make the currency untraceable. Digicash was unable to grow. One of the reasons for this is that it was in the market before the revolution of e-commerce and was reliant on being supported by formal banks. Digicash filed for Chapter 11 bankruptcy in 1998, and while not being long-term, it was a prominent first step.

Much of the 1990s was defined by an increase in what can be called the crypto wars, where the government attempted to slow down the spread of commercial encryption. The government, particularly the military, had had a virtual monopoly on the cryptograph market until the rise of the Cypherpunks. The government also placed strict export restrictions on encryption technologies. There were a myriad of legal challenges from libertarians and privacy advocates, but what finally broke the government's back was a successful legal challenge led by Matt Blaze against the Clipper Chip (Lopp, 2016).

Further development was made with Adam Back's Hashcash, which he originally proposed in 1997 and further explained in his 2002 paper "Hashcash- A Denial of Service Counter-Measure." Hashcash was one of the more successful pre-Bitcoin digital currencies. It was a proof-of-work system that could be used to prevent Email spam and DDoS attacks (Loop, 2016). It is much of Back's Hashcash that became Bitcoin mining.

In 1998, Wei Dai proposed "b-money," an anonymous, distributed electronic cash system. Dai's proposal included a system in which each participant maintains their own separate database, a distributed ledger. This system was enforced by making participants put money on the line to incentivize them to be honest (Loop, 2016).

The real turning point for the Cypherpunks and their quest to create digital currency was in the early 2000s. In 2004, Hal Finney created a reusable proof of work (RPOW), which was directly built on Hashcash. Much of the design of RPOW can be seen in Bitcoin's unspent transaction outputs protocol. Finally, in 2005, Nick Szabo proposed "bit gold." This was directly built on RPOWs and was a proof of work system that would have the units valued based on the amount of computer work that was used to create them (Loop, 2016). Szabo had been thinking through his framework for bitgold since 1998, and while it was never implemented, many have seen it as a direct prelude to Bitcoin. These decades of work by the Cypherpunks, building on top of each other and laying the foundational frameworks, led directly to the creation of Bitcoin.

Creation of Bitcoin and Its Design

On the 31st of October,2008, Satoshi Nakamoto, a pseudonym for the still unidentified person or group behind Bitcoin, published the Bitcoin whitepaper on a cryptography mailing list frequented by many Cypherpunks called Metzdowd. For further

proof that the Cypherpunk movement and the creation of Bitcoin are linked, Satoshi directly cited both Hashcash and b-money in the whitepaper as well as there is evidence of email correspondence between Wei Dai and Satoshi in which Satoshi explains that Dr. Back pointed him in Dai's direction and pointed out the similarities between their systems (Loop, 2016).

Satoshi was clear about why he believed Bitcoin was a necessary invention and what problems it aimed to solve.

> "I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. The root problem with conventional currency is all the trust that's required to make it work. The Central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files. Then strong encryption became available to the masses , and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what. It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless. Bitcoin's collusion is to use a peer-to-peer network to check for double spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle" (Nakamoto, 2009).

The case made for Bitcoin by Satoshi is clear. Our current institution of money is unfit for a digital society. Our current financial system is one that is built upon trust of each other and of third parties. There is a massive encroachment of our privacy from the government of individuals, and there is the constant threat of our transactions being censored. The answer for Satoshi is to create a digital form of cash that solves all of these

problems. Bitcoin aims to be a truly revolutionary technology that brings decentralization to money and finance.

The first thing that Bitcoin attempts to do is remove the middleman, financial intermediaries, from the system. By removing the middleman this creates the peer-to peer-system that Satoshi referred to. Banks and financial intermediaries serve as ledgers. Their job is to safeguard and keep accurate information regarding accounts and transfers. Suppose you want to send money to someone else. In that case, you tell a financial intermediary how much and to whom and the intermediary completes and records that transaction in both accounts on their ledger. The ledgers are centralized systems because they have one central actor, a bank or other intermediary, who is the only one who can make changes. The goal of Bitcoin is to make it so the ledger does not have a single authority but instead has many, making it decentralized (Pritzker, 2019).

This is done by everyone wanting to participate by joining a network. Everyone on the network has their own ledger copy. When someone wants to make a transaction, they announce it to everyone on the network, and everyone records that transaction. This is known as a distributed and decentralized ledger. This seems great, but there is still a significant problem, and that is developing consensus among all the various ledgers if there is a discrepancy. It is very easy for there to be consensus failure in a system of majority rule, bad actors can collude together to control the network and ledger for their advantage. Satoshi had to figure out how to make it a permissionless system, meaning anyone can join and make it resistant to bad actors. This is known as the Distributed Consensus Problem or the Byzantine General Problem and is “one of the hardest

problems in computer science: distributed consensus between parties where some are dishonest or unreliable" (Pritzker, 2019).

The answer for Satoshi was to build a system with so many participants, with their identities hidden, so that they would be immune from coercion or violent threats. Satoshi constructed a type of lottery system to add new transactions to the ledger. It operates roughly like this:

1. Anyone can participate in the network
2. People announce transactions to the network
3. Hold a lottery to pick who will write in the new entry
4. Winner writes all the transactions into the ledger
5. If the transactions are valid, then they receive a payment
6. Everyone updates their own ledger copy with the new information
7. Repeat every so often.

This system solves many problems, but there are still questions about how to run it without a central authority or how to trust that the winner acts honestly (Pritzker, 2019).

The lottery has to have several components:

1. Participants have to be able to generate their own tickets so that there is no central authority.
2. The tickets must cost something so that people can not generate infinite tickets.
3. Everyone must be able to verify that the winner actually won.

The solution to these problems is the resulting system colloquially referred to as "Proof of Work." Satoshi did not invent proof of work. It was initially created in 1993 by Cynthia Dwork and Moni Naor, who were looking to use this type of system to thwart spam and DDoS attacks. Adam Black implemented this in his HashCash design. The term "Proof of Work" was first used to describe this system by Markus Jakobsson and Ari Juels in their 1999 paper, and finally, Hal Finney applied proof of work to digital currency.

The system functions like rolling a dice, and each roll generates a lottery number. To do so, your computer must pass information through a cryptographic hash function. These actions require a high amount of electricity, meaning the costs of these tickets are energy costs. To win, you produce a number that is derived from the transactions that will be recorded. There is then also a system for the rest of the participants on the network to verify that the winner is valid. It may take billions of attempts to find the winning number, which costs thousands of dollars in energy, but to check the solution is easy and cheap. Because it costs so much to win, the winner is incentivized to write valid information because if they are rejected, then they will lose all of that money. If correct, they are awarded Bitcoin, which will cover their electricity costs and allow them to make some profit. The computer science behind this is hashing, and Bitcoin institutes the sha256 hash function (Pritzker, 2019).

This process is what Bitcoin mining is. It operates like this.

1. Anyone who wants to join the network by connecting a computer
2. People announce their transactions to the network and spread amongst it.
3. Computers that want to play the lottery start running hash functions
4. About every 10 minutes, a computer will produce a winning number derived from the transactions that is lower than the target number
5. The winning computer announces its winning number and all the information together; this winning combination of information is a block
6. The rest of the computers on the network validate the block to make sure it has all correct information
7. Every computer on the network adds the new block to the ledger along with the rest of the blocks, making a blockchain

This lottery process is also how new Bitcoins are created or “mined.” The winner gets to write an additional transaction, known as a coinbase transaction, giving them an amount of newly issued Bitcoin to cover their electricity costs and make a profit. These blocks can be quickly confirmed by an easy mathematical check, making it so no one can

write an invalid block because the rest of the nodes will reject it. This makes Bitcoin impossible to counterfeit. Because all the blocks are linked together in a chain, any computer on the network can go back and check the work, essentially auditing Bitcoin all the way back to the genesis block that Satoshi originally mined (Pritzker, 2019).

The schedule for the minting of new Bitcoins was set in advance because one of Satoshi's goals was a system immune from debasement or the unending expansion of the money supply. The process he created was known as halving. About every four years, the reward for mining a block will be cut in half. The original reward was 50 Bitcoin in 2008. In April 2024, the reward will be reduced to 3.125 Bitcoin per block. By 2032, 99% of all Bitcoins will be mined, and the reward will be less than 1 per block. In 2140, all 21 million Bitcoins will have been created, and miners will be incentivized by transaction fees. There is a finite amount of space available in each block, and fees are determined by a free market proportional to how much space they take up in a block and how many pending transactions there are (Pritzker, 2019). This means "a transaction that sends 1 million bitcoin from one person to another could actually be cheaper than one that splits 1 bitcoin to 10 recipients because the latter requires more block space to represent" (Pritzker, 2019).

Every block of transactions from the beginning is linked, which is why the ledger is called a blockchain. The ledger, being a blockchain, is also what secures it. Each additional block added to the chain strengthens it, and the ones before are better protected. That is because to change a previous block, a computer has to rerun all the proof of work operations for every prior block to change the one they want to change. This costs an inordinate amount of energy and money. Once a block becomes six deep on

the chain, all of those transactions are considered final. What happens if two miners simultaneously mine a block, causing a division in the network? Which chain is the correct one? This results in a chain split, and Satoshi provides a simple answer in the Bitcoin code: simply wait. When the next block is mined, the chain that has expended the most total energy is considered to be the correct chain; this is known as the Nakamoto Consensus. The other block is rejected, and the miner will not get a reward, and the transactions will not count. Those transactions are not lost; they could have been in the second block, or they will be included in a subsequent block. These splits happen sometimes in the Bitcoin blockchain but are normally fixed in the next block and become less of an issue as network connectivity technology is improved (Pritzker, 2019).

The last thing is how Satoshi designed Bitcoin to accomplish his goal of removing an identity from finance, protecting users' privacy, preventing identity theft, and getting rid of the need for entrusting central third-party actors with our private information. Bitcoin does this through encryption, a method that obscures data so that someone can use a key to read the original message. Bitcoin implements a two-key system known as asymmetric encryption, where one key encrypts and the other decrypts. When you make a Bitcoin wallet you also create an address. You generate a key pair that is mathematically linked together called a public/private key pair. You share your public key with everyone, and they use that to encrypt the transactions they want to send to you. The person wishing to send an address a transaction will sign it with their private keys and the recipient will verify this by running a mathematical check based on the sender's public key (Pritzker, 2019).

In the end, Satoshi and his Bitcoin creation represented a true technological innovation in money and digital currency, in line with the principles of the Cypherpunk movement. Bitcoin created a system that contains “A distributed ledger, a copy of which is kept by every participant. A lottery system based on Proof of Work and difficulty adjustments to keep the network secure from tampering and the issuance schedule consistent. A consensus system that ensures that every participant can validate the entire history of the blockchain for themselves using an open-source piece of software called the Bitcoin client. An identity system using digital signatures that allows for the arbitrary creation of account-like mailboxes that can receive coins without a central authority” (Pritzker, 2019).

History of Bitcoin

Bitcoin has now been around for nearly 15 years and through the years the price of bitcoin has fluctuated dramatically. The world's first transaction of bitcoin took place on January 12th of 2009 when Satoshi gifted Hal Finney, the creator of reusable proof of work, 10 bitcoins (Peterson, 2021). Satoshi was involved with bitcoin at the beginning, mining many of the first blocks, however, he would completely disappear in April of 2011.

One of the first recorded sales of bitcoin occurred in October of 2009, when a Finnish computer science student, Martti Malmi, made a sale of 5,050 bitcoin online over Paypal for a total of $5.02, giving each bitcoin a value of just $0.0009 (Ashmore, 2022). The first time that bitcoin was used as a medium exchange in a real-world transaction was in May 22, 2010, when Laszlo Hanyecs paid Jeremy Sturdivant 10,000 bitcoins for two pizzas (Kaloudis, 2023). This is one of the most high-profile stories of

the early Bitcoin days and it is widely celebrated as Bitcoin Pizza Day by many in the Bitcoin community. At the time of the purchase, Bitcoin was worth around $0.0041 (Ashmore, 2022). While on its face it looks as if Laszlo made a terrible mistake, it may be that without this initial transaction, giving bitcoin monetary value in the real world, bitcoin never would've taken off (Kaloudis, 2023).

Bitcoin first crossed the mark of being worth a dollar for the first time in February of 2011. The price of Bitcoin really began to pick up steam throughout the first half of 2011 reaching a price of $30 per coin by June. At this point, the first Bitcoin payment processor, BitPay was founded in May of 2011 with the goal of providing a platform for businesses to accept Bitcoin as a form of payment. However, this is when the first sign of volatility in the market would show itself with the price of Bitcoin diving to $5 by the end of the year. This would continue throughout 2012 with Bitcoin price bouncing around and ending the year worth about $13 (Ashmore, 2022). 2012 also saw the founding of the now major crypto exchange, Coinbase.

Eventually, there was a massive turning point in the history of Bitcoin and its price broke through $1,000 in November, 2013, a meteoric rise from the price of $13 at the start of the year. Most of this was due to increased access to trading, greater institutional investor support, and greater acceptance as a form of payment (Ashmore, 2022). However, this built up institutional support was short lived and distrust in Bitcoin returned. This occurred due to the collapse of the largest exchange at the time Mt.Gox, an incredibly rudimentary exchange compared to what is available today. Mt.Gox was responsible for 70% of all Bitcoin transactions in the world (Ashmore, 2022). In February of 2014, MtGox abruptly suspended trading and closed their website as well as filed for

bankruptcy. The cause of the insolvency was a severe security breach to Mt.Gox that resulted in hackers stealing 744,000 bitcoins worth tens to hundreds of millions of dollars (BBC, 2014). It had a large institutional effect on how investors felt about Bitcoin and crypto in general. The Mt.Gox event caused the price of Bitcoin to plummet, but by the end of 2016 the price of Bitcoin had recovered to close to $1,000 (Ashmore, 2022).

After years of skepticism toward Bitcoin, there once again was burgeoning interest in it. This was highlighted by a return of investor support, a growing number of businesses accepting Bitcoin, and BitPay announcing that their transaction rate had grown 3 times were major catalysts (Pair, 2017). Bitcoin started to gain legitimacy from traditional financial institutions, such as futures contracts being available on the CME and more acceptance from governments (Ashmore, 2022). For example, Japan passed a law to make Bitcoin a legal method of payment (Kharpal, 2017). All of this began to make many feel that Bitcoin was a true asset, and many doubters were beginning to be won over, sparking a sharp increase in price. Bitcoin started 2017 at $1,000 in a few months it broke through $2,000 and by August it had already doubled again to $4,000.

One of the most significant time periods during the history of Bitcoin occurred between 2015 and 2017 and has been dubbed the “Blocksize Wars.” The war was a debate over the increase of the block size limit in the Bitcoin code in order to allow for the maximum size of a block on the Bitcoin blockchain to be larger. During the early stages of the development of Bitcoin, Satoshi had placed a 1 MB limit on the size of blocks. One of the sides of the block size debate, big blockers, wanted to increase the limit as they believed it would allow more transactions to be processed and for more people to use Bitcoin. They argued this would reduce transaction fees and improve the

scalability of Bitcoin into the future. On the other hand, “small blockers” wanted to maintain the status quo, they argued that increasing the blocksize would make the network more centralized. This is because the large blocks would require greater computing power and thus more energy costs to process which could exclude small miners from being able to participate.

This sort of distinction between big blockers and small blockers can also be seen as one of the reasons for Ethereum. Ethereum and its founders felt that Bitcoin was too limited by not being able to run additional applications on the blockchain. However, it seems that the small blockers were correct. There is a good reason for the blocksize of Bitcoin to be where it is and that is because it does allow the network to remain decentralized. Bitcoin is incredibly good at what the goals it is trying to accomplish. That is being a decentralized, peer-to-peer, form of digital cash. In order to accomplish this it does require tradeoffs. The small blockers favored layer 2 or off-chain scaling solution, like the Lightning Network. In the end the small blockers won out and those in favor of a large block size were forced out through the consensus process. This resulted in a hard fork or a split in the Bitcoin blockchain which created Bitcoin Cash (8 MB block size) and the original blockchain (1 MB block size) in August 2017. Over the last 7 years the market has also seemed to vindicate that the small blockers were right.

After the unprecedented growth of Bitcoin in 2017, a return of 1,388%, led many to call Bitcoin a bubble (Cross et al, 2020). There were also several companies that decided to no longer accept bitcoin due the price volatility (Liao, 2017), and South Korea made traders of crypto identify themselves, potentially signaling fear of what could come of government regulation (Griffin,2018). All of this led to a massive sell-off and crash in

the price of Bitcoin. In January of 2018, Bitcoin fell from over $17,000 to nearly $6,000 (Ashmore, 2022). The decline of Bitcoin in 2018 wouldn't stop there and by November Bitcoin had fallen to Below $4,000 making the 2018 crash of Bitcoin worse than the Dot-Com bubble with an over 80% fall from the peak of Bitcoin, compared to the 78% collapse in the dot-com bubble (Patterson, 2018). The massive crash was not entirely pinned to Bitcoin or its underlying technology, but rather tied to the massive inflation that was experienced due to the ICO boom.

Following the crash in 2018, many financial experts began to use the term "crypto winter." This period in time closely resembled the feeling after Mt.Gox. There was a lack of interest from the broader public or institutional interests. While the mainstream view was beginning to write off Bitcoin as a fad, the Covid-19 pandemic and the response of the Fed bucked this notion. Loose monetary policy and fiscal stimulus saw assets, including Bitcoin, boom, increasing $6,000 in less than two months hitting $10,00 once more in May of 2020 (Ashmore, 2022). Bitcoin would absolutely take off over the next year, hitting an all-time high of over $15,000 in November, over $20,000 in December and $30,000 by the end of the year. The growth was only just beginning. Before even making it halfway through January 2021, the price of Bitcoin was already over $40,000, added another $10,000 by the end of February, and by March it was over $60,000. This sparked a volatile period with the price going all the way below $30,000 over the summer before recovering to an all-time high once again of $69,000 in November. This is the strongest supporting evidence to the claim that Bitcoin can be a hedge against inflation and uncertainty. During a time of uncertainty and a massive increase in the money supply, investors rushed to put their money in Bitcoin.

Price volatility continued and 2022 issued in another “crypto winter”, indicating prolonged and suppressed prices in the crypto market and an overall reduced amount of interest in the asset class. From December 2021 to January 2022, Bitcoin fell more than 50% from its all-time high to below $30,000. The price of Bitcoin has long been associated with major events in the crypto industry at large, and that has been true throughout the last year and a half. Major events affecting the price of Bitcoin have been the Terra/Luna collapse in May 2022, which saw Bitcoin plummet to $20,000. After a brief recovery, the price took another hit following the collapse of Three Arrows capital. Finally, Bitcoin hit two-year lows of nearly $15,000 following the collapse of the crypto exchange FTX in November 2022. Bitcoin recovered to over $20,000 by January 2023 and for most of 2023 the price has been between $25,000 and $30,000.

At the beginning of 2024 the SEC approved 11 Bitcoin ETFs. This was a massive win for the Bitcoin community and something that many interested parties had been pushing for for years. This approval highlights that there is a high level of demand from average investors seeking to gain exposure to the price of Bitcoin for something like retirement. Additionally, two major institutional financial companies, JP Morgan Chase and BlackRock sought approval. This signals an increased level of institutional support for Bitcoin as both Jamie Dimon and Larry Fink have previously been massive skeptics of Bitcoin. This monumental moment in the history of Bitcoin sent prices skyrocketing again, hitting an all-time high of $73,000 in the beginning of 2024.

Development of other Cryptocurrencies (2009-2014)

The growth of cryptocurrencies and the overall crypto industry was rather slow and small for the first five years following the creation of Bitcoin. As mentioned,

throughout the early years of Bitcoin most of the transactions were done directly peer-to-peer through the use of platforms such as PayPal or in person cash transactions. There weren't any major exchanges in operation as by 2014 the largest Bitcoin exchange in the world was Mt.Gox. The current largest exchange in the US, Coinbase wasn't founded until 2013 and their exchange didn't begin operation until 2015. Throughout the early years of cryptocurrencies, there were already signs that the industry would be overrun by a growing number of Ponzi schemes and scams, an issue that still plagues the industry today.

In 2011 the first alternatives to Bitcoin, or other cryptocurrencies, began to be developed, colloquially known as alternative coins or altcoins. Altcoins were brought about by growing interest in Bitcoin as it gained traction. Altcoins are typically designed with the intent to improve upon Bitcoin offering some new feature or advantage. The first major altcoins founded were Namecoin and Litecoin. Litecoin was the more successful of the two and is still a top 20-priced cryptocurrency, trading at $62. Litecoin is a Proof of Work coin founded by Charlie Lee and is the first cryptocurrency to use scrypt as a hashing algorithm. The goal of Litecoin was to improve upon Bitcoin and fix inefficiencies that Lee identified, primarily improving the ease and speed of transactions and improving issues around security. 2013 saw the founding of the industry's largest memecoin, Dogecoin, based on the Doge internet meme of a picture of a Shiba Inu dog. It also saw the launch of the cryptocurrency XRP by Ripple, which was a settlement asset and has been under intense scrutiny from the SEC as Ripple raised funds by completing unregistered security sales.

While the crypto market/industry was nearly unrecognizable to what is seen today during the years from the creation of Bitcoin through 2014, there was still a significant amount of growth. The market cap for crypto was only about $1.5 million by the end of 2010 but had grown massively to $140 million in 2012. By the end of 2014, the market cap was above $4.5 billion (Faulkner, 2023). In 2013 there were 66 cryptocurrencies in circulation (de Best, 2023). There were many major crypto companies founded during this time including Coinbase, Bitpay, and Xapo, helping improve the ease of usage, purchase, and storage of cryptocurrencies. By the end of 2014 one of the first stablecoins, Tether (USDT), pegged to the US dollar, was created. Tether has remained one of the most popular stablecoins and the concept of stablecoins have continued to grow for a variety of use cases, amongst them being a way for traders to move funds between exchanges without using traditional fiat currencies.

Creation of Ethereum

Ethereum, created by Vitalik Buterin and proposed in late 2013, is a decentralized blockchain platform designed to enable the creation and execution of smart contracts and decentralized applications (Dapps). Ethereum launched a crowdfunding effort known as an initial coin offering (ICO) which raised more than $18 million. The Ethereum Blockchain network launched on July 30, 2015. It goes beyond the functionality of Bitcoin by incorporating a flexible and programmable environment

At the heart of Ethereum's design is the concept of smart contracts. These self-executing contracts with coded terms and conditions automate and enforce the execution of agreements. Smart contracts are written in Ethereum's native programming language, Solidity, and are stored on the blockchain, making them tamper-proof and transparent.

Ethereum features a decentralized virtual machine (EVM), which executes the code of smart contracts. The EVM allows developers to create complex applications by providing a Turing-complete environment. This versatility empowers developers to implement a wide range of functionalities, from financial transactions to identity verification.

Ethereum employs a blockchain, a distributed ledger that records transactions across a network of nodes. The consensus mechanism was initially Proof of Work (PoW) and transitioned to Proof of Stake (PoS) in Ethereum 2.0. Ether is Ethereum's native cryptocurrency, serving multiple purposes. It acts as a fuel for executing smart contracts (gas), a store of value, and a means of compensating participants who contribute to the network's security through mining or staking.

Ethereum's primary purpose is to facilitate the creation and deployment of decentralized applications. Dapps operate on the blockchain, providing users with secure, transparent, and trustless interactions. These applications span various domains, including finance (DeFi), gaming, supply chain management, and identity verification. Ethereum is a pivotal platform for the explosive growth of decentralized finance. DeFi applications built on Ethereum enable peer-to-peer lending, decentralized exchanges, and yield farming, among other financial services. The programmability of Ethereum allows developers to create complex financial instruments and protocols.Ethereum's design allows for the creation of custom tokens through a standard known as ERC-20. These tokens represent assets or utilities within the Ethereum ecosystem, enabling crowdfunding (Initial Coin Offerings or ICOs) and the creation of digital assets ranging from stablecoins to non-fungible tokens (NFTs).

Growth of the Crypto Industry (2015-Present)

The last near decade has seen an explosion of growth in the broader crypto industry. The launch of Ethereum served as the launching point for much of this development. The success of the 35thereum ICO led many others to jump onto this fundraising mechanism as a way to support blockchain and token projects. This became an emerging trend that would continue in the market for years to come. The features of the Ethereum blockchain allowed for an explosion of new coins to be created.

The Gemini crypto exchange, led by the Winklevoss twins, most famously known for their role in the creation of Facebook and the lawsuit that followed, was launched in 2015. Gemini has long held a legitimate and reputable crypto exchange due to all of the regulatory hoops that it jumped through. This is because the exchange is one of the only exchanges to be fully regulated as it is licensed by the New York State regulator, the New York State Department of Financial Services (NYDFS). The Winklevoss twins have also been some of the leading proponents of establishing federal regulatory standards for the industry. Gemini has a strong system of security measures and has never been hacked, offers insurance coverage for assets held in its custody, has its own stablecoin, Gemini Dollar (GUSD), and has engaged in a variety of education initiatives to advocate for the broader adoption of cryptocurrency in the financial system. The Winklevoss twins filed for regulatory approval for the Winklevoss Bitcoin Trust (COIN), a Bitcoin exchange-traded fund (ETF). While the ETF proposal faced several setbacks and delays, it marked an early attempt to introduce traditional financial instruments tied to cryptocurrencies. The quest to establish a Bitcoin ETF has been a long process in the investment community.

A major event in 2016 was the exploitation of a vulnerability in a decentralized autonomous organization (DAO) built on the Ethereum blockchain. This led to a significant amount of Ether (ETH) being transferred to the hacker. In response, the Ethereum community executed a contentious hard fork to reverse the effects of the hack. This resulted in the creation of two separate chains, Ethereum (ETH) and Ethereum Classic (ETC). This was a significant moment in the early history of the Ethereum blockchain and potentially pointing out some of its flaws.

The ICO trend that began in 2015 continued to gain momentum in 2016. Numerous blockchain projects conducted initial coin offerings to raise funds for development. Notable ICOs included those of Golem, Augur, and ICONOMI. An ICO or Initial Coin Offering was a way for new blockchain projects to sell tokens in order to raise funds for the development of their project. The ICO boom saw a massive amount of venture capital investment flooding into the market. This led to a rise in altcoins, or alternative cryptocurrencies, gained prominence as investors sought opportunities beyond Bitcoin. Cryptocurrencies like Ripple (XRP), Litecoin (LTC), and Cardano (ADA) experienced substantial price increases and increased market capitalization. The ICO boom marks a significant shift in the overall tone of the crypto industry. Following the remarkable price surges in 2017, 2018 saw a significant market correction. The prices of many cryptocurrencies, including Bitcoin and Ethereum, experienced substantial declines, leading to a more prolonged bear market. The driving factor of this decline was the bursting of the ICO bubble in February of 2018 which represented the crash seen during the Dot.com bubble.

In mid-2019, Facebook announced its intention to launch a cryptocurrency called Libra (later rebranded as Diem). The project faced intense regulatory scrutiny and raised concerns among policymakers globally, leading to delays and reevaluation of the initiative. Concerns about its potential impact on the global financial system led to regulatory scrutiny, hearings in the United States Congress, led to several key partners withdrawing their support, such as Mastercard and Visa.

In December 2020, the U.S. Securities and Exchange Commission (SEC) filed a lawsuit against Ripple Labs, alleging the sale of unregistered securities through the XRP cryptocurrency. The lawsuit had significant implications for the regulatory status of certain cryptocurrencies. While there had been actions by the SEC before in the crypto market this was one of the first major cases against a major alternative token and foreshadowed what was to come from the SEC under the command of Gary Gensler. The case also highlights the ongoing debate between whether cryptocurrencies represent a security or a commodity.

Ethereum's price surged in 2021, and the network continued to be a hub for decentralized finance (DeFi) and non-fungible tokens (NFTs). Progress was made on Ethereum 2.0, with the Beacon Chain already launched, marking the beginning of Ethereum's transition to a proof-of-stake consensus mechanism. Cardano, a blockchain platform known for its focus on sustainability and scalability, completed the Alonzo upgrade in 2021. This introduced smart contract functionality, enabling developers to build decentralized applications (Dapps) on the Cardano blockchain. Several cryptocurrency exchanges, including Coinbase and Kraken, explored or completed initial

public offerings (IPOs) in 2021. Coinbase went public in April through a direct listing on the NASDAQ, marking a significant milestone for the industry.

A lot of these developments coincided with the surge in popularity surrounding the concept of Web3. The term Web3 was created by Gavin Wood in 2014. Wood is the co-founder of Ethereum and the founder of the blockchain company Polkadot. Web3 is the notion of reorganizing the internet into a new decentralized model built on the technology of blockchain. Polkadot was founded in 2020 with the goal of being able to link together blockchains, fitting into and helping to facilitate Wood's concept of Web3.

Non-fungible tokens (NFTs) gained widespread attention, leading to a surge in digital art sales and blockchain-based collectibles. Several high-profile NFT sales and collaborations between traditional artists and blockchain platforms occurred. The massive growth in the market was driven by a massive marketing plot by many in the industry. This market has in large part crashed from the highs it reached in 2021. In a similar vein, the meme token, DogeCoin, experienced a massive surge in its price. This was done through an online campaign, which started in online chat boards, eventually migrating onto Twitter. The goal was a futile attempt to pump Doge to $1 or "to the moon", very similar to the ploys used during the GameStop Saga. DogeCoin went from a job to soaring over 18,000% in a short period of time reaching an all time high of 73 cents and currently in trading at 7 cents.

Then the fraud started. Throughout 2022 a lot of bad actors in the crypto market had their schemes unearthed and crumbled, causing waves throughout the industry. In May 2022, the Terra/Luna algorithmic stablecoin lost its peg and collapsed. Largely driven by the collapse of the UST stablecoin, the inept practices of the crypto lending

company Celsius were brought to light. The company halted customer withdrawals in June and filed for bankruptcy in July. Then at the end of the year in November, the major cryptocurrency exchange FTX collapsed and filed for bankruptcy when their balance sheet showing many irregularities was leaked.

Following the disastrous 2022 for the industry, 2023 brought a heightened amount of regulatory scrutiny especially in the American perspective. The US Congress began holding several hearings on digital assets and working towards passing comprehensive pieces of legislation for both Stablecoins and the broader cryptocurrency market. Most of the regulatory work has come through enforcement actions from the SEC. In June of 2023 the Securities and Exchange Commission (SEC) announced lawsuits against two major crypto exchanges, Coinbase and Binance. The lawsuits claim that the exchanges had been allowing the buying and selling of unlicensed securities.

The launch of Ethereum and the success of their ICO can be viewed as the major turning point in the crypto movement. After Ethereum was able to successfully raise millions of dollars from their ICO many other developers looked to do the same. Since then many projects have been launched pledging to be the next big thing and better than Bitcoin. They claim that with this money from venture firms they will be able to develop their blockchain and attract more users. One prime example of this was Solana, which was launched in 2018 by the former head of development at Qualcomm. He pledged to make Solana an Ethereum killer and was able to raise millions of dollars. These projects would gin up massive marketing campaigns before the tokens were listed on a trading platform like Coinbase. Once they were, a large number of average investors would buy these tokens only to see the price of the token immediately start to drop as VC firms

cashed in their returns. In many ways the crypto currency can be viewed as a new Silicon Valley, with these blockchain projects being analogous to tech firms.

There are now thousands of tokens in the marketplace, most of them that don't make much sense. Take the Munchee token for example, which was supposed to be a food review token of some sort as well as a social media app. The company had planned for an ICO, but the SEC halted it. There are numerous tokens that have ludicrous schemes like this. They operate almost like a worse version of a rewards app at a fast food restaurant. There is even a token that is supposed to be redeemable for a Costco hotdog on the Solana blockchain. There is now a growing number of influencers that will cite these tokens as reasons to invest in a certain project or attempt to pump up these goofy tokens. The crypto market now operates like a casino. Average investors look at the thousands of tokens or pick from some new offshoot project and hope that it will be the next big thing. The cryptocurrency movement, which started as a group of innovators attempting to solve real problems and provide sound forms of currency, has devolved into something that is hardly that.

Conclusion

It is clear through the study of the history of the development of cryptocurrency that led to the creation of Bitcoin, was a legitimate innovation. It was the years of hard work and study and many researchers building on the efforts of one another that culminated in the creation of a new technology, one that follows in the long line of human history, developing new forms of currency. Private money, outside the scope of government, is not a new concept, it is in fact the way money got started in the first place, and also has a place in the history of the United States. Economists, Benjamin Klein and

F.A. Hayek spent time thinking about what it would look like to create a private currency outside of government once again in the 1970s. Bitcoin was not a mistake or the random thought of a guy one day, but rather the culmination of deep thinking, economic research, and computer science development. As Bitcoin gained traction and popularity many other actors have entered the crypto space and, in many ways, the original concept of Bitcoin and the work of the Cypherpunks is hard to recognize.

CHAPTER IV: USE CASES

Satoshi and the Cypherpunks were clear about their aims and the purpose of digital currency. They viewed the increasing digitization of our financial system as a threat to individual privacy. If your banking and payment history, as well as your information, is available online, then it is possible for someone to access it. We are increasingly becoming a cashless society; Americans are reporting using cash less and less, and the most recent estimate from the Federal Reserve (Fed) found that only 1 in 5 transactions in the US are completed in cash (Jones, 2022). Beyond the general trend of consumers moving away from cash, a growing number of businesses are not accepting cash. Physical cash used to be the alternative for those seeking privacy, but that is increasingly becoming a less viable option. That is why the goal of the Cypherpunks and all of their work was to develop a form of electronic cash that is suitable for our modern era of finance. Satoshi wrote, "The root problem with conventional currency is all the trust that's required to make it work" (Nakamoto, 2009). The element of trust is littered throughout our financial system, but Bitcoin can remove that need for trust and offer many advantages to traditional currency and finance.

Innovation: Better Money

There is a widespread perception amongst many, including prominent economists, that money cannot exist without government. This assumption does not follow the long history of monetary developments in human history. As mentioned earlier in the *History of Money* subsection, a private monetary system is not only viable, but the norm in

human history. As economist Lawrence White writes, “the origins of money and the development of better monetary institutions have stemmed from private initiative rather than from government” (White, 2023). The totality of human history showcases the role of the private sector in the development of money and monetary institutions, and there is precedent for private money in the United States, most notably during the free banking period from 1837 to 1864. It is entirely plausible that Bitcoin can represent an innovation in money, returning to private money, but this time, it removes the middleman and allows for privacy, amongst other advantages. Due to the decentralized nature and design of Bitcoin, the need to trust the issuer of the currency, as experienced in other periods of private money, has been removed. In the past, banks would issue their own forms of currency in the form of bank notes. However, there was still an element of trust that was required in these institutions. If you received a note redeemable for 1 oz of gold, you had to trust that the issuer had that gold to give you if you chose to cash it in.

This element of trust was still present in early forms of electronic cash that the Cypherpunks attempted; David Chaum’s Digicash would be a perfect example. Digicash was centralized, with one corporation issuing the currency and verifying payments. Digicash was also reliant on partnerships with traditional financial institutions, such as banks, where users stored their cash. This is the same problem that private currencies have run into throughout history. Bitcoin’s design, as mentioned previously, was able to solve these problems by being decentralized and not needing to rely on a central actor or third parties.

Many have argued that Bitcoin is worthless or can not be money because it is not “backed by anything.” This argument can also be applied to fiat currency or money

backed by the "faith" of the government. There is nothing of inherent value that is used to back currency like the US dollar, but we all acknowledge that it has value. The same can be said for even a trusted commodity like gold; what is inherent about gold that has provided its value over millennia?

Let us break down this argument from the beginning: What is money? There are three primary features of money.

1) Medium of Exchange
2) Store of Value
3) Unit of Account

Based on these three principles, Bitcoin would be classified as money (Hileman, 2014). Certain characteristics have been identified that can make one form of money a better medium of exchange. Some of these include durability, you don't want your money to deteriorate over time. This was a problem with using tobacco leaves for example as a currency. Bitcoin is incredibly durable as the network will always run unless all nodes on the network are shut down. Another is divisibility, or the ability to divide an amount of money into smaller increments. This is another thing that bitcoin can accomplish. Finally, is the ability to transport it, this was a problem with coinage because it was difficult to carry pounds of gold coins around with you at all times and it was this problem that in part contributed to the advent of paper money. Bitcoin is incredibly easy to transport as it is digital and can be accessed from a computer or phone.

We can also look at Ludwig Von Mises's Regression Theorem, which he posses in his 1912 book, *The Theory of Money and Credit,*

"The theory of the value of money as such can trace back the objective exchange value of money only to that point where it ceases to be the value of money and becomes merely the value of a commodity…. If in this way we continually go farther and farther back we must eventually arrive at a point where we no longer find any component in the objective

> exchange value of money that arises from valuations based on the function of money as a common medium of exchange; where the value of money is nothing other than the value of an object that is useful in some other way than as money… Before it was usual to acquire goods in the market, not for personal consumption, but simply in order to exchange them again for the goods that were really wanted, each individual commodity was only accredited with that value given by the subjective valuations based on its direct utility" (Von Mises & Batson, 1912).

Mises argues that you can trace back or regress the value of money to its utility. On its face, people may dismiss Bitcoin and say it would fail to meet this definition. However, there is a good argument to be made. Bitcoin is not just a currency but also a payment system. It is designed to allow for peer-to-peer transactions. This gives Bitcoin utility and, thus, value under the regression theorem (Tucker, 2023). In many ways, the regression theorem better applies to Bitcoin than the US Dollar because what is the inherent utility of a fiat currency backed by the "faith" of the government?

Going back to Lawrence White, "the origins of money and the development of better monetary institutions have stemmed from private initiative rather than from government (White, 2023). Private currency was the norm of human society, but over time, the government began to monopolize the supply of money. Perhaps they could have made the case that this system was unreliable and that issuers were untrustworthy. While there are certainly examples of fraudulent issuers, this was not the norm, and the market had a way of rooting out these actors (Studenski & Krooss, 2003). Even given this, it is at least a plausible argument that could have been made. However, the evidence tends to suggest that governments monopolized the supply of money not because it was correcting a market failure or providing greater value but rather for political reasons. The government sought out a monopoly on money due to the power it grants them for raising revenue, specifically for emergency financing during times of crises or war

(Hendrickson, 2024). This begs the question of whether the state should have a monopoly on money.

This has been a question that monetary economists have long discussed, and there is no clear consensus on this question. Benjamin Klein concluded in *The Competitive Supply of Money* that a monetary system based on competing private money issuers would not result in high money prices or hyperinflation as long as these issuers could prevent counterfeiting (Klein, 1974). As mentioned, the design of Bitcoin renders it nearly impossible to counterfeit.

Perhaps the harshest critic of the government monopoly on money was economist F.A. Hayek. He frequently advocated for a competitive market of privately issued currencies where customers could choose their currency.

> "What is so dangerous and ought to be done away with is not governments' right to issue money but the *exclusive* right to do so and their power to force people to use it.…Why should we not let the people choose freely what money they want to use? … If governments and other issuers of money have to compete in inducing people to hold their money…they will have to create confidence in its long-term stability… I hope it will not be too long before complete freedom to deal in any money one likes will be regarded as the essential mark of a free country" (Hayek, 1976)

In many ways, the rise of Bitcoin and other cryptocurrencies is giving people this again. Consumers now have choices in a market for money. They can choose to use US dollars because it is accepted everywhere and relatively stable. They can elect to use Bitcoin because it offers value in being a digital cash that is based on principles that make it function like a digital form of gold. There are also options to choose a different cryptocurrency because the ability to make instant transactions or run applications on the blockchain provides utility to the user.

Decentralization: Removing the Middleman

Bitcoin is a peer-to-peer version of electronic cash, allowing for any two parties to directly make a transaction between one another without the need of a trusted third party, the middleman. Why is this important? More and more transactions are occurring electronically, and they have to be processed through some third-party institution, whether that be a bank, a credit card company, or some other institution. The necessity of using a third-party intermediary means that trust enters the equation. Both parties have to trust that the middleman will not screw one of them over or make a mistake. This reinforces one of the elements of trust that Satoshi mentions, "Banks must be trusted to hold our money and transfer it electronically, but then lend it out in waves of credit bubbles with barely a fraction in reserves" (Nakamoto, 2009). This might seem silly or doesn't matter, but history shows it is a valid fear.

There is a long history of bank failures in the United States that have resulted in the loss of customer money. Primarily, this has been the result of bad lending practices. During the Panic of 1907, many Trust Companies failed or were put under immense stress due to their heavy involvement in the overnight call loan market (Studenski & Krooss, 2003). In the 1980s and early 90s, more than 1,600 banks failed or had to receive assistance from the FDIC. The primary culprit was the Savings & Loans market, resulting in billions of dollars of lost customer funds (FDIC, 1997). During the financial crisis from 2008 to 2013, 489 banks failed primarily due to the lousy lending of banks, principally in terms of granting bad mortgages to people who could not pay them back (Buchwald, 2023). Just recently, Silicon Valley Bank failed due to the lack of diversification and risk management in the bank's balance sheet.

Beyond failures, there are other concerns about trusting your money to intermediaries. Banks have frequently frozen or closed customer's accounts without explanation (Meyer, 2023). This is prevalent in the largest banks in the country, but one of the most prominent examples is the Chime banking app. Jonathan Marrero was locked out of his $10,000 account after receiving this email from Chime, "We regret to inform you that we have made the decision to end our relationship with you at this time. Your spending account will be closed on March 18, 2021" (Kessler, 2021). He is far from alone, as there have been 920 complaints filed against Chime with the Consumer Financial Protection Bureau for similar instances (Kessler, 2021). Rather than mandating a return to paper cash, Bitcoin offers a different solution for removing the middleman: private electronic money.

Cryptocurrency represents a revolutionary shift in the financial landscape by eliminating the need for traditional intermediaries, often referred to as middlemen. In conventional financial systems, transactions typically involve banks, payment processors, or other financial institutions that act as intermediaries, facilitating and validating transactions between parties. These intermediaries add both costs and time delays to financial transactions. Cryptocurrencies, operating on decentralized blockchain technology, remove the middleman from the equation, enabling peer-to-peer transactions.

The removal of intermediaries is particularly evident in cross-border transactions. Traditional international transfers often involve multiple banks and intermediaries, leading to higher fees and longer processing times. Cryptocurrencies, functioning on a global scale without the need for centralized control, allow individuals to transact directly with one another across borders. This not only streamlines the process but also

significantly reduces costs associated with currency conversion and intermediary fees, democratizing access to financial services for a global audience.

Moreover, the absence of intermediaries enhances financial inclusivity. Cryptocurrencies provide individuals who are unbanked or underbanked with direct access to a digital financial ecosystem. Cryptocurrencies empower users to take control of their finances by eliminating the dependency on traditional banking structures, fostering greater financial autonomy, and reducing reliance on centralized entities. This transformative aspect of cryptocurrencies has the potential to reshape the financial landscape, making it more accessible, efficient, and equitable for people around the world.

Privacy

Cryptocurrencies play a pivotal role in improving privacy in the digital age, offering innovative solutions to the growing concerns surrounding personal data security. The data supports that this is a widespread concern among Americans. A Pew Research poll found that most Americans believe it is impossible to go through everyday life without having data collected about them. Additionally, over 80% said they have little control over the data collected, and 80% say the risks of data collection by firms and the government outweigh the benefits (Auxier et al., 2019). These concerns were the top priority for the Cypherpunks and something that Satoshi also mentioned:

> "A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what. It's time we had the same thing for money.

With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless" (Nakamoto, 2009).

Traditional finance institutions, such as credit card companies, banks, and payment processors, serve as massive information repositories. Not only do you have to trust the actors to be good stewards of your information and not to be nefarious, but these large centralized data centers serve as a giant bullseye for hackers. This is something that Satoshi also pointed out, "We have to trust them with our privacy, trust them not to let identity thieves drain our accounts" (Satoshi, 2009). There are a plethora of examples of data breaches in financial institutions where consumer information has been lost.

In May 2019, 886 million financial and personal records were leaked from The First American Corporation due to a simple website error. One of the largest data breach disasters occurred with Equifax in September of 2017 when 147 million customers had their names, date of birth, Social Security numbers, Driver's license numbers, and credit card numbers leaked due to lackadaisical cyber security practices. This data breach was estimated to impact up to 40% of Americans. Russian hackers used malware injections to compromise 130 million credit and debit card numbers from Heartland Payment Systems in January 2008 (Kost, 2023).

Banks have not been safe from cyber-attacks and data breaches. In 2014, JP Morgan Chase was hacked, and the personal information of 83 million accounts was stolen. There have also been two recent data breaches within banks, one at Flagstar bank in 2022, when 1.5 million customers had their personal and banking information as well as Social Security number obtained by hackers (Kost, 2023). Just this past summer, 11,000 Bank of America customers had their Social Security numbers and financial account information stolen during a leak (Steven, 2023).

To show that there are no safe havens within our digital society, Sony and PlayStation Network Servers were hacked in 2011. This included personal information and financial information tied to the Playstation Network Store. The server stored consumer credit card information when used to purchase content online, and hackers indicated that they had accessed more than 2 million credit cards during the attack (Arthur, 2020).

One key advantage lies in the decentralized nature of cryptocurrencies, as they operate on blockchain technology. Unlike traditional centralized systems, where a single entity can control and potentially misuse vast amounts of personal data, cryptocurrencies distribute transactional information across a network of nodes. This decentralization ensures that there is no single point of failure, significantly reducing the risk of large-scale data breaches that could compromise the privacy of millions of individuals.

Furthermore, the use of pseudonymous addresses in many cryptocurrencies enhances user privacy. Instead of revealing personal details during transactions, users transact using cryptographic addresses. This pseudonymity provides a layer of privacy, as users can engage in financial activities without exposing their real-world identities. While the blockchain ledger is transparent, the link between a user's identity and their transactions is not inherently visible, safeguarding their privacy.

In the digital age, where online surveillance and data mining are prevalent concerns, cryptocurrencies offer a refuge. Traditional financial institutions often collect extensive metadata on individuals, including spending habits, location data, and transaction history. Cryptocurrencies, on the other hand, allow users to control the extent of information they disclose. With careful use of privacy-focused cryptocurrencies and

techniques, users can conduct transactions with a level of anonymity that is challenging to achieve in traditional banking systems.

Additionally, the cryptographic principles underlying cryptocurrencies provide a robust layer of security. Transactions are secured through complex cryptographic algorithms, making it extremely difficult for unauthorized parties to alter or manipulate the transaction history. The secure, tamper-resistant nature of the blockchain contributes to the overall improvement of digital privacy, ensuring that the integrity of personal financial data remains intact.

Beyond fear of hacking, there are ample reasons to be skeptical of trusting financial intermediaries with your financial information and the government. Following the January 6th Capitol riot, Bank of America voluntarily turned over the banking records of hundreds of people in the area to the FBI. All of these people turned out to be innocent (O'Neill, 2021). The Canadian government invoked an emergency act to freeze the bank accounts of hundreds of trucking protesters who were peacefully protesting the country's vaccine mandate (BBC News, 2022).

There is a long history of the government attempting to gather financial information from citizens. In 1990, the US founded the Financial Crimes Enforcement Network (FinCEN), which is a bureau within the US Department of the Treasury that collects financial data with the mission of preventing financial crimes. This has led to a rise of Know Your Customer (KYC) laws and regulations, which place requirements on financial institutions such as banks to collect information to identify their costumers, understand the nature of their activities, and assess the potential risks. These requirements

fit underneath the larger umbrella of government work on anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

In recent years, the Treasury Department has proposed implementing a new reporting requirement for banks so that the government can collect more financial information to prevent things like tax evasion. The proposal would require banks to report to the IRS, including the total amount of money flowing in and out of a bank account if it exceeds $600. This proposal has drawn stark backlash from the banking industry and privacy advocates as this would essentially encapsulate all Americans, “The American Bankers Association has said the reporting requirements would capture too much information from too many Americans, and has vowed to oppose any effort to get banks to disclose more information — regardless of how high the dollar threshold goes” (Ivanova, 2021).

It is these types of proposals and the push from the government to gather more financial information that once again shows the value of cryptocurrency and the privacy that it offers. It also has many people concerned over what the future could hold, with some in government calling for a Central Bank Digital Currency , which could mean that the government would have access to all financial transactions of American citizens. The work of the Cypherpunks and the invention of Bitcoin brought cryptography to finance, protecting the right to financial privacy for users that has been on the downtrend in America for 50 years (Anthony, 2023).

Hedge Against Inflation and Potential in Foreign Countries

Cryptocurrency has emerged as a potential hedge against inflation and a means to escape the impact of bad monetary policies implemented by central banks. Satoshi wrote,

“The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of the trust” (Nakamoto, 2009). Unlike traditional fiat currencies, which are subject to inflationary pressures as central banks can increase the money supply, many cryptocurrencies have built-in scarcity mechanisms. For instance, Bitcoin has a capped supply of 21 million coins, making it resistant to inflationary pressures. This scarcity is designed to mimic the characteristics of precious metals like gold, making cryptocurrencies a store of value that can potentially preserve wealth in times of economic uncertainty.

In situations where governments implement poor monetary policies, such as excessive money printing or currency devaluation, cryptocurrencies can offer an alternative financial refuge. Citizens experiencing the negative effects of inflation, which erodes the purchasing power of their money, may turn to cryptocurrencies as a way to safeguard their wealth. This is particularly relevant in countries facing economic crises, where citizens seek alternatives that are not subject to the same vulnerabilities as their national currencies.

This is precisely what Hayek was talking about when calling for an end to government monopoly on money. “Practically all governments of history have used their exclusive power to issue money in order to defraud and plunder the people” (Hayek, 1976). Governments frequently run massive deficits and, in turn, have resorted to money printing or monetizing the debt in order to finance these debts, and the result has been the stealing of their citizen’s money through inflation.

From the American perspective, this might seem like it is not a concern. The United States Dollar is the standard of global currency. However, recently, the US

experienced high inflation of about 9% at its peak (BLS, 2022). Over the last four years, cumulative inflation in the United States has totaled over 20% (Tobey, 2024). The US also experienced two stints of double-digit inflation in the 1970s and the early 1980s. Most of this inflation can be directly linked to the Federal Reserve's monetary policy (Bryan, 2013). Even in a country like the United States, with a currency as strong as the US Dollar, inflation still represents a significant concern. Granted, the volatility that has been associated with cryptocurrencies makes it hard to be viewed as a good bet against inflation. However, the volatility in the price of crypto or Bitcoin is not a function of the asset or technology, but rather experienced because Bitcoin is not the standard payment method. If Bitcoin were to supplant the US dollar, the volatility could disappear.

The notion that Bitcoin can not serve as a suitable escape from inflation or central bank debasement is based on American privilege. Numerous countries do not have a stable monetary base or currency. In Venezuela, as a result of their autocratic government, excessively printing money has seen their currency become essentially worthless in the last 10 to 15 years. "The Venezuelan Bolivar went from 2 Bolivar to the U.S. dollar in 2009 to 250,000 Bolivar to the US dollar in 2019 (Pritzker, 2019). The Argentine Peso has a long history of inflation. In the 1970s and 1980s, Argentina experienced hyperinflation with 300% annual inflation rates. These inflationary pressures have returned to the economy, with the annual inflation rate hitting 161% (Nessi, 2023). The Argentine Peso went from 2.93 pesos to the U.S. dollar in 2003 to 803 pesos to the U.S. dollar. What do the people in these countries and many others worldwide have to lose by putting their money in something like Bitcoin when they know their monetary

base is unstable? The money they already have is either worthless, or they know that its purchasing will be worth considerably less year after year.

Cryptocurrencies also provide a means for individuals to escape capital controls or restrictions on financial transactions imposed by governments. In scenarios where traditional financial systems are subject to government interventions, people may turn to cryptocurrencies to maintain control over their assets and conduct cross-border transactions without the same level of scrutiny. The decentralized and borderless nature of cryptocurrencies allows users to circumvent certain limitations that might be imposed by national monetary policies, providing a degree of financial autonomy in the face of economic challenges. The global accessibility of cryptocurrencies further contributes to expanding financial services in regions where traditional banking infrastructure is lacking or unreliable.

Low-cost, High-speed Transactions

Cryptocurrencies have revolutionized the financial landscape by introducing a paradigm shift towards low-cost and high-speed transactions. Traditional financial systems often involve multiple intermediaries, such as banks and payment processors, each imposing fees and contributing to delays in transaction processing. In contrast, cryptocurrencies leverage blockchain technology to enable peer-to-peer transactions, eliminating the need for intermediaries and substantially reducing associated costs. This direct and decentralized approach allows users to transfer value globally with minimal transaction fees, democratizing financial transactions and making them more accessible to a broader population.

The speed of cryptocurrency transactions is a key advantage, particularly in cross-border payments. Traditional international transfers can take days to settle due to the involvement of intermediary banks and the reliance on legacy financial infrastructure. Cryptocurrencies, operating on decentralized networks, facilitate near-instantaneous transactions, significantly reducing the time required for funds to move across borders. This speed is particularly advantageous in global commerce and remittances, where the ability to settle transactions quickly can enhance efficiency and reduce the impact of currency exchange rate fluctuations.

Moreover, the 24/7 nature of cryptocurrency markets ensures continuous transaction availability, allowing users to engage in financial activities at any time without being constrained by banking hours or national holidays. This accessibility, combined with low costs and high speed, positions cryptocurrencies as a disruptive force in the financial industry, offering a compelling alternative to traditional payment systems for individuals and businesses.

Stablecoins

Stablecoins serve as a bridge between the volatility of cryptocurrencies and the stability of traditional fiat currencies, offering a range of practical use cases in the digital economy that differ from those offered by Bitcoin or other coins. One primary function is as a store of value, providing users with a cryptocurrency that maintains a stable value by pegging it to a fiat currency, such as the US Dollar. This stability makes stablecoins an attractive option for individuals and businesses looking to hedge against the price fluctuations often associated with other cryptocurrencies like Bitcoin or Ethereum. Moreover, stablecoins facilitate seamless and efficient cross-border transactions, enabling

users to transfer value internationally without exposure to the exchange rate volatility inherent in traditional currency transactions. Stablecoins, such as USDC, Tether (USDT), and DAI, have become integral to the cryptocurrency ecosystem, providing a reliable medium of exchange, a stable unit of account, and a store of value for users engaging in various financial activities (Su, 2021).

Stablecoins have begun to gain attention in the context of national security applications, particularly in the realm of international trade and financial transactions. The ability to move money at a quicker pace is becoming more important to ensure competitiveness. Incorporating payment stablecoins is becoming a key component of ensuring the dominance of the US Dollar in the global market, which is crucial for US competitiveness and national security. Circle, a leading stablecoin company, had its CEO, Jeremy Allaire, testify on the Hill. In his testimony, he stated

> "All eyes are on the US dollar, and the steps that the US government takes in the coming years will have a significant impact on dollar competitiveness in the decades that follow. Failing to take the appropriate steps could have devastating consequences for our country. […] As a nation, we need to ensure that the dollar is the most competitive currency on the internet, and that there can be universal access to the safest and most secure digital dollars possible. The stakes are simply too high to ignore."

The stability they offer makes stablecoins a potential tool for countries to mitigate the risks associated with currency volatility. In cross-border trade, stablecoins can streamline transactions, reducing the impact of exchange rate fluctuations and providing a more predictable environment for international commerce. This stability can enhance economic resilience and security by minimizing the exposure of nations to the uncertainties of global currency markets. Moreover, stablecoins can play a role in national security by providing a secure and efficient means of transferring funds across borders. The speed and transparency offered by blockchain technology, on which

stablecoins are built, can be leveraged for secure and traceable financial transactions. This feature is particularly relevant in situations where traditional financial systems may be subject to restrictions or delays, offering a reliable alternative for nations to facilitate essential transactions, including those related to defense, intelligence, and emergency response (Quinn, 2022).

Conclusion

The original concept for cryptocurrencies was fundamentally based on the desire to solve problems and provide value to the world. The Cypherpunks wanted to create a new form of money that would modernize and revolutionize the financial system. They wanted a form of money that would allow people to have control over their money, maintain their privacy, make transactions with people without the necessity of trust, and remove the need for massive third-party companies. These functions were becoming increasingly more challenging to find in our quickly digitizing society. In these instances, cryptocurrencies provide a solution and value to people who are concerned with those problems, filling the need for an electronic form of cash. Cryptocurrencies remove from the equation the control of central banks and the government over the money supply, offering holders of the currency more peace of mind against fears of inflation or debasement, particularly true for countries where a stable monetary supply is unfathomable.

Bitcoin is steeped in the economic theory of private commodity money, which is present throughout a vast swath of history and has roots in the American tradition. However, with the development of blockchain technology, Bitcoin and cryptocurrencies can offer significant improvements to private commodity money. The decentralized

nature solves the problem of the issuer, the chief obstacle that plagues private money throughout its existence. Cryptocurrency offers all the benefits brought about by the digital revolution in terms of finance and money while also being a solution to the problems that have spurred up. The people who say you cannot make new money or money cannot change are the ones who are standing against the face of the insurmountable evidence that money has constantly been evolving, and cryptocurrencies represent that next evolution. In every sense of the word, Bitcoin represents an innovation. Cypherpunks and Satoshi had identified a set of problems and crafted a system that was able to solve them, providing value to users.

CHAPTER V: POLICY PROBLEMS AND SCAMS

Intro

As cryptocurrencies have proliferated throughout the financial ecosystem in the last 15 years following the creation of Bitcoin, several policy and regulation problems have begun to present themselves. Some notable issues include taxation, concerns over money laundering and other illicit uses by criminal organizations, and environmental concerns. However, by far the most prominent issue has been the massive amount of scams and frauds that have taken place in the crypto industry. As crypto has expanded, many bad actors have emerged to try to make a quick buck off of the boom. Crypto has also evolved from the original innovation of Bitcoin and the promise of decentralized finance to something much more resembling traditional finance. Massive third-party companies have emerged to offer financial services to make the use of crypto easier, and they very much resemble conventional financial intermediaries. None of these scams have anything to do with the underlying technology that made Bitcoin such a powerful invention. Nonetheless, many think they provide an impetus for a comprehensive regulatory framework surrounding cryptocurrency and digital assets.

Taxation

The intersection of taxation and cryptocurrency has become a focal point of concern for governments and individuals alike. One primary challenge stems from the decentralized and pseudonymous nature of many cryptocurrencies, which can make it difficult for tax authorities to track and regulate transactions. This anonymity can

potentially lead to tax evasion as individuals may attempt to conceal their cryptocurrency holdings or transactions to avoid taxation. Governments are increasingly working to establish comprehensive regulatory frameworks to address these concerns and ensure that cryptocurrency transactions are subject to taxation.

Another concern revolves around the complexity of accurately reporting cryptocurrency transactions for tax purposes. The volatile nature of cryptocurrency markets and the prevalence of various tokens and decentralized finance (DeFi) platforms pose challenges for individuals and tax authorities alike. Determining the fair market value of transactions and calculating capital gains or losses becomes intricate in an environment where prices can fluctuate rapidly. The lack of standardized reporting practices and the evolving nature of the cryptocurrency space adds an additional layer of complexity, making it crucial for both taxpayers and tax authorities to stay abreast of regulatory developments.

Additionally, the global and borderless nature of cryptocurrencies raises questions about jurisdictional challenges. Cryptocurrency transactions can occur across international borders, complicating the process of enforcing tax regulations. The absence of a unified international approach to cryptocurrency taxation further exacerbates these challenges. As governments grapple with these issues, some have suggested there is a need for cross-border cooperation and standardized reporting mechanisms to ensure fair and accurate taxation in the rapidly evolving landscape of digital assets. As the regulatory environment continues to evolve, finding a balance between taxation and the decentralized principles inherent in cryptocurrencies remains a complex and ongoing challenge.

Illicit Uses

Although there is much discussion about the use of cryptocurrency for illicit and criminal activities, and while these are mainly valid and will be discussed in more detail, there are several reasons why the hysteria has been blown out of proportion. While crypto is undoubtedly used for crime, this is not different from any other form of money that has ever been seen in the totality of human history (Butler, 2019). Additionally, physical cash remains, by far, the most prominent form of money for criminal activity. As we have moved away from cash as a society, the use of cash for crime has not changed, and there is no evidence to suggest that this will change anytime soon. The percentage of criminal transactions that occur with cash massively dwarfs that of cryptocurrency (Butler, 2019). One study found that only 0.25% of Bitcoin transactions are for illicit uses (Robinson & Fanusie, 2018). Another European report found that of the $100 billion laundered in Europe annually, only 4% is related to cryptocurrencies (The Economist, 2018). Additionally, the use of cryptocurrency for illicit uses has been decreasing. This is both in terms of the ratio of illegal activities as cryptocurrencies continue to garner more mainstream use and in total. Chainalysis, an independent blockchain research company, found that crypto crime decreased by 65% from 2022 to 2023 (Chainanalysis, 2023).

Butler concluded that “cryptocurrencies currently do not present any great advantage over existing methods [for financial crimes]” (Butler, 2019). Cash is still massively preferred because something like Bitcoin is not a perfect substitute for cash. If you sell an illegal item and receive a payment of bitcoin, your anonymity is only guaranteed while you remain on the Bitcoin network. If you create a Coinbase account, for example, to sell Bitcoin for cash, then your identity will be revealed. So, while there

is reason to be concerned about crypto and its use in crime in a future world where crypto is the dominant currency, it is not some existential threat that we have not always experienced with physical cash.

Money Laundering

The decentralized and pseudonymous nature of many cryptocurrencies has raised significant concerns about their potential use in money laundering activities. Cryptocurrencies offer a degree of privacy and anonymity, allowing users to transact without revealing their real-world identities. While this feature is valued by many for enhancing financial privacy, it has also attracted illicit actors seeking to exploit these characteristics for money laundering purposes. Criminal entities may leverage cryptocurrencies to obfuscate the origin of funds, making it challenging for authorities to trace and identify individuals involved in illegal activities.

Furthermore, the borderless nature of cryptocurrencies presents challenges for regulatory authorities attempting to enforce anti-money laundering (AML) and know-your-customer (KYC) regulations. Cryptocurrency transactions occur on global networks that transcend traditional jurisdictional boundaries, making it difficult for any single government or regulatory body to oversee and regulate these activities effectively. This lack of centralized control can create opportunities for money launderers to exploit regulatory gaps and inconsistencies across different jurisdictions and move funds seamlessly across borders. To address these concerns, many countries are working to implement or enhance regulatory frameworks for cryptocurrencies, requiring cryptocurrency exchanges and service providers to adhere to AML and KYC procedures.

The previous section mentioned KYC regulations and the growth of these regulations. The primary reason for this has been that the vast majority of AML and other regulations to prevent financial crimes have been incredibly ineffective in achieving their desired result (Barefoot, 2020). Instead of attempting to investigate why the regulations are not working, the government has just expanded them, believing that if they can collect more and more information, they will eventually be able to prevent or catch the crime.

Dr. Ron Pol has described anti-money laundering rules as arguably "the least effective of any anti-crime measure, anywhere." One study found that AML regulations have less than a 0.1% impact on criminal financing (Pol, 2020). An additional study has found that AML regulation captures less than 1% of the $2 trillion in yearly financial crimes (Barefoot, 2020). These policies not only appear to be ineffective, they also carry significant costs in terms of enforcement and compliance. FinCEN has a budget of nearly $200 million annually, and American financial institutions spend a combined $50 billion on compliance (Klein, 2020). The same study from Pol found that the costs associated with AML regulations are hundreds of times greater than the money they stop from being laundered (Pol, 2020). AML regulations only serve to increase the government's power over individual privacy and place burdensome and costly restrictions on banks, businesses, and consumers attempting to engage in legitimate transactions.

Additionally, these regulations have made it more difficult, longer, and more expensive for ordinary Americans to access financial services, with the greatest impact predominantly being felt amongst poorer communities (Mitchell, 2016). All of this considered, there are real questions of whether or not we should extend these principles

that have led to a complete disaster of policy in conventional finance and bring them over to crypto.

Use by Crime Organizations and Terrorist Groups

Cryptocurrencies have gained notoriety for their potential misuse by criminal organizations and terrorist groups seeking to exploit the privacy and pseudo-anonymity they offer. The decentralized nature of many cryptocurrencies allows illicit actors to conduct financial transactions outside the traditional banking system, making it challenging for authorities to monitor and track these activities. Criminal organizations have been known to use cryptocurrencies for a range of illicit purposes, including money laundering, drug trafficking, ransom payments, and financing illegal activities. “Though illicit crypto volumes reached an all-time high at $20.6 billion in 2022 (primarily due to sanctioned entities), the share of all crypto activity linked with illegal activity was only 0.24%” (Hooper, 2023).

Terrorist groups, too, have shown interest in leveraging cryptocurrencies to fund their operations. The relative anonymity provided by certain cryptocurrencies allows these groups to move funds across borders with reduced risk of detection. Additionally, the borderless nature of cryptocurrency transactions enables them to bypass traditional financial channels, which may be subject to stringent regulatory oversight. Some terrorist organizations have also used cryptocurrencies to raise funds from sympathizers globally, taking advantage of the decentralized and pseudonymous characteristics to conceal the source and destination of funds.

The scrutiny surrounding crypto and terrorist financing has returned following the October 7th,2023, Hamas terrorist attacks when the Israeli government seized several

crypto accounts tied to Hamas. Once again, the fear surrounding crypto is not totally invalid, but the evidence still strongly suggests that the greatest challenge regulators face when trying to stop terrorist attacks remains cash. Right now, the UN estimates that somewhere between 5-20% of terrorist attacks have some level of crypto financing (Wilson, 2023). Chainanalysis has stated that the total amount of terrorist financing makes up less than 1% of the illicit crime usage of crypto (Chainanalysis, 2023).

Governments and regulatory bodies around the world are increasingly recognizing the potential risks associated with the illicit use of cryptocurrencies and are taking steps to implement robust regulatory frameworks. These frameworks aim to strike a balance between preserving the legitimate use cases of cryptocurrencies and mitigating the risks posed by their misuse for criminal and terrorist financing. The development of effective strategies to address these challenges remains an ongoing and complex task for law enforcement and regulatory authorities globally.

While it is reasonable to have concerns surrounding crypto and its potential to be used in criminal activities, the evidence does not support that crypto poses some massive risk on a scale yet to be seen, or that it is an even larger risk than paper currency. Attacking crypto based on these concerns might be one way of wanting to knock down the legitimate uses of the technology when it is clear that only a tiny fraction of crypto activity is criminal.

Environmental Concerns

Cryptocurrency's environmental impact has become a growing concern, primarily due to the energy-intensive mining process, particularly in the case of Proof-of-Work (PoW) consensus algorithms. Bitcoin relies on PoW, which involves miners solving

mathematical puzzles to validate transactions and secure the network. The computational power required for these tasks is significant, leading some to speculate about the carbon footprint and high energy consumption. This energy cost associated with mining Bitcoin is a design of the system, not a bug. It is what drives the lottery game, making it costly to play. It also secures previous transactions by making it incredibly costly to go back and alter.

The environmental concerns extend beyond Bitcoin, as other cryptocurrencies also employ energy-intensive consensus mechanisms. Ethereum transitioned from PoW to Proof-of-Stake (PoS) to address its environmental impact. PoS is considered more energy-efficient as it does not require the same level of computational power as PoW. Instead, it relies on validators who are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Efforts are underway within the cryptocurrency community to address these environmental concerns. Some projects are exploring alternative consensus mechanisms, such as PoS or delegated proof-of-stake (DPoS), that are inherently more energy-efficient.

Additionally, there is an increasing focus on sustainable and renewable energy sources to power cryptocurrency mining operations. However, PoS systems have a significant disadvantage which goes against the fundamental point and goal of the Cypherpunks and Satoshi, it is not sufficiently decentralized. The staking system is subject to being dominated by a few of the large coin holders, rather than the validation being spread out throughout the entire network, that power is concentrated in perhaps only a few.

Overall, it is not clear exactly what the impact of Bitcoin and other proof-of-work cryptocurrencies is on the environment, as many conflicting perspectives exist. The lead research regarding Bitcoin and its environmental impact came from researchers at the United Nations; their report stated that Bitcoin has immense value and provides unique opportunities and that any environmental challenges should not destroy Bitcoin but rather can be overcome (Chamanara et al., 2023). The report found that there is a strong correlation between Bitcoin price and energy consumption. As Bitcoin becomes more popular, there are more mining efforts, "A 400% increase in Bitcoin's price from 2021 to 2022 triggered a 140% increase in the energy consumption of the worldwide Bitcoin mining network" (Chamanara et al., 2023). The report also found that 67% of the energy consumed for Bitcoin came from fossil fuels, with 45% of total energy being provided by coal. In total, Bitcoin mining 85.89 Mt of CO2 from 2020-2021 (Chamanara et al., 2023).

However, newer research is showing a shift. China used to dominate the crypto mining market but has begun to crack down on crypto and kick out their miners, which accounted for 50% of Bitcoin mining power globally. This has caused a massive geographic shift to countries who have cleaner energy than China (Sigalos, 2021). This is where several Bitcoin proponents are now arguing that crypto and Bitcoin provide significant opportunities for renewable energy growth. "Bitcoin has the potential to expand renewable energy generation. Renewable energy currently struggles with reliability, cost, and electricity use throughout American power grids. Bitcoin mining provides a solution to each of these issues" (Porter, 2023). These functions are called "grid-balancing services" and could be provided by Bitcoin miners.

Scams and Frauds

By far, the biggest problems and crimes that have arisen from crypto are tied to scams and frauds. Chainanalysis, the company that tracks crime in the crypto market, has tracked that scams have made up the vast majority of crypto crime (Chainanalysis, 2023). The cryptocurrency industry has been plagued by various frauds and scams, exploiting the relative novelty and decentralized nature of digital assets. These frauds have become more prevalent as the crypto ecosystem has evolved and large third-party companies have arised. In 2021, the total amount of crypto stolen from scams topped $14 billion (Sigalos, 2022).

One prevalent form of deception involves fraudulent Initial Coin Offerings (ICOs), where projects raise funds by issuing tokens with promises of revolutionary technologies but often fail to deliver, resulting in significant financial losses for investors. Ponzi schemes and pump-and-dump schemes have also been rampant, with fraudsters artificially inflating the value of a cryptocurrency before dumping it, leaving unsuspecting investors with losses. Additionally, there has been a significant number of major crypto companies that have turned out to be scams. This has occurred throughout the entire history of crypto, from Mt.Gox to the biggest crypto scandal, FTX. It was the complete collapse of FTX that has led to the new push for crypto legislation in Congress.

Mt.Gox

Nearly a decade following the collapse of the largest crypto exchange (at the time), Mt. Gox, it is still not entirely clear what exactly happened. What is known is that it was massive, with more than 850,000 bitcoins being lost and or stolen, totaling over 450 million dollars. This was the largest scandal in crypto history up until the meltdown

of FTX. In many ways, the two events parallel each other. Mt. Gox highlighted how the crypto industry was in its infancy, and the people controlling it were unprofessional and unserious at best or bad actors at worst.

Mt.Gox was founded in 2006/2007 designed initially as an online forum to trade cards of the Magic the Gathering game by Jeb McCaleb. The name Mt.Gox stands for Magic the Gathering Online eXchange. McCaleb, who became interested in Bitcoin, felt that the community needed an exchange and sold Mt.Gox to Mark Karpeles. Mt.Gox completed its transition to a Bitcoin exchange and quickly began to dominate the market, accounting for over 70% of all Bitcoin transactions. This highlights the rudimentary stage of Bitcoin and the broader crypto industry at the time. From its inception, the site was filled with many technical problems; the original data breach occurred in 2011, and the first Bitcoins were stolen. None of these issues were ever addressed or fixed, and the exchange continued to operate as if nothing had happened.

In February 2014 Mt.Gox suddenly suspended withdrawals, sparking fears in investors and customers that their investments and coins were unsafe. Mt.Gox initially claimed that this was due to technical issues, but eventually admitted to having lost a considerable amount of Bitcoins due the data-breach that had never been addressed. By the end of February, Mt.Gox had filed for bankruptcy (Perez, 2021).

As mentioned earlier, this was a massive shock to the entire crypto community, sent the price of Bitcoin plummeting, called the entire crypto industry into question, and caused thousands of investors to lose their coins and savings. Eventually, it came to light that Karpeles was shifting customer funds to other accounts to cover both business and personal expenses. In 2015, Karpeles was arrested in Tokyo and charged with embezzling

more than $1 million worth of Bitcoin and aggravated breach of trust (Hern, 2017). In 2019, however, Karpeles was acquitted of embezzlement and instead was found guilty of a lesser crime of tampering with financial records as he inflated Mt. Gox's holding by more than $30 million (Pham, 2019).

While the overall crypto industry has matured considerably from the time of Mt.Gox, the scandal that was Mt.Gox still holds many important lessons for the present. It is nearly impossible not to notice the parallels between Mt.Gox and the most recent exchange disaster, FTX. The throughline of both of these collapses is that in the United States, there has yet to be any legislation to create a comprehensive federal regulatory framework for conducting oversight of these crypto companies.

ICOs and Pump and Dump Schemes

The Initial Coin Offering (ICO) bubble refers to a period between 2017 and early 2018 when the cryptocurrency market experienced explosive growth in the number of ICOs, with a significant surge in funding and speculative investment. ICOs emerged as a fundraising method for blockchain projects, allowing them to raise capital by issuing their own tokens. While some ICOs were legitimate and represented innovative projects, the rapid proliferation of token sales led to a speculative frenzy resembling the dotcom bubble of the late 1990s. During the ICO bubble, investors were attracted to the potential for high returns as new projects promised groundbreaking technologies and solutions. However, the lack of regulatory oversight and the absence of clear guidelines for evaluating the legitimacy and viability of these projects created an environment ripe for abuse. Many ICOs turned out to be fraudulent or failed to deliver on their promises, resulting in significant financial losses for investors. As the bubble burst, regulatory

scrutiny increased, leading to a more cautious approach in the cryptocurrency space. Governments and regulatory bodies worldwide began to attempt to create clearer guidelines, investor protections, and measures to distinguish legitimate projects from fraudulent ones. The ICO bubble serves as a cautionary tale, highlighting the importance of due diligence, regulatory compliance, and skepticism in evaluating investment opportunities within the dynamic and evolving cryptocurrency landscape.

During the ICO (Initial Coin Offering) bubble, the cryptocurrency market witnessed a surge in pump-and-dump schemes that took advantage of the speculative frenzy and lack of regulatory oversight. These schemes involved artificially inflating the price of a newly issued token, typically through coordinated efforts of groups or individuals, and then swiftly selling off their holdings to maximize profits. The ICO boom attracted a vast number of retail investors eager to participate in the next big project, creating an environment ripe for manipulation. These pump-and-dump schemes during the ICO bubble exploited the lack of regulatory safeguards and the euphoria surrounding the potential for quick profits in the cryptocurrency space. The prevalence of such schemes contributed to a growing awareness of the risks associated with investing in ICOs. For some, it underscored the need for regulatory measures to protect investors from fraudulent activities in the crypto market.

In the period of the bubble primarily from 2016 to early 2018, millions of new tokens were created, most not receiving any attention whatsoever. A handful of several thousand went through the ICO process to attempt to raise money. In the span of three years various ICOs raised a total of $13 billion (Grobys, 2020). It has also been found that more than half of all ICOs failed within the first four months (Palmer, 2021). The

entire market was rotten with fraud. The Satis Research Group studied 1,500 ICOs in 2018 and found that approximately 78% of the projects were fraudulent (Dowlat & Hodapp, 2018). Another study concluded, “The cumulative losses due to scam in the ICO market correspond to $10.12 billion which is 66% of our identified overall market capitalization and highlights the enormous societal impact of this criminal activity” (Sapkota et al., 2020). The bubble burst at the beginning of 2018, resulting in an 85% drop in the total market capitalization of cryptocurrencies, which was a decrease of more than $700 billion. This massive crash was more significant than another prominent tech bubble, the dotcom bubble of the early 2000s, which had a 78% decrease in market cap (Qureshi, 2021).

Pump and Dump (P&D) schemes were prevalent in the ICO bubble. The excitement surrounding crypto and the lack of oversight of the market and the mechanisms available made it incredibly easier for fraudsters to conduct P&Ds (Li et al., 2019). “P&D is a form of price manipulation that involves artificially inflating an asset price before selling the cheaply purchased assets at a higher price. Once the assets are “dumped,” the price falls, and investors lose money” (Li et al., 2019). While some of these schemes were carried out by institutional investors or the founders of the token, many of them were done by individuals banding together. Many of these schemes resemble what we saw with the Game Stop Sage a few years after the ICO bubble. Many individual investors organized themselves into “pump groups” primarily on the app telegram but also other online channels in order to coordinate a pump. They would select a time, and all would start buying the coin, massively jumping up the price and creating momentum around the coin. Eventually uneducated investors would try to tag along on

the trend. When the organizers felt the price was high enough, they would all coordinate their sale, and the price would plummet, leaving some poor fellows at the end holding the losses and making the organizers a whole bunch of money (Li et al., 2019).

The aftermath of the ICO bubble and the rise of P&Ds in crypto has increased the calls for oversight and regulation from the SEC and cooperation amongst global parties. Many have cited that lack of rules and oversight of the market is what allowed for so many of these scams to be carried out (Li et al., 2019) (Sapkota et al., 2020). For example, the US has strict rules against P&Ds on stock exchanges, however these rules are not clearly applied to the crypto market or crypto exchanges and there has not been clear guidance on this from the SEC or from Congress. Finally, it is stressed that the global and borderless nature of cryptocurrencies, with many tokens trading on several exchanges all across the world, has allowed fraudsters to engage in regulatory arbitrage (Li et al., 2019). However, not only does the ICO bubble and P&Ds show the necessity for government action in the crypto market, it also highlights the role that these major companies in crypto, primarily exchange, play in protecting their consumers from these fraudulent activities.

Terra/Luna

The collapse of Terra/Luna was significant in the history of crypto because it was the first time that a major stablecoin, which was meant to be separate from the volatility suffered by the rest of the market, broke its peg and plummeted. In May of 2022, the stablecoin TerraUSD (UST) broke its peg to the US dollar, plummeting to below 30 cents in a matter of days. Terra's native token, Luna, which was used to stabilize UST's price,

also collapsed, falling from $84 to $1.25. The Terra/Luna collapse is complicated, so we will start from the beginning (Orcutt & Manoylov, 2022).

Terraform Labs is the organization behind developing the Terra blockchain and its associated ecosystem of stablecoins. Terraform Labs was co-founded by Do Kwon and Daniel Shin in 2018 and was initially backed by other major crypto companies such as Binance and other institutional investors. The Terra blockchain is designed to provide a stable and scalable platform for decentralized applications (DApps) and smart contracts. One of the notable features of Terra is its focus on stablecoins. Terra had its stablecoin called Terra (UST), that it launched in 2020, which was pegged to the US Dollar, aimed to reduce price volatility commonly associated with other cryptocurrencies. Most stablecoins are characterized as collateralized stablecoins and that is that they are backed by cash or a physical asset. Other major stablecoins in the market, Circle's USDC, and Tether's USDT operate in this fashion. However, Terraform Labs designed UST to operate based on market incentives, which are called algorithmic stablecoins. This is where Luna (LUNA), the native token of the Terra blockchain, comes into play. Luna serves a crucial role in the stability of the Terra stablecoin. Luna is used as collateral to mint new UST or burn UST to release Luna, helping to maintain the stablecoin's peg (Orcutt & Manoylov, 2022).

Here is Do Kwon, the CEO of Terraform Labs, explaining the design of the stablecoin and how, by tying Terra and Luna together, it would be able to maintain the peg of Terra to the dollar.

"The idea is that at any given time a person can burn a dollar's worth of Luna in order to mint one TerraUSD, and vice versa you can always redeem one TerraUSD for a dollar's worth of Luna. So insofar as the Luna token has some sort of market value, you can always try to arbitrage against the system in order to mint and redeem stablecoins…Just in case a

de-pegging event happens — so for example if TerraUSD is trading for $0.90 — an arbitrageur can simply buy up TerraUSD from the open market and then trade it against the protocol for a dollar's worth of Luna, thereby capturing 10% arbitrage profit that way. And vice versa, if TerraUSD is ever trading at $1.10, you can buy a dollar's worth of Luna from the open market, mint TerraUSD and then sell that to capture 10% profit on the other side" (Do Kwon, 2022).

However, this mechanism is inherently flawed and is doomed to fail from the start. TerraUSD is a dollar liability that is issued without any real value, the only thing that says it is worth a dollar is the issuer who tells you that it is worth a dollar. The theory behind terra was simple supply and demand. The issuer, Terraform, would control the supply of Terra in accordance with the demand in order to ensure that the price of the coin remained at $1. However, this is easier said than done because you cannot just go around taking away coins from people to control the supply because that is theft. What the people at Terraform Labs came up with was Luna. Terraform issued Luna as a second liability that did not have a mandated price and was free-floating. The two liabilities were tied together in a way to incentivize people with risk-free arbitrage to control the supply of UST. If the price of UST was over $1, then you could trade Luna to Terraform in exchange for UST, giving the trader a profit. This would increase the supply, thus lowering the price of UST. If UST is below $1 then a trader can give Terraform units in exchange for an amount of Luna that will guarantee the trader a profit. This would decrease the supply, increasing the price of UST (Hendrickson, 2022). While this sounded like a great design, it is very clear to see why it collapsed in on itself, and frankly, it is shocking it lasted as long as it did.

The two assets that were created, UST and LUNA, were both completely worthless. Their only value was in reference to the arbitrage that could be gained from

the other. This was able to work as long as everyone was willing to play the arbitrage game.

> "For example, suppose someone starts shorting both assets. This drives down the price of both assets. If people think that the prices are going to continue to decline, this decreases the demand. In terms of [UST], this is fine as long as the supply is falling faster than the decline in demand. If so, the price will move higher. But remember, when the supply of [UST] is declining, this is because I am increasing the supply of [LUNA] So [LUNA] has a declining demand and an increasing supply. Both of these cause prices to fall" (Hendrickson, 2022).

In this case, there is no longer any incentive to trade UST for LUNA because you expect the price of LUNA to decrease as well. This takes away the risk free-arbitrage. This makes it to where holders of UST will look to trade for some other asset other than LUNA. This will trigger a "death spiral," with both assets headed toward zero. This is essentially what happened in the case of Terra/Luna.

On May 7th and 8th of 2022 it began to appear that there was a large amount of sales of UST into other stablecoins. This caused the original breaking of the peg to the dollar. That is when a third party, LFG, who was holding a reserve of Bitcoin to back UST, announced they would be using part of it. This caused a partial recovery in UST from below 60 cents to slightly over 90 cents. Then, it was reported that LFG needed significant investment to fill its reserve, causing a massive collapse in the price of UST to below 30 cents. During this time, Binance suspended withdrawals of UST and LUNA, along with the largest exchanges in Korea, suspending trading of LUNA, harming the ability to stabilize the system. Terraform Labs several times throughout the collapse halted the blockchain entirely in an attempt to assist. In the end, UST never came close to regaining its peg, and the referential LUNA token lost more than 98% of its value. The collapse ended up wiping out around $60 billion in total market cap with UST, LUNA,

and the rest of the Terra ecosystem (Orcutt & Manoylov, 2022). UST and Luna were eventually no longer tradeable anywhere, and the project was abandoned. Terraforms Labs tried to restart their scheme; they eventually shut down amid lawsuits.

Celsius

Celsius Network was a crypto lending company that was founded in 2017 by Alex Mashinsky during the height of the ICO boom. It was pegged as the future of financial services, offering an alternative to the traditional banking system. Mashinsky would frequently proclaim that he is coming for the big banks and ask users to join him in "unbanking" themselves. Mashinsky claimed to be a zero-risk institution where users could store their wealth, and this was incentivized through massive yields on deposits of up to 18%. Users were also able to take out loans on the platforms. Many people were quick to see through the facade, and the company faced many accusations of fraud from its founding, many of which Mashinsky would directly take on. By May 2022, Celcius had $12 billion in assets under management and was lending out over $8 billion to users (Kuhn, 2023).

Celsius turned out to be nothing more than a scam and Mashinsky a total fraud, who built the company on nothing more than lies and deception from the very beginning. In June 2022, the company froze all withdrawals from accounts, citing market conditions; in reality, Celsius had no money left. While it was portrayed to be a safe steward of customers' assets operating as this new, better, and safer version of a bank, it was nothing more than a hedge fund. "It was funded almost entirely by customer deposits, which it gambled and lost, racking up an over billion dollar deficit" (Kuhn, 2023). In July 2022, Celsius filed for bankruptcy, and a year later, Mashinsky was arrested on a litany of fraud

charges. “In total the DOJ charged Mashinsky on seven counts, including securities, commodities and wire fraud and several conspiracy-related allegations” (Kuhn, 2023). Ironically, the final nail in the coffin for Celsius was the collapse of the Terra stablecoin, putting its finances in complete ruin, albeit Celsius was far from sustainable prior.

The criminal filings allege that essentially everything Mashinsky claimed about the business was a lie, even including how much Celsius raised from the sale of their own crypto native token, CEL. Mashinsky lied about their insurance policy, massively inflating to say that they had $750 million for each client. While railing against the risks of traditional banks and also of self-custodying your crypto, Mahsinsky pledged that all users who deposit into a Celsius account would maintain ownership of their assets. However, Celsius would pool all of the customers’ funds together to make risky bets. For years before the paper tiger collapsed, users experienced days of delay in being able to withdraw their funds. Celsius did not keep records of their transfers until 2021, and there is evidence of employees speaking up beginning in 2019 about the company’s financial situation. The unbelievably high yields were costing Celsius money hand over fist, but they were also the only way to attract new users, which was the only way to keep funding the scheme (Kuhn, 2023). It had essentially developed into a Ponzi scheme. An additional lawsuit from Jason Stone, an investment manager who had a relationship with Celsius, alleges that Celsius was nothing more than a Ponzi scheme. His lawsuit alleges that, “Celsius artificially inflated the price of its own digital coin, failed to hedge risk and engaged in activities that amounted to fraud” (Kharpal, 2022).

FTX

The largest fraud in the crypto industry is the most recent and has sparked much of the energy behind bringing reform through Congress. FTX, one of the largest crypto exchanges in the world, collapsed like a house of cards when it was revealed that it was little more than a giant fraud. FTX cannot be talked about without mentioning its famous and quirky Founder/CEO, Sam Bankman-Fried, more commonly referred to as SBF. FTX was also more famously known for being associated with SBF along with its massive marketing scheme, such as naming the arena for the Miami Heat or having a plethora of Celebrity surrogates, such as Tom Brady, rather than any actual function. The entire saga seems fit for a Hollywood script. The media has been quick to classify FTX as Crypto's Enron and write off the industry and technology as a whole. However, FTX is the seminary moment that brought to light a few of the uneasy truths of what the broader crypto industry has become, teaching us several key lessons and hopefully moving the ball forward to putting crypto into a better place.

The downfall of FTX began on November 2nd, 2022 when CoinDesk published a story exposing the balance sheet of SBF's trading firm, Alameda Research. Alameda was a crypto hedge fund. The story heightened long-standing questions and concerns surrounding the intertwined relationship between FTX and Alameda. It showed that Alameda heavily relied on FTT holdings to make up their assets, which was the native token of FTX. This realization sparked a run of deposits at FTX by customers, which was further compounded when Binance founder, "CZ", announced the firm would sell its FTT holdings. The result led to a fast and massive collapse, with FTX filing for bankruptcy on November 11th (Huang, 2022). A year later, SBF was found guilty on seven counts of fraud and conspiracy, and in March 2024, was sentenced to 25 years in prison. FTX and

SBF were playing with customer's funds, moving them to the hedge fund, Alameda, and manipulating the price of FTT. This was all in an effort to make risky bets to turn those funds into big profits. It raises significant questions about the comingling of customer funds in crypto firms.

The story of FTX highlights several important aspects. One is the complete lack of corporate governance at FTX. The entire company was run by a band of young and inexperienced friends that had no real structure or plan for the company. John Ray, who was placed as the CEO to lead FTX through bankruptcy who has decades of experience in these matters, has called it the worst failure of corporate governance that he has ever seen. FTX only had two members of its Board of Directors and did not keep any notes of its meetings where they went through major transactions. They also had no system records, and it was unclear where many of the assets were located. The company's little records were kept on the $12 per month software, Quickbooks. By the end, FTX had developed into an incredibly complex corporate structure with many companies associated with it, with many of these companies having significant conflicts of interest with one another. All of this is to say that FTX is not a story of the failure of crypto but rather the story of the failure of people to manage a company and a case of outright fraud, disguising itself as a new innovative company in a new technological field.

The collapse of FTX showcases that we should not be so quick to trust, idolize, and make heroes of so-called geniuses. SBF was labeled as the golden boy of crypto, and if he was given enough resources and influence, he could single-handedly lead the industry to brighter days. SBF used his money to donate to politicians and attempt to be the leading voice for crypto regulation. Ultimately, his preferred policy was to support

FTX and punish its competitors, most notably Binance. The deception of SBF was strong; he was successfully able to convince institutional investors to give him billions of dollars, and many unknowing retail inventors followed suit. The anointing of SBF as the leader of crypto goes against the direct principles of decentralization that the Cypherpunk movement and Bitcoin were based on.

The fiasco that was FTX fully highlighted for the general public what many in the broader crypto community had been noticing for some time, that there is a difference between "Crypto," the underlying technology and developers, and the "Crypto Industry," companies like FTX and Celsius. What caused the collapse of FTX had nothing to do with the underlying technology of cryptocurrency or blockchain. What happened was like any other case of white-collar fraud that has been experienced in industries and throughout time. The people behind FTX and other frauds in crypto were not true crypto believers; they were investors looking to use a hot new technology to make a profit, misleading unsophisticated and sometimes even institutional investors with unrealistic promises of high yields. People and investors who truly understand the technology of crypto, the principles that undergird it, both with regards to economic and computer science, and who believe in the promise of the Cypherpunks are not worried about cases like FTX. As lead Bitcoin researcher at CoinShare, Christopher Bendiksen put it "I don't think FTX would freak out in the slightest anyone who understands the fundamental investment case of bitcoin". The people behind Bitcoin, the sound work behind it, and the people who truly believe in the technology and have worked on moving it forward are not going anywhere. The result of something like FTX can better the industry, pointing out the bad actors and showing where regulators can make reasonable changes to

institutionalize and legitimize the innovators and sound companies in the crypto industry.

Conclusion

The rise of cryptocurrencies has brought about a considerable amount of challenges and problems. While these problems are real, and there are actions that should be taken to help address them, none of these issues are particularly unique to crypto or insurmountable. Many crypto skeptics, both in everyday life, business, and amongst politicians, have pointed to these problems to show why crypto is unstable, unsafe, or unusable and use them to justify throwing crypto out of the financial system. This could not be further from the truth. The problems associated with cryptocurrencies are either inherent to the nature of money or have been present in every technological wave in human history. While there are certain actions that can and should be taken to mitigate against these problems, they by no means should eliminate crypto from the financial system or from having a future.

The problems of taxation and illicit uses such as money laundering or use by criminal organizations are not unique to crypto but rather a result of what money is. Tax fraud and evasion are already evasive in our society without cryptocurrency. It has always been an issue and will always be an issue. People hiding crypto payments from taxation is not different from people hiding cash payments from taxation. This similar logic applies to illicit uses. The same elements that allow cash to be used for illicit purposes apply to crypto; however, as examined, cash is still by far the chief choice for criminals to carry out illicit financial activities, and by all review of the evidence, cash will continue to reign supreme because crypto is an imperfect substitute for cash. It is

also clear that many of the actions taken by the government to attempt to thwart financial crimes have been wholly ineffective and have led to overburdening regulations on businesses and infringed upon the privacy of US citizens.

The prevalence of scams and frauds in the crypto industry is the most pressing problem that plagues it. It is the one that has drawn the most attention from the skeptics and believers alike. While the issues of scams are something that should be addressed and solved in the crypto industry, they do not take away from the value or potential of crypto. "[Scams are] something that happened to crypto, not something intrinsic to it" (Qureshi, 2021). The purpose and promise of cryptocurrency, a revolutionary innovation born out of the workings of the Cypherpunks to decentralize finance and money in the digital age still is true and present in the industry. The true believers, the very people who developed the concept and people who believe in what the Cypherpunks created are still present and developing the industry and they are not going anywhere. The concept of scammers attaching to the hot not industry in an attempt to make a quick buck is nothing new; it is present in every single new technology. The rise of scams in crypto may be something that the industry needed. As the scams have cropped and been discovered it has allowed the industry to purge itself of bad actors, learn where the problems are, and begin to make the changes necessary to allow crypto to be prominent and mainstream. Frauds have been prevalent in nearly every aspect of the crypto industry, and each one has sparked new debates in policy circles about potential government regulatory action to prevent future schemes. The collapse of FTX pushed this debate to the forefront and created traction on Capitol Hill and in the United States to pass comprehensive legislation to lay the

groundwork for rules to govern the industry, which would further cement the legitimacy of the industry.

PART II: REGULATION

Introduction

In the rapidly evolving financial technology landscape, few innovations have captured the imagination and potential for transformation, quite like cryptocurrencies. Born from the vision of a decentralized digital currency system, cryptocurrencies such as Bitcoin have disrupted traditional notions of money, finance, and commerce, sparking debates, speculation, and innovation worldwide. Nevertheless, amidst this wave of technological advancement and financial revolution, several critical questions remain: Should they be regulated? Can they be regulated? And how should they be regulated?

This part delves into the intricate and multifaceted realm of cryptocurrency regulation in the United States, as well as the broader global context, exploring the complex interplay of legal frameworks, regulatory agencies, enforcement actions, and market dynamics that shape the evolving landscape of digital assets. Through a comprehensive examination of key regulatory bodies such as the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Financial Crimes Enforcement Network (FinCEN), this part seeks to unravel the intricate tapestry of laws, regulations, and enforcement mechanisms that govern the use, trading, and issuance of cryptocurrencies. From the Howey Test and securities regulations to anti-money laundering (AML) and know-your-customer (KYC) requirements, each chapter offers insights into the legal and regulatory landscape that both enables and constrains the growth of the cryptocurrency industry.

Drawing upon case studies, regulatory developments, and expert analyses, this part aims to provide a comprehensive overview of the challenges, opportunities, and implications of cryptocurrency regulation in the United States. It explores the tensions between innovation and investor protection, decentralization and regulatory oversight, economic empowerment, and systemic risk. Whether you are a policymaker, investor, entrepreneur, or enthusiast, this serves as a timely and essential guide to navigating the complex and dynamic terrain of cryptocurrency regulation in the United States. It seems clear that the United States is moving towards adopting a framework for crypto regulation, but the question remains of what it should look like.

CHAPTER VI: CURRENT REGULATORY LANDSCAPE

Overview

Since the inception of cryptocurrencies, digital assets, and blockchain technology, there have been ongoing questions about how it should all be regulated. The scope of the industry is so broad that it covers many regulatory bodies and jurisdictions. In the early days following the creation of Bitcoin, these questions were not as important because the overall impact of the crypto market was relatively small. However, as the industry has grown, so have the discussions surrounding how it should be regulated. This is especially true in the last couple of years as the amount of crypto legislation being discussed worldwide has increased dramatically, especially in the wake of multiple massive scandals in the industry. This is also true in the United States, where numerous crypto-based bills have been discussed, and some even passed through Congressional Committees along with aggressive moves by regulators, most notably the Securities and Exchange Commission (SEC).

The regulatory landscape for crypto is complex. Crypto is a global market, and regulations are currently happening across the globe, with many different countries taking very different approaches to how they view technology. While this paper predominantly aims to focus on the happenings of the United States, it is essential to understand what other countries are doing and discussing on this front. The current regulatory situation in the United States is also very complex, with competing regulatory agencies and jurisdictions.

Global Regulation

As the number and overall interest and usage of crypto has increased, along with the massive growth in the broader apparatus of the crypto industry, all the countries around the world have had to deal with what approach they want to take in regard to dealing with crypto. These conversations and efforts have also started to pick up and increase across the globe. A report from the firm PWC found that 2023 was the most active in the world in terms of crypto discussions, with more than 40 countries discussing various legislation or regulations. This resulted in more than 20 adopting new policies. Some of the significant developments in 2023 were the development and advancement of the European Union Market in Crypto-Assets Regulation, also known as MiCA, as well as the UAE working to establish the first independent regulatory body solely working on digital assets (Blumenfeld & Talvitie, 2023).

Cryptocurrency, at its core, is a global technology and borderless, meaning that people across the world in different countries can interact. This means that every single company is impacted by crypto, making it a unique technology. This global nature of crypto has led certain institutions, most notably the International Monetary Fund, to call for global cooperation in regulating crypto. However, there has been little interest in this approach.

Countries have taken vastly different approaches to handling crypto and crypto companies, ranging from outright banning to making it legal tender. In terms of the pro-crypto countries, it would be hard-pressed to find one more friendly, especially with regard to Bitcoin, than El Salvador, which in 2021 became the first country to make Bitcoin legal tender, and the President has pledged to build “Bitcoin City.” Other crypto

friendly countries include the Bahamas which has become a massive hub for blockchain-based companies to domicile in, most notably of these was the infamous crypto exchange, FTX.

Finally, according to many, Switzerland has the most sophisticated regulatory framework. This is not a shock considering the country's history of being pro-business, but Switzerland has provided regulatory clarity and been clear about wanting to partner with the growing crypto industry. The Ethereum Foundation operates out of Switzerland, and the city of Zug has been dubbed "crypto valley."

Some countries have taken a middle-ground approach. These countries can be categorized as those that are bringing forth clear regulations and guidelines, but they might not be the most favorable to what supporters of crypto or the crypto industry would prefer. A perfect example of this is a country like Singapore, which has developed a comprehensive regulatory system for digital assets, leading to a boom in companies wanting to domicile in the country. However, the regulations are not necessarily pro crypto. Another would be the EU MiCA regulations which would be a massive milestone in the history of crypto by having a set of uniform market rules established across the EU.

Finally, some countries have been antagonistic and anti-crypto, going as far as to ban the mining or trading of cryptocurrencies. There is a trend that more authoritarian regimes are more anti-crypto. Countries such as Algeria and Morocco have banned crypto. Additionally, China, which has always had a negative relationship with crypto, entirely banned mining and trading in 2021. This was an incredibly significant move because, at the time, Bitcoin mining in China accounted for over 70% of the hash rate. So many mining operations occurred in China due to the wide availability of cheap energy,

and a significant amount of this mining activity has shifted over to the United States. Just this past year, Vladimir Putin signed a law in Russia that prohibited the use of digital assets for payments. Finally, there are countries like the Netherlands that are deemed crypto-negative because of the way they tax cryptocurrencies. In the Netherlands, crypto is treated as an asset and subject to their wealth tax. This means any increase in the price of a token is taxed at 30%.

As other countries around the world begin to pass comprehensive frameworks surrounding how to regulate digital assets, the United States has not, making it hard to place the US in any of the three broad categories.

The United States

At the Federal level, the power for creating new legislation constructing a framework or rule for the regulation of crypto rests in the hands of the United States Congress. Congress has not yet passed any laws directing this, so all current regulations have been passed by executive agencies taking matters into their own hands and attempting to apply existing laws to crypto. This has resulted in a turf war between three major bodies: the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Federal Trade Commission (FTC). Other major bodies include the Internal Revenue Service (IRS), charged with figuring out how to tax digital assets, and the US Department of the Treasury Financial Crimes Enforcement Network (FinCEN) has been attempting to apply AML and KYC laws to crypto, with varying degrees of success.

Securities and Exchange Commission (SEC)

The Securities and Exchange Commission is the primary federal regulatory agency responsible for enforcing securities laws in the United States. The SEC has authority over securities offerings, trading, and exchanges, and it plays a crucial role in determining whether specific cryptocurrencies or token sales qualify as securities under U.S. law. The SEC has issued guidance and taken enforcement actions against individuals and entities engaged in fraudulent or unlawful cryptocurrency-related activities.

The Securities and Exchange Commission (SEC), over the last few years under the leadership of Chair Gary Gensler, has been the harshest of the regulators against the crypto industry, attempting to implement rules by bringing numerous enforcement actions against crypto companies. Gensler has been waging war against the crypto industry with the intent of bringing them into compliance with existing securities law. This has become more prominent following the increasing number of frauds in the industry and, most significantly, after the collapse of FTX. In Gensler's view, the current laws on the books make it clear how crypto assets should be handled: "Nothing about the crypto markets is incompatible with the securities law" (Gensler, 2022). Gensler has also called the crypto industry the "Wild West" and stated that there are "Far too many frauds and bankruptcies" and "Crypto's entrepreneurs have 'generally built a business model around noncompliance with the law." Finally, Gensler believes that his enforcement actions have been clear and consistent with the laws, "there's been clarity for years," and that crypto companies just "need to come into compliance" (Gensler, 2023).

Gensler views on crypto also seem to have shifted since the beginning of and before his time as SEC Chair, adding to concerns from people critical of his decisions. In

2018 Gensler taught a course at MIT on digital currency where he seemed to be rather interested in the concept. Shortly after, in 2019, Gensler wrote in an op-ed:

> " I remain intrigued by Satoshi's innovation's potential to spur change – either directly or indirectly as a catalyst. The potential to lower verification and networking costs is worth pursuing, particularly to lower economic rents and data privacy costs, and promote economic inclusion…further, shared blockchain applications might help jumpstart multiparty network solutions in fields that historically have been fragmented or resilient to change. Even in this slightly less ambitious form – acting as an innovative irritant to incumbents and traditional technologies – cryptocurrencies and blockchain technology have already prompted real change and can continue to do so" (Gensler, 2019).

During his confirmation process to become SEC chairman in 2021, Gensler said, "Markets—and technology—are always changing. Our rules have to change along with them," and that "financial technology can be a powerful force for good." Gensler also called upon Congress to pass legislation to make the rules around crypto clearer, seemingly in stark contrast to his current position that existing securities law is clear.

More recently, Gensler embodies the opinion that crypto, at its core, is useless and worthless. Gensler seems to be taking the position that there is nothing fundamentally unique about the creation of Bitcoin, saying that "no one invests in something because of how they keep their ledger" and the opinion that crypto has no use beyond criminal uses. When he once seemed to be warm to the idea that the law and rules of the SEC needed to be updated to meet the technology of crypto, he stated in 2022 at a conference that "There's no reason to treat the crypto market differently just because different technology is used" (Gensler, 2022). In the course of just a few years Gensler appears to have made a notable shift in the way he views not only the broader crypto industry, but also the technology of crypto itself.

The actions by the SEC and Gensler have been controversial particularly from the crypto industry who have claimed Gensler is waging a war on crypto. Many proponents

of crypto have taken to the term “regulation by enforcement” to describe the actions of the SEC. Many have criticized the SEC for not providing a clear interpretation of the law as an attempt to carve out as much authority over the crypto industry due to the lack of a clear framework. Others have claimed that Gensler is simply attempting to root out crypto for some sort of personal reasons. Finally, the industry and policymakers in Congress have claimed that the SEC has not been transparent with their actions towards crypto companies and that there has been a lack of clarity on how they can comply. When reaching out to te SEC for comments or assistance, they have been provided with few answers or nothing more than public information.

In the US, an asset is deemed to be security and thus subject to regulation by the SEC under the Securities Act of 1933 and the Securities Exchange Act of 1934 if an asset is considered to be an “investment contract” (Tierno, 2023). In determining whether an asset meets the criteria of an “investment contract,” a four-part test was created in the 1946 landmark Supreme Court case, SEC v. W.J. Howey Co. This court ruling established what is known as the Howey test, and it defines an “investment contract” if the four features of the contract (Tierno, 2023):

1) the investment of money
2) in a common enterprise
3) with a reasonable expectation of profits and
4) to be derived from the efforts of others

The SEC and Chair Gensler have been relatively straightforward that they believe that the Howey test and existing securities law can be applied to most crypto assets. The SEC has also stated that whether each individual cryptocurrency is a security depends on the “specific facts and circumstances” of that case (Tierno, 2023). Gensler stated in 2023 fully that, in his view, Bitcoin is a commodity, and Ether is a security.

While the SEC has been clear that they view most cryptocurrencies as securities, they have not been clear in providing rules and guidance for crypto issuers and most specifically crypto exchanges who list said securities to comply with regulations. None of the major exchanges have registered with the SEC as a national securities exchange, and only a few minor cryptocurrency issuers have registered as assets. Many members of the industry are saying that the current rules do not fit or make sense for crypto companies. The industry is calling on the SEC to make a set of rules tailored for crypto so that they know how to register. This has created a standoff-like situation between the SEC and the crypto industry, with the SEC stating that these companies are not complying with the law and the industry saying that the SEC is not providing the necessary rules or guidance to comply with the law.

As mentioned, the SEC has yet to proactively regulate crypto through the rulemaking process, which would allow them to update their existing regulations to be better tailored for crypto companies. However, two major proposed rules over the last two years do have important implications. Nonetheless, these rules have been left in limbo with little prospect of moving forward for many months now. The first proposed rule came back in the spring of 2022 when the SEC proposed adding to their definition of an "exchange" to add "Communication Protocol Systems." Many people believed that this addition was specifically done in order to capture exchange platforms that specifically offer digital assets for trading (Tierno, 2022). This rule, however, has seen no further action for nearly two full years since its proposal.

The second rule is referred to as the "qualified custodian" rule. The SEC proposed last year to expand upon its custody rule, which requires companies to follow specific

guidelines and safeguards when they hold customer funds. This is what is referred to as a "qualified custodian." Under existing rules from the SEC, federally-regulated entities and state-regulated entities are both eligible. However, under the proposed rule, the SEC specifically questioned whether the final rule should make it so that only federal regulation will be sufficient to be a qualified custodian (Leonardo, 2023). This rule has not proceeded, as it has received backlash across the entire banking industry. States like New York and Nebraska, which have developed regulations allowing entities, including banks, to custody digital assets, were not pleased with this rule, as it would breach the authority of their regulators.

In the absence of rulemaking the SEC has relied on enforcement action to regulate the crypto industry. The SEC has been involved in cryptocurrency since 2013, however the amount of enforcement actions has exploded since Gary Gensler took over as chair of the SEC, more than doubling since before his time. The highest number of enforcement actions in a single year (46) came in 2023. These actions amounted to a 53% increase from 2022 (Mola, 2024). This follows with what Gensler has claimed to want to do in terms of bringing the industry into compliance in terms of his view of the law, especially following the collapse of FTX. 37% of these actions from the SEC have to do with ICOs, and 82% of these actions alleged fraud. 61% of the actions from the SEC alleged that it was an unregistered securities offering, and this extended to two NFT actions brought by the SEC, which stated that certain NFTs qualify as a security (Mola, 2024).

The overall takeaway from the Cornerstone Research report was that "The SEC has continued in 2023 to focus on its implementation of the *Howey* test…The SEC has increasingly concentrated on trading platforms for their crypto lending and staking

programs or for allegedly failing to register as an exchange, a broker-dealer, and a clearing agency" (Mola, 2024). Some of the significant cases that the SEC has brought include the 2020 case against Ripple Labs, the creator of the XRP token, and this past summer, suing the world's largest crypto exchange, Binance, and the largest exchange in the US, Coinbase.

In July 2023, Federal Judge Torres of a New York District dealt a big blow to the view of the SEC, that cryptocurrencies are always securities, in the *SEC vs Ripple Labs* ruling. Torres ruled the XRP itself was not a security and sided with Ripple in two of the three transaction types in question. The three transaction types were:

1) Institutional Sales: sales of XRP to institutional investors directly
2) Programmatic Sales: sales of XRP on trading platforms through an algorithm
3) Other Distributions: XRP being distributed to employees or some other party

The court found that the institutional sales did satisfy all of the aspects of an investment contract as the investors provided money and due to the communication of Ripple the investors could reasonably expect profits based on the efforts of Ripple Labs. However the court found that programmatic sales and other distributions did not meet all of the aspects of an investment contract under Howey. The programmatic sales on exchanges were blind sales meaning the buyer didn't know who was selling and thus couldn't reasonably expect profits. The distributions to employees for example, lacked the "investment of money" component for an investment contract.

The SEC's lawsuit against Coinbase is a significant development. The SEC's complaint focuses on the fact that Coinbase is not registered as an exchange with the SEC and thus has been engaging in unregistered security offerings since 2019. The SEC alleges that Coinbase offers 13 tokens on their platform that are securities, including two

popular tokens, Solana and Cardano. Through this case, the SEC is making it clear that in its view, all crypto exchanges are in violation of US law.

This is significant because Coinbase is considered to be one of the best actors in the crypto market and a company based in the United States. Coinbase has been a publicly traded company since 2021 and went through an extensive review process with the SEC before it could be listed. Additionally, Coinbase releases annual statements that are audited by Deloitte and to everyone's knowledge they aren’t stealing customer funds like FTX, but rather operating like any traditional exchange.

Coinbase has established a review process by which issuers can apply to have their tokens listed on the exchange. This process is done to ensure that Coinbase isn't offering securities, as the company is confident in their analysis. The process is also designed to protect customers from tokens that pump-and-dump schemes or could expose them to malware or shady business practices. Coinbase has had thousands of tokens submitted to them for review and over 90% of these applications have been rejected.

Commodity Futures Trading Commission (CFTC)

The Commodity Futures Trading Commission (CFTC) regulates commodities and futures markets in the United States. While the CFTC primarily oversees traditional commodities such as agricultural products and energy, it also has jurisdiction over certain types of digital assets, including Bitcoin and other virtual currencies. The CFTC considers certain virtual currencies to be commodities under the Commodity Exchange Act (CEA), and it regulates derivatives contracts based on virtual currencies, such as Bitcoin futures.

The CEA broadly defines commodities as “all services, rights, and interest in which contracts for future delivery are presently or in the future dealt in” (Tierno, 2023). Since 2015, the CFTC has taken a role in overseeing crypto. The CFTC Chairman at the time said that the agency had a role in overseeing crypto derivatives even though they did not have specific policies for virtual currencies. The CFTC has frequently maintained that Bitcoin is a commodity through enforcement actions along with several other cryptocurrencies (Tierno, 2023). The CFTC has also maintained that Ether is a commodity with Chair Behnam reinforcing as much in 2023 during a congressional hearing (Hamilton, 2023).

A federal court decision in the 2018 case *CFTC v. McDonnell* supported the CFTC’s view of what cryptocurrencies the CFTC viewed as commodities. The court found that cryptocurrencies have elements to resemble “government paper currency, commodities, and securities.” The ruling states that cryptocurrencies can be viewed as commodities “based on common usage,” “because virtual currencies provide a ‘store of value,” and “because they serve as a type of monetary exchange” (Schwinger, 2018). The court also said that without an action by Congress the law is not clear on how cryptocurrencies should be treated. This means that the CFTC’s jurisdiction over crypto is “incomplete” and that they are one of several federal agencies that have authority.

The view of the CFTC clearly is in contrast to that of the SEC. The CFTC has stated that they plan on producing a more substantial framework surrounding digital assets in the coming years. There have been concerns that the CFTC lacks the resources that are necessary to regulate the large chunk of the crypto market that they are claiming.

Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) is a regulatory agency in the United States responsible for protecting consumers and promoting competition. While the FTC does not have direct authority over cryptocurrency regulation, it plays a role in addressing fraudulent or deceptive practices related to cryptocurrencies and blockchain technology.

The FTC's jurisdiction primarily covers matters related to consumer protection and antitrust laws. In the context of cryptocurrencies, the FTC has taken several enforcement actions against individuals or companies engaged in deceptive practices, such as fraudulent initial coin offerings (ICOs), Ponzi schemes, or misleading advertising related to cryptocurrency investments. The most notable of these actions was the FTC's enforcement action against the defunct crypto lending company Celsius for their many deceptive and fraudulent claims about the company (Johnson & Pozza, 2023). In 2018, the FTC created a Blockchain Working Group to focus on the FTC's ability to regulate blockchain companies in the face of rising fraud in the industry. "The working group has at least three goals. First, build on FTC staff expertise in cryptocurrency and blockchain technology through resource sharing and by hosting outside experts. Second, facilitate internal communication and external coordination on enforcement actions and other related projects. And third, serve as an internal forum for brainstorming potential impacts on the FTC's dual missions and how to address those impacts" (Chilson, 2018).

The FTC has issued guidance to consumers warning about the risks associated with investing in cryptocurrencies and advising them to conduct thorough research and exercise caution before making investment decisions. The agency also provides resources and educational materials to help consumers recognize and avoid cryptocurrency-related scams. While the FTC itself has largely stayed away from crypto regulation, there is a

growing number of calls from within the industry and from within government for the FTC to take a broader role in regulating blockchain companies with broader utility in the greater role of commerce and for consumer protection in the space of digital assets like NFTs (Casey, 2023).

Internal Revenue Service (IRS)

The Internal Revenue Service (IRS) is responsible for enforcing tax laws in the United States, including those related to cryptocurrencies. The IRS treats cryptocurrencies as property for tax purposes, meaning that transactions involving cryptocurrencies are subject to capital gains tax and reporting requirements. Taxpayers are required to report gains or losses from cryptocurrency transactions on their tax returns. Due to concerns over the anonymity of crypto, which allows for tax evasion that contributes to the tax gap, the IRS has consistently attempted to modify and enhance the reporting requirements with regard to crypto transactions.

Financial Crimes Enforcement Network (FinCEN)

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury responsible for combating money laundering and terrorist financing. FinCEN regulates cryptocurrency exchanges and other money services businesses (MSBs) that deal with cryptocurrencies, requiring them to comply with anti-money laundering (AML) and know-your-customer (KYC) regulations. FinCEN also collects and analyzes data on suspicious transactions involving cryptocurrencies.

Federal Reserve

The Federal Reserve, as the central bank of the United States, does not have direct regulatory authority over cryptocurrencies. However, its role in regulating the broader financial system and monetary policy indirectly impacts the cryptocurrency landscape.

The Federal Reserve monitors the financial system for systemic risks and vulnerabilities that could pose threats to financial stability. While cryptocurrencies represent a relatively small portion of the overall financial system, their rapid growth and integration into financial markets may warrant attention from regulators concerned about potential systemic risks. In 2023 the Federal Reserve announced that they will be beginning a new program to allow for oversight of their member banks' crypto activity. In order for a bank that the Fed oversees to engage with crypto they have to obtain pre-approval from the Fed. This sticks the line that the bank regulators have publicly stated with wanting to maintain a stark line between the traditional banking system and crypto (Hamilton, 2023).

The Federal Reserve has also been very clear that they want to see themselves have a significant and robust role involved in the regulation of stablecoins and stablecoin issuers, believing that stablecoins represent risk to the dollar and the overall financial system. Vice Chair of the Fed, Michael Barr, had this to say in regard to stablecoins and the Fed:

> "Private money that's linked to the dollar basically borrows the trust of the Federal Reserve in its issuance…Private money needs to be well regulated…We think there's very strong interest in having strong federal regulation of stablecoins that make sure that the Federal Reserve can approve stablecoin issuers, can regulate stablecoin issuers, can enforce against stablecoin issuers."

State Regulators

The Constitution of the United States instills the governing principles of federalism in the United States. Federalism is a form of government where the national government, which is at the center, shares power with state or local governments. Both levels of government under a federalist system have certain authority and duties. Usually, these authorities are defined to keep a balance of power and to avoid infringing on each

other's authority. This is also true with regards to the banking system in the United States where the debate surrounding the role and powers of the federal government in the banking and financial sector have always been hotly debated. This has resulted in the dual-banking system in the United States where banks can be chartered at the federal level or chartered at the state level though various institutions.

This structure has impacted cryptocurrency. This is increasingly true given the lack of a clear and consistent regulatory framework at the federal level. This has meant that states in the United States have been free to pursue their own crypto regulation in some aspects. This is the case with current stablecoin regulation which essentially is occurring fully at the state level, where stablecoin issuers register with the state as they are deemed as money transmitters (Financial Services Committee, 2023).Some states have passed laws to conduct studies surrounding the benefits or cost of crypto and blockchain and to see where they can update their regulations. Other states have begun passing laws to protect the rights of citizens to own and use cryptocurrency, this is something that has been tried for years in the US Congress, but has not passed. There are a few states however that have enacted detailed regulatory frameworks surrounding crypto companies.

The state of Nebraska passed the Nebraska Financial Innovation Act in 2021. “The Act authorizes a new charter for digital asset depositories and puts the state of Nebraska on the forefront of financial innovation and regulation of the blockchain/digital asset industry” (Nebraska Department of Banking and Finance, 2023). Crypto companies who are chartered in Nebraska are regulated by the Nebraska Department of Banking and Finance. The goal of the act is to provide crypto companies with the space to operate in a

controlled environment and to protect customers, while allowing the state to partner with finance and technology industries and safely grow the state into a leader on the crypto front. This act has allowed for banks to provide more crypto-related services to customers than in many states across the country (Jasperse, 2023).

The state with the most comprehensive and intensive crypto regulation is the state of New York. With New York City and Wall Street being the financial hub of the world, the New York State Department of Financial Services is one of the most advanced state level regulators in the entire country. The NYDFS was incredibly early when it came to regulation of crypto and in 2015 created their guidelines for regulation crypto companies called ‘BitLicense”. Companies must comply with consumer protection rules, KYC, AML and standards of cybersecurity in order to provide services in New York. Over the years the number of crypto companies willing to comply with regulations has increased although several have decided that the requirements are too harmful. One of the major companies to suspend New York operations was the crypto exchange Kraken. Currently the NYDFS under their framework has licensed and regulated major companies such as Coinbase, Gemini, and Robinhood Crypto (NYDFS, 2022).

CHAPTER VII: CHALLENGES TO CRYPTO REGULATION AND NEED FOR REGULATORY CLARITY

As crypto has become more ingrained in everyday life and in the financial markets, along with the growing industry and increased amounts of scandals or frauds, there has been an increased amount of scrutiny placed on the adequacy of the current regulatory structure in the United States as it pertains to digital assets. The criticism of the current regulatory regime comes from all places of the crypto spectrum, from extreme skeptics to the strongest supporters of crypto proliferation. While their arguments differ, there is one common throughline, and that is that the current regulation is not sufficient for the current industry and that congressional action will be needed to provide regulators with the tools and resources necessary to regulate the market along with providing increased clarity to the crypto industry.

Security vs Commodity

The most pressing issue in the discussion surrounding cryptocurrency is the distinction between security and commodity and which tokens fit each category. The current system of regulation for digital assets has not adequately addressed this question. This is primarily due to the fact that the laws and tests used to determine these distinctions are old and were designed for traditional assets. The innovation in technology and the creation of cryptocurrencies stretches these older rules. The rules were not made with cryptocurrencies in mind, which can make them hard to neatly fit inside one of the boxes. The two in question are the Howey Test and the definition of "commodity" in the

Commodity Exchange Act. First, the definition of "commodity" is extremely broad and obviously was not designed with the notion that there could one day be virtual commodities. Second, there are concerns with the application of the Howey Test to digital assets. The test is not designed as a "balancing test." This means that in order for an asset to be declared a security, all of the four elements of the test must be present (Financial Services Committee, 2023). In the case of digital assets, there are unique characteristics that may make the test inapplicable. One of these is if the token has a functional use case, which would eliminate the expectation of profits. Second, if the token is decentralized, then it does not depend on the "efforts of others" (Financial Services Committee, 2023). There was also no existing case law specifically dealing with how to treat digital assets for the longest time. All of this has led to a sort of turf war between the SEC and CFTC, attempting to claim different cryptocurrencies. This creates a massive amount of uncertainty for investors and for the industry and is one of the major problems with the current regulations.

The previous section discussed the official views of the SEC and the CFTC. It is clear that there is a significant amount of conflict between their viewpoints. The SEC, especially as of late under Chair Gensler, has been clear that they believe the Howey Test is applicable to digital assets and that all of them, except Bitcoin, are securities (Gensler, 2023). The CFTC, on the other hand, has maintained that Bitcoin, Ether, and a slew of other tokens are commodities. Outside of this obvious disagreement, the two agencies showcased their differences in 2023 court filings. The CFTC sued the trading exchange Binance, and their filing claimed that the Binance stablecoin, BUSD, is a commodity. However, in a separate filing, the SEC has alleged that BUSD is a security (Financial

Services and Agriculture Committee, 2023). These views are further muddled by Chair Gensler's statements in the previous year where he called for the CFTC to take a more active role in the regulation of stablecoins. This, once again, puts the agencies at direct odds with one another, adding confusion to the market.

The basic views of the CFTC and SEC are also not universally agreed upon, even amongst former employees of the agencies. SEC Commissioner Hester Peirce and former Commissioner Elad Roisman have both stated that they do not agree with Chair Gensler's assertion that the Howey test is clear on how to treat digital assets (Peirce & Roisman, 2021). The idea that the test is not always clear is backed up by the sheer amount of requests for clarity and assistance the SEC has received from the industry. This disagreement also extends to the CFTC, where former Commissioner Dan Berkovitz has stated that Ether can be both a security and commodity, which is a novel interpretation and would put the token under the oversight of both agencies (Mitchelhill, 2023). All of this further reinforces the point that there is significant confusion in the market, lack of clarity and lack of a consensus on how to classify digital assets, highlighting the necessity of Congressional action to provide definitive answers.

The reason that the debate over cryptocurrencies being a security or a commodity is so important is due to how they are regulated. The law of the United States treats these financial assets incredibly differently. For one, they are regulated by different bodies. More importantly however, the authority of the SEC and security law is considered stronger. This means that for tokens that are deemed securities the issuers and exchanges would have to go through the process of obtaining a license from the SEC. This process

is tricky and quite difficult to complete. This might make certain projects leave the US or have exchanges delist the tokens in order to avoid an enforcement action.

It seems clear the many cryptocurrencies have characteristics of both commodities and securities creating a significant gray area in how they should be treated. There is a starting point we can use when trying to figure out where each asset fits. Virtually everyone agrees that Bitcoin is a commodity. As mentioned previously, Coinbase rejects more than 90% of the tokens that apply to be listed on their exchange because it doesn't meet their standards. It is relatively safe to assume if a token is rejected by Coinbase it is most likely a security. That means there are several hundred tokens that have at least some gray area.

> First, it seems clear that ICOs do meet the Howey Test and are thus securities offerings. This has been the view of the SEC and it seems to be supported by the Ripple ruling as well which found that institutional sales did meet the requirements of an investment contract. This makes sense, most of these ICOs were done by these blockchain projects in order to fund development. How do you get people to invest? You market the asset as an investment that will generate a profit based on the work you are able to do with the funding. This has been the case in the marketing of ICOs. Some are even incredibly explicit, such as the CEO of Kik, Ted Livingston saying that buying their token would make investors "a ton of money." (Stevens, 2024). The Ripple ruling also states that it is not the token themselves that are securities, but rather the circumstances surrounding them. The SEC has accepted this ruling and has updated the language of their

enforcement actions to match it. Let us take a look at three tokens, Ethereum, Solana, and Dogecoin, to see the arguments.

We will start with Ethereum, which is an important case due to the fact it is the second largest cryptocurrency. It is also an interesting case as there is strict disagreement between the SEC and CFTC. The case for Ethereum being classified as a security is pretty straightforward. The Ethereum Foundation raised 18 million dollars via sales of their tokens to initially fund the development of the blockchain. The foundation is still incredibly active, constantly proposing changes to make fixes to the code. The foundation also pays salaries to the developers. This work by the foundation is also explicitly done to increase the value of the token. The founders also allocated a massive number of tokens to themselves not through a process related to how the token functions. The lead founder, Vitalik Buterin, also remains incredibly influential over the future of development.

Additionally, following the switch to Proof of Stake, the Ethereum blockchain has become significantly less decentralized. “over 85% of Ethereum’s supply is held by entities with 100 ETH or more. Around 30% of its supply lies in the hands of entities with over 100,000 ETH” (Radmilac and Van Straten, 2022). This becomes problematic because it requires a minimum of 32 ETH to be staked in order to be a validator. This can essentially remove small users from being able to play a role in securing the blockchain as “69% of the total amount staked on the Beacon Chain is staked by just 11 providers. A total of 60% of the staked supply is staked by four providers, while a single provider, Lido, accounts for 31% of the staked supply” (Radmilac and Van Straten, 2022).

However, the view of Ethereum as a security is not agreed upon. Some have argued that Ethereum shouldn’t be deemed a security because it has been allowed to

operate as a commodity for nearly a decade. This argument doesn't hold up well. First, the blockchain switching from proof of work to proof of stake massively alters how it can be viewed. Second, the Howey Test comes from case law and is not a statute, so there is no statute of limitations on when the SEC can allege Ethereum is an unregistered security.

A better argument can be made. First, the SEC in October, 2023 approved several ETH Futures to be traded on SEC regulated exchanges. This seems to be an admission by the SEC that Ethereum is not a security and thus not under their jurisdiction. Some have also argued that even with the presence of Ethereum Foundation, the network is still significantly decentralized as there are thousands of other validators. Ethereum presents an interesting case and may be an example of a hybrid asset.

Solana, a token created as an alternative to Ethereum, seems to present a much clearer example of a security.

1) Investment of money?: Yes, Solana sold SOL tokens to raise money to fund the development of the blockchain

2) Is there a common enterprise?: Yes, there is a foundation that works to develop the blockchain to compete with other projects like Ethereum and Cardano to attract users. The foundation also has a considerable amount of control over the network. Solana frequently breaks and the foundation pauses the blockchain for a period of time to make fixes.

3) Expectation of profits? Yes, people purchased SOL hoping to make money.

4) Effort of others?: Yes, SOL increased in value due to the efforts of the developers within the common enterprise. This was the explicit goal that Solana stated when originally raising funds. They stated that the funds would go towards development, operations, and marketing which would attract users. The increased user base would increase demand for SOL and thus the value.

Even with this clean cut argument, there is still some gray area. The development of the Solana blockchain is not solely dependent on the efforts of the foundation, but also on

independent and third-party users and developers. This means that like most blockchains, Solana is at least in part decentralized. Furthermore, it can be argued that not everyone who purchased SOL as a speculative investment with the goal of making a profit. They have done so to complete transactions on the blockchain or to run programs. In this case SOL was purchased merely as a utility token which would make it not a security. Since most cryptocurrencies have both functional utility and investment qualities, analyzing them as securities can be tricky.

It seems to be that a lot of crypto tokens are simply a stand-in for stock in tech firms. The business is the blockchain ecosystem that is used for building apps and everyone who purchases these tokens is very similar to a shareholder of a company. In some cases, like FTX's FTT token, they are clearly a work around of the law. Instead of having to go through the process of registering with the SEC to issue stock, the company can just issue a token in order to raise funds. Now while a lot of crypto projects do have the goal of creating a decentralized ecosystem not owned by a central team, like Solana or Ethereum for example, their systems were built and are still developed largely by centralized groups. In the case of Solana, much of the promise behind the project was directly tied to the background of the founder, Anatoly Yakovenko. Yakovenko was the lead developer of operating systems at Qualcomm and many who bought SOL did so because they believed his background would allow Solana Labs to be successful in developing the blockchain to overtake Ethereum.

There is another argument against cryptocurrencies being securities that can be called the Beanie Baby argument. This is an argument that the lawyers for Coinbase have trotted out in court filings related to their lawsuit with the SEC. The argument is that

some cryptocurrencies are more like collectibles, like a Beanie Baby or a baseball card, than it is stock in a company. A Coinbase attorney said this, "It's the difference between buying Beanie Babies Inc. and buying Beanie Babies." Under this explanation, cryptocurrency would be neither a security nor a commodity. One token that can represent this argument is the meme token, Dogecoin. Dogecoin is purely a joke and it is explicitly worthless. There are no efforts by the creators of Dogecoin to build or develop a broader blockchain ecosystem. The people who buy Dogecoin do not expect profits based on the efforts of others but rather under the belief that others will buy Dogecoin and drive the cost up. This means that Dogecoin does not meet the Howey Test, however it is hardly plausible to make an argument for Dogecoin as a commodity. This raises the question of who should be the authority that oversees Dogecoin? The answer is easy. If Dogecoin is akin to a Beanie Baby, what is the body that regulates their sale? That would be the Federal Trade Commission. This interpretation highlights the need for a more robust role of the FTC in overseeing the crypto market.

Complaints About SEC Regulatory Actions

There are a wide variety of complaints against the actions of the SEC that are outside of their application of the Howey Test and views that the test is clear and that almost all cryptocurrencies are securities. While the majority of the harshest of these critiques come from the larger cryptocurrency industry, a number has been raised by lawmakers on the Hill and various experts. All the criticisms take aim at the overall approach to regulation that the SEC has taken, claiming that they have created more confusion, a lack of clarity, have not been transparent, and overall the policy approach has been ineffective.

The crypto industry has been harshest in their rhetoric against Chair Gensler and the SEC, saying that they are waging "a war on crypto" and taking aim at the agency's approach to policymaking that they have labeled "regulation by enforcement". The industry takes issue with the abandonment of the agency's chief responsibility which is to be a rulemaking body. Rather than providing official rules or guidance the SEC has relied on enforcement actions and statements from Chair Gensler to answer the question of whether cryptocurrencies meet the conditions of an "investment contract" thus making them a security. Gensler and the SEC have also taken an absolutist stance on the question, stating that all tokens outside of Bitcoin are securities, which stand outside the scope of court rulings that say the Howey Test must be carefully applied and take into account the facts of each individual case (Wolf, 2023). The Blockchain Association, the primary trade association for the crypto industry, wrote this in a piece, "Despite continued requests from the industry for regulatory clarity, the SEC has refused to adopt any rules or issue any guidance on this issue, among many others, for over four years. Instead, the SEC has chosen to regulate digital assets solely through enforcement actions" (Wolf, 2023). The SEC has not produced any guidance since 2019 on the question and has not passed any rules related to cryptocurrency.

The largest crypto exchange in the United States, Coinbase, has also been incredibly public about its gripes with the SEC. As previously discussed in March, 2023 Coinbase received a "Wells Notice" from the SEC, essentially the precursor to the eventual enforcement action against Coinbase for engaging in unregistered securities offerings. After the notice, Coinbase went public with many complaints. First, the SEC reviewed the business practices of Coinbase in 2021 before allowing them to become a

publicly traded company. Coinbase claims to have asked the SEC which tokens they viewed to be securities and the SEC staff refused to provide an answer. The SEC approached Coinbase, asking them what they thought a registration model could look like, admitting that there currently is none in place; after Coinbase spent millions developing two different models, the SEC provided zero feedback. Coinbase has frequently asked the SEC to question any of the assets on its platform, and the SEC never raised any concerns with them before the notice. The SEC has long held the position that all crypto companies need to is "come in and register" however Coinbase met with the SEC 30 times over nine months and received no feedback or guidance on how to register (Grewal, 2023).

There is evidence to back up what Coinbase and the industry are saying: there is a lack of crypto companies that have registered with the SEC. Out of the thousands of crypto companies in the United States, only a small number have actually gone through and registered with the SEC, not including any of the major players. The CEO, Alan Silbert, of the crypto exchange INX, stated that the process needs significant improvement (Dale, 2023). It is not that these companies do not want regulation, many of the best faith companies openly call for it. Take Coinbase, for example, has stated, "Tell us the rules, and we will follow them. Give us an actual path to register, and we will register" (Grewal, 2023). It is the view of the industry that the approach from the SEC has been wholly inadequate and that it is the job of Congress to act to provide clarity, answer the important questions and provide a regulatory framework.

There are many other stakeholders that have also raised concerns about the SEC's approach to regulating digital assets. While Republicans have been most boisterous in

their attacks against the agency, explainable in part due the political environment, as Gary Gensler is a Democrat appointed by President Biden, the criticism has also been bipartisan. Multiple Democratic members of the House Financial Services Committee have raised concerns about the SEC's crypto policy. One of the members is Congressman Stephen Lynch of Massachussetts who during a hearing with Chair Gensler questioned the SEC's "retroactive policymaking" as opposed to "proactive policymanking. This is in line with the industry criticism that the agency is overly reliant on enforcement actions instead of utilizing the rulemaking process to provide clear rules and issue guidance to crypto companies on how to operate within the bounds of the law. This view is in line with the view of SEC Commissioner Heather Pierce, who has criticized the overall approach of the agency as not having a clear objective. Pierce stated, "There doesn't seem to be a rhyme or reason for a lot of cases we bring," and "litigation is not the most effective way to carry out regulations" (Wagner, 2023).

Another prominent Democrat who has publicly spoken out against the SEC is Congressman Ritchie Torres of New York, who is frequently viewed as one of the most pro-cryptocurrency Democrats. He has echoed much of the same language of the industry and Republicans, calling the SEC "an overzealous traffic cop" and stating in a letter after the Ripple court ruling, "writing to inquire if the SEC intends to come to terms with the folly of the Commission's crusade against crypto assets in light of the latest decision by Judge Analisa Torres of the Southern District of New York…Needless to say, regulation by enforcement had a dreadful day in court". Torres also penned a bipartisan letter in coordination with Rep. Mike Flood (Nebraska), taking aim at the SEC's proposed expansion of the qualified custodian rule. The agency appeared to be angling to expand

the rule to curtail the power of state regulators in defining who is deemed a qualified custodian. Both Torres and Flood hail from states that have developed their own regulatory frameworks surrounding digital assets, and the fear was that the SEC was attempting to usurp their authority (Leonardo, 2023). These arguments are that there is a vast array of stakeholders who are dissatisfied with the approach of the SEC, and there is a growing consensus that Congress must act to answer the questions.

Competitiveness of the US

There is an argument, coming primarily from the crypto industry, that is aligned with their arguments against the SEC actions that the lack of clarity in US regulations is making the United States fall behind the rest of the world in crypt regulation. This is an argument about US competitiveness in the market and that because crypto companies are asking for clear regulations and not receiving them from the United States they will begin to search elsewhere to domicile their companies. This applies to new companies and projects along with existing US companies looking for new jurisdictions that have comprehensive regulations that allow them to operate clearly. The industry argues that the United States is now in last place in the G7 in terms of providing clear guidance and regulations to the crypto industry. Policymakers are concerned with this argument because the United States will miss out on the potential benefits of the crypto market and will also not lead the world in the innovation of blockchain technology, cryptocurrency, and financial technology.

This argument is not entirely off based. A growing number of crypto companies and projects are looking for countries with more comprehensive regulations to headquarters their operation due to fear that the uncertainty in the United States makes it incredibly difficult to operate (Yaffe-Bellany, 2023). This includes Bittrex crypto

exchange, which shut down its US operations, citing the regulatory environment in the United States as the chief reason. The company states that it is “no longer feasible” to operate inside the United States (Yaffe-Bellany, 2023). Coinbase and Gemini have also started to seek licenses in other countries, with Coinbase receiving a license in Bermuda (Yaffe-Bellany, 2023). However, neither of those companies have made any serious indications that they plan on leaving the United States. This largely indicates a broader pattern: that serious crypto companies do want serious regulation of the market by the United States. Most of the companies that are leaving the United States or beginning in some other country are choosing countries that are incredibly lenient on crypto and very friendly countries. This is primarily because these companies are seeking to avoid scrutiny because their practices would not meet the high standards that are typical of the United States financial system to begin with. That is why there has been such a high number of crypto companies domiciling themselves in the Bahamas and other crypto friendly countries, a prime example of this is FTX.

While it is important for the United States to create regulations that provide clarity to companies so that they know how they can operate without fear of harsh enforcement actions, if the United States passes new regulations surrounding crypto, there will most likely be a mass exodus of crypto projects regardless due to the high number of bad actors in the market. Regardless of what the truth is on this front, the fact that other advanced economies have been able to take steps towards creating regulations, including the approval of the European Union MiCA regulations and the UK efforts to make themselves a development hub, showcases that there is no reason for the United States Congress not to take action.

Prevalence of Frauds

One of the most simplistic arguments against the current regulations is that they have not done enough or been able to prevent fraud from occurring. The premise is easy to grasp. If we assume that we want to limit or end fraud in the crypto industry, then the regulations present should be sufficient to do so. Since there has been an ample amount of fraud in the crypto industry under these regulations they are not adequate and new regulations or rules must be passed to make them appropriate.

This is a salient argument; the amount of scandals that have plagued cryptocurrency has been incredibly high, and the amount of money customers have lost due to scams, such as misleading marketing or outright fraud, is in the billions of dollars. The current actions that have been taken by the SEC, FTC, or other regulatory bodies have not stopped any of the total disasters such as FTX, Celsius, or the many instances of pump-and-dump schemes or fraudulent ICOs. The existing structure of regulation for stablecoins did not prevent the collapse of the Terra/Luna stablecoin regime, which resulted in tens of billions of dollars in losses to holders due to the collapse of the asset price. The endpoint of is that the regulations must bring the industry into control, limiting the number of frauds and scams and, most importantly, protecting customer funds.

Regulatory Gaps

The term “regulatory gaps” represents two things in the context of cryptocurrency regulation. The first concerns the debate surrounding which cryptocurrencies are securities and which are commodities. The current ongoing debate, the mixed signals from the SEC and the CFTC, court cases, and attempting to fit the existing rule onto cryptocurrency has created a regulatory gap in which there are several cryptocurrencies that are not sure where they classify. This creates uncertainty for crypto companies along

with investors as there is a batch of cryptocurrencies that currently operate in a sort of limbo. The conflicting views of the SEC, CFTC, and various court rulings showcase the necessity for Congressional action to provide a clear answer and close this gap.

The second regulatory gap specifically relates to the CFTC and the authority that they are granted under current law. This critique is two-pronged and relates to the language of The Commodity Exchange Act (CEA). First, the definition of "commodity" is incredibly broad in the CEA and there is not a precise test that has been established that can clearly be used to help guide the classification of digital assets. This provides Congress with the opportunity to provide additional language in the definition of commodity in order to make it more clear and applicable to cryptocurrencies. The second part of this is that the CFTC really lacks the authority to properly regulate the market of cryptocurrencies that are deemed commodities. Under the CEA the CFT has broad authority over derivatives and can bring civil actions in instances of fraud. "The Commission currently does not have regulatory authority over spot market transactions unless the transaction is a margin, leveraged, or financed retail commodity transaction or retail foreign exchange transaction. As such, the CFTC currently does not have regulatory authority over spot market transactions or intermediaries in the digital commodity spot markets" (Financial Services Committee, 2023). This means that even cryptocurrencies that are deemed commodities by the CFTC have a lack of ability to regulate the activity in the market truly. This in itself can be a gap in regulation, but it is even more pressing if there is to be a greater number of cryptocurrencies deemed commodities. Additionally, there are concerns that the staff at the CTFC lacks the size and expertise to handle the sheer volume of activity in the crypto market.

Stablecoins

Stablecoins have been able to work themselves into their own silo of the cryptocurrency industry, and the policy discussions surrounding how to handle them have been different and separate from the rest. Reaching a bipartisan consensus surrounding stablecoin legislation and regulation has long been viewed as the "low hanging fruit" of crypto policy. Stablecoin issuers have been able to make the case that stablecoins represent a payment system that offers benefits and use cases, such as being an on and off ramp to other digital assets, providing protection for customers, able to empower economically disadvantaged people by giving them access to digital dollars and allowing for cross border transactions, and serving to help preserve the US Dollar as the global reserve currency (Chervinsky & Blockchain Association, 2023). There was also the example of stablecoin company, Circle, partnering with the United Nations to help provide financial aid to Ukrainian Refugees by utilizing their stablecoin (Disparte & Circle, 2023).

The current regulation for stablecoins is primarily handled only at the state level, with each state having its own regulations. This is due to the lack of clarity at the federal level on how to treat stablecoins. This has led to the calls for legislation from Congress to provide these answers to Federal agencies. This dates back to the President's Working Group on Financial Markets, which in 2021 released a report on stablecoins in which they highlighted the benefits and risks. The report stated the necessity of Congress to pass legislation that brought stablecoins under a federal prudential regulatory framework (Financial Services Committee, 2023). This is where the Fed asking to be a part of

overseeing stablecoins comes in. The stablecoin industry has been wanting regulation at the federal level and welcoming oversight from the Fed.

The industry has also noted that the SEC and CFTC have very limited authority over stablecoins. This is due to the fact that the SEC and CFTC are financial market regulators and do not oversee payment systems (Chervinsky & Blockchain Association, 2023). This is designed by the law rather than a shortcoming in regulation, meaning those two agencies should have a limited impact in regulating these assets. This is at odds with actions and statements by both the SEC and CFTC who have been fighting over jurisdiction of various stablecoin assets.

While there are still ongoing disagreements and discussions surrounding stablecoin policy, the bipartisan nature of this policy and the general groundwork laid on it seems to indicate that some comprehensive stablecoin legislation will pass Congress.

Illicit Uses

As previously mentioned, one of the major concerns when it comes to the proliferation of cryptocurrency throughout the financial system and across the globe is the potential use case for illicit uses such as money laundering, terrorism and other criminal purposes. As explored, the evidence that this is a prominent use for cryptocurrencies is limited and cash is still the primary vehicle for criminal usages. This is primarily because cryptocurrencies are not a perfect substitute for cash, and any bad actor seeking to carry out financial crimes would prefer cash. However, due to the global nature of cryptocurrencies, there are some benefits for bad actors, such as being able to send payments across borders and the ability to circumvent sanctions. Because of this, policymakers have stayed interested in exploring policy options to limit or investigate the

illicit uses of cryptocurrencies, such as expanding AML regulations. While this is the more of a top priority for crypto skeptics, most notably Senator Elizabeth Warren, there has been broad interest across the spectrum for finding some legislation on this front. These policy discussions go straight to the heart of one of the key questions, which is balancing privacy versus security. As previously explored, many cryptocurrency are drawn to the anonymity of cryptocurrency for legitimate reasons, one of the chief reasons they were created was to provide for uncensored transactions from the government.

Recent Congressional Activity

The interest and buzz on Capitol Hill surrounding cryptocurrency and passing substantial regulation has never been higher than it has been in the 118th Congress. This was driven by the collapse of FTX which truly brought the problems of both the current regulations and of the industry to the forefront for both the public and for Congress. Most of the Congressional action has taken place in the US House of Representatives rather than in the US Senate. This action has been primarily driven by House Republicans after they took control of the House in the beginning of 2023. As part of the first actions of the majority the House Financial Services Committee (HFSC) and the House Agriculture Committee created new subcommittees, specifically related to digital assets. In the House, the Financial Services Committee has jurisdiction over the financial system, including the SEC. The Agriculture Committee oversees the CFTC. It has been the expressed intent of House Republicans, most notably Financial Services Committee Chairman Patrick McHenry, to pass significant legislation surrounding cryptocurrency. Three committees in the House, HFSC, the Agriculture Committee, and the Energy & Committee, have held hearings related to cryptocurrency, covering issues such as

stablecoins, regulatory gaps, AML and illicit uses, broader blockchain uses, and security vs commodity. Additionally, all three of these committees have passed bills through their committees.

While the House has been active on the issues, the other side of Capitol Hill has seemed much less interested in pursuing legislation. Outside of an investigative hearing on FTX, the Senate Banking Committee, under the guidance of Chairman Sherrod Brown, has not held any additional hearing on cryptocurrency. Senator Brown has seemed somewhat uninterested in pursuing comprehensive legislation, potentially highlighting a roadblock for major regulation to pass in the near future. Regarding the political breakdown of view on cryptocurrency, the traditional partisan divide doesn't necessarily exist on this issue. While Republicans generally appear to be more pro-cryptocurrency and the industry as a whole and Democrats more negative, numerous examples of crossovers and policy negotiations on the House side have been relatively bipartisan.

CHAPTER VIII: POLICY PROPOSALS AND RECOMMENDATIONS

Overview and Regulatory Framework

Before analyzing the individual policy proposals, it is necessary to establish what the goal should be when it comes to passing comprehensive cryptocurrency regulations and establishing a regulatory framework surrounding digital assets. The first part of this is defining what a regulatory framework means. A regulatory framework refers to a system of laws, regulations, guidelines, and enforcement mechanisms established by governments or regulatory authorities to govern a particular industry, sector, or activity. The primary purpose of a regulatory framework is to ensure that organizations, businesses, and individuals operate in compliance with applicable laws and regulations while also achieving specific policy objectives such as consumer protection, public health, environmental conservation, financial stability, or national security.

The most important part of the regulatory framework is that it must allow for serious innovators to remain in the United States. If we believe that cryptocurrency and blockchain technology might provide immense or revolutionize our world, then it is important for the United States to be a leading nation. This means that Congress must act to provide clear rules to the road. This includes closing the regulatory gaps. First, providing a set of criteria for digital assets that can be used to classify an asset as a security or commodity on an individual basis. Second, grant the CFTC the necessary authority to truly regulate the assets that are defined as commodities. Third, there must be strict requirements placed on crypto companies to ensure that there is significant

customer protections, which can help prevent fraud. With a foundation laid, we can begin to access various policy proposals.

Market Structure

When it comes to the regulation of cryptocurrencies, the term market structure deals with how tokens should be characterized as securities or commodities and also addresses the delineation of authority between the CFTC and SEC. The 118th Congress has seen two significant bills that deal with this question differently. The first comes from the House Financial Service Committee and the House Agriculture Committee, the *Financial Innovation and Technology for the 21st Century Act* or the FIT Act. The Second is a bipartisan Senate Bill sponsored by Senators Cynthia Lummis (R-WY) and Kirsten Gillibrand (D-NY), the *Responsible Financial Innovation Act* or RFIA Act.

Financial Innovation and Technology for the 21st Century Act

The FIT Act aims to resolve the uncertainty of which digital assets are a security or a commodity by creating classification criteria and setting in place new regulatory requirements. A digital asset would be classified as a commodity and thus regulated by the CFTC if the blockchain in which the assets run is functional and decentralized, creating a pathway for a digital asset that is initially offered as a security to become a commodity over time. A blockchain is considered "functional" if it allows participants to use the digital assets for transmission and storage, participate in the governance of the blockchain, or participate in an app that runs on the blockchain. The requirements for a blockchain network to be a "decentralized network" are

1) No singular person can unilaterally alter the function of the network or restrict someone from using the network for the past year.
2) No issuer has 20% or more of the outstanding digital asset in the last year.

3) The issuer did not market the asset or network to the public or issue units of the asset for the past 3 months.

4) The tokens issued in the prior year were end user distributions (i.e airdrop or mining reward)

The bill institutes a parallel permission process for firms to submit applications to the SEC or the CFTC to certify that the digital asset is on a decentralized network. The certification application explains who the filer is with requirements on specific information. Also, it must provide a detailed analysis of how that network is decentralized by meeting the criteria outlined in the bill. The certification will be approved within 30 days unless the SEC or SFTC provide a detailed rebuttal to the application, explaining that the network is not decentralized. There is also a process for the filer to then appeal this decision from the regulators (Tierno & Scott, 2023).

This bill addresses a regulatory gap by granting the CFTC new authorities, including giving it sole jurisdiction over "spot" market digital commodities. These new authorities to deal with regulating the new "digital asset commodities". The CFTC is given the power to regulate three types of intermediaries: Digital Commodity Exchanges, Digital commodity Brokers, and Digital Commodity Dealers. These entities would have to monitor for fraud or manipulation, eliminate their conflict of interest to a reasonable level, maintain books and records to the CFTC's standard and have them readily available, separate customer and company funds, and meet minimum capital requirements. These intermediaries will be required to register with the CFTC and comply with the rules of the Commodity Exchange Act, along with additional rules implemented by the CFTC (Tierno & Scott, 2023). The bill also grants the CFTC an additional $120 million, giving them the resources to carry out these new responsibilities.

The assets that do not meet the criteria for being decentralized are classified as securities and subject to the authority of the SEC. The bill also contains language that is consistent with the ruling in *SEC v. Ripple* that states that if an asset is sold pursuant to investment contracts are not necessarily securities themselves. Primary market transactions will be subject to disclosure requirements similar to traditional security disclosures. For secondary market transactions, there will be a new system of registration for digital asset trading platforms and brokers. These intermediates would still be able to register under existing SEC regulations, but the bill requires the SEC to institute a new set of rules for these entities. The bill allows certain digital assets to be exempt from current securities regulation if they meet a set of requirements. Such as restrictions on the amount of transactions, access caps, purchase limits, and disclosure requirements. If the issuer relies on this exemption to offer security, then they must file with the SEC and maintain periodic reports.

The bill gives the SEC and the CFTC a lot of authority to write and implement the rules that would institute the board requirements laid out in the act. As this will take time to complete the bill also for intermediaries to file for provisional registration with SEC or CFTC which grants them the ability to operate without fear of receiving enforcement actions for not meeting requirements that are not yet fully implemented (Tierno & Scott, 2023).

In July 2023, the FIT Act passed both the Financial Services Committee and the Agriculture Committee, receiving bipartisan support in both. The vote in HFSC was 35-15, including all Republicans on the committee and 6 Democrats. The bill passed by voice in the Agriculture Committee, signifying a higher level of bipartisan support.The

overwhelming reason why members voted for this bill was that it is far better than the current status quo, which has been chaos in the industry, resulting in a lack of customer protections, lack of clarity from regulators, innovation going overseas, and massive scandals such as FTX or Celsius. Concerns raised by members who voted against the bill were that the consumer protections were not strong enough, particularly regarding the commingling of funds; the entire thing is not necessary because existing securities law already fits crypto, and the protection during the provisional registration period is too long. The bill has not received any action on the floor of the House as additional negotiations are still ongoing on how to reach a significant bipartisan agreement, specifically trying to determine how to get the bill through the Senate.

Responsible Financial Innovation Act

The RFIA has been introduced in multiple Congress now but has yet to receive any significant traction. The bill attempts to be incredibly comprehensive, covering the questions of market structure, stablecoins, taxation, and illicit financing. This approach has been ineffective, as it takes getting members on board with all of the provisions rather than splitting them up into smaller bills on each issue.

The bill states that CFTC has authority over digital assets that are deemed commodities, and the SEC has authority over those deemed securities. However, the bill's text doesn't include a specific definition or set of criteria for these classifications. It does carve into the SEC's authority by allowing issuers whose efforts "primarily determine" the value of the asset to avoid the full scrutiny of security law. The RFIA also grants the CFTC with the power to regulate spot markets for digital assets in a similar manner to the FIT Act. It also allows for digital asset exchanges to be registered with the

CFTC, subjecting them to a set of requirements regarding reporting, removing conflicts of interest and preventing the commingling of customer funds (Scott, et al, 2022).

The RFIA takes a novel approach, with one of the sections creating a new asset category specifically for digital assets, called "ancillary assets". "Ancillary assets would include digital assets that are sold pursuant to investment contracts but do not provide their holders with financial interests in a business entity" (Scott, et all, 2022). Issuers of ancillary assets would be required to issue disclosures that will be administered by the SEC. Once these disclosures are met, the asset would be treated as a commodity and not a security giving the CFTC regulatory authority.

Recommendation

There is a lot to work through with these proposals as they have massive implications for the cryptocurrency market. First, the framework that is laid out in the *Responsible Financial Innovation Act* is massively incomplete, rendering the bill inadequate to be passed. This is primarily the reason why the bill has received essentially no legislative traction despite being introduced in multiple Congress. The bill states that digital asset commodities will be regulated by CFTC and digital asset commodities will be regulated by the SEC. This provides almost no new information because we have already established in law that the SEC regulates securities and the CFTC regulates commodities. The most glaring omission from this bill is the fact that it provides no definition, criteria or test that can be applied to a digital asset in order to determine if it is a commodity or security. The lack of this makes the bill largely useless because that is one of the key questions we are seeking to answer through legislative action.

There is one intriguing section about the bill and that is the creation of "ancillary assets." This is sort of in the vein of the European Union approach which is to create a separate asset class for cryptocurrencies. This acknowledges that the old lines between commodity and security that were drawn for traditional assets are a bit blurred when it comes to cryptocurrencies. There is something interesting about creating a system that shares authority between the SEC and CFTC. However, this idea is also half baked in the proposal.

The much more interesting bill is the *FIT Act* as it has passed committee with at least some level of bipartisan support and is expecting a floor vote at some point this Congress. The bill does accomplish some really good things and largely represents a step in the right direction, however questions and concerns still remain.

The bill takes a good approach in its framework for determining if a digital asset is a commodity with the "decentralized" and "functional" tests. However, the question is whether it gets the criteria correct, specifically when it comes to the criteria it sets in place for "decentralized." The text in the bill for determining if a digital asset is decentralized is far too broad. The language says that "no singular person" can alter the network. This certainly will encompass far too many assets that are very much centralized. Under these broad definitions it seems a large majority of tokens would meet that definition of decentralized and functional. The SEC has listed 30+ tokens by name as securities in their various enforcement actions with Coinbase, Kraken and several others. It is likely safe to say most of those tokens listed as securities would meet the definition of decentralized and functional under the current language and would be deemed commodities. This would include a token like Solana. As we discussed, there is an

incredibly strong case to be made that Solana does meet the Howey Test and can be classified as a security, however this bill would classify it as a commodity.

Proponents of the bill would argue that even if this definition is too broad it is ok. This is because at least it is providing clear guidelines and rules for the market to operate under. Additionally, the bill grants the additional authority that the CFTC would need in order to regulate this market effectively. I agree with a great deal of this assessment, however there seems to be a better path forward. This bill could strengthen the criteria for being decentralized, thus only encapsulating the cryptocurrencies that are truly decentralized, like Bitcoin. Additionally, a section can be incorporated that is similar to the "ancillary asset" approach. This would be greeting a second set of criteria for assets that aren't quite purely commodities, but also not fully securities. A prime example for a token that might fit this definition would be Ethereum. The assets would be forced to provide certain disclosures to the SEC, however the primary regulatory authority would still rest with the CFTC under their new powers.

Even given this gripe with the text of the bill it still accomplishes a lot. Primarily when it comes to customer protections and overall just boosting the amount of transparency and oversight that would occur in the market. The concerns presented by opponents that the bill would still allow for the comingling of customer funds do not appear to be true. An independent analysis of the bill by the Congressional Research Service found this:

"The bill would impose certain requirements on intermediaries, including ensuring trading is not susceptible to manipulation, requiring disclosures, and addressing market integrity and recordkeeping requirements. Seeming to address concerns that platforms' current consolidation of various functions represents a conflict of interest, the bill would prohibit an exchange from acting as a counterparty to transactions on its own platform. The bill

would prohibit platforms from comingling their own funds with those of customers" (Tierno & Scott, 2023).

These provisions are crucial given the amount of fraud that has been prevalent in the cryptocurrency space. The requirements that are set forth in this bill could very easily have prevented the FTX fiasco and that alone makes a strong case for its passage.

While I do not think that this bill is perfect and urge that Congress make the necessary changes to it. I would still recommend passing this bill because of the major improvements to the overall market that it does provide. I take a very similar view to Rep. Jim Himes (D-CT) who said this on the *FIT Act*:

"My question is does it improve on the status quo? I am confident that this legislation, while not perfect, makes the status quo better. Are we comfortable walking away having done nothing? The status quo is this, $2 trillion in value lost in the crypto asset markets. An FTX collapse which might have been prevented by this legislation. We don't want to see another FTX collapse. An algorithmic stablecoin allowed to flourish until it to collapsed and evaporated. An inability of our regulator to look at Ethereum and say we don't know if this is a security or not. Coinbase going to the SEC and saying we want to register, we want to comply, how do we do that? No answer, no answer, until the SEC issues litigation against this entity who went to the SEC and said we want to be regulated. That is the status quo, utter lack of transparency, total chaos. I think that this industry is filled with utter nonsense. I don't get a lot of the insanity that is being peddled in the crypto market. But I feel the way I did in 1999 when the internet was new, and there was an immense amount of utter nonsense, but the internet proved to be valuable. I am a deep skeptic of this industry, but we deserve better than the status quo."

The status quo is not acceptable and should not be allowed to continue in the United States. This bill does represent a massive improvement in the current status quo, by providing clear rules to guide innovators, regulators and investors. This bill addresses the regulatory gaps in the market even if not perfect. This bill also provides a comprehensive list of requirements that will increase regulation, transparency and oversight of the market that will better protect customers. It is true that a vast majority of the industry is nonsense, blockchain projects and tokens that make no sense, but at its

core cryptocurrency was a revolutionary innovation that promised to rethink our financial system. This legislation does right by that promise.

Central Bank Digital Currency (CBDC)

The creation of a Central Bank Digital Currency or CBDC is one of the biggest political hot button issues when it comes to the broader crypto policy landscape. A CBDC is a digital form of a country's national currency issued and regulated by its central bank. Unlike cryptocurrencies such as Bitcoin or Ethereum, which operate on decentralized blockchain networks, CBDCs are centralized and issued by a government authority. CBDCs aim to provide a digital representation of a country's fiat currency, allowing for electronic payments and transactions while retaining the stability and security associated with traditional currency (Nelson, 2023)

One of the key concerns of a CBDC is technological design. The fundamental foundation for Bitcoin and other cryptocurrencies is the decentralized ledger stored on the blockchain. If a CBDC is run by one singular entity, the Fed (Central Bank), then there is no reason for it to be stored on a blockchain. There is also the question of whether or not the central bank should then provide wallet services, essentially creating a central bank account, or whether it will use third-party service providers. Finally, how much information does the Central Bank have access to? Will they in real time be able to see where each "digital dollar" is being stored and what it is used to purchase? If not, then how can a digital dollar instituted by a central party not possess these properties? Overall, there are a lot of questions surrounding how to build a CBDC that has not been figured out.

Proponents of creating a CBDC in the United States have cited benefits in several areas, such as modernizing payment systems both domestically and internationally,

strengthening the dollar as the global currency, and supporting the monetary policy of the central bank, and that it will help to mitigate risks from the rest of the financial system. A CBDC can modernize the payment system by allowing for streamlined processes that settle transactions in real time at lower costs. This would make the payment system faster, cheaper, and more efficient overall. Additionally, offering digital wallet services to the current unbanked population can help expand access to financial services. Proponents of a CBDC also make the similar arguments to those who prefer stablecoin and that is that it would help facilitate global transactions, allowing people to send dollars around the world at fast rates, which would only strengthen the position of the dollar.

There are also a wide variety of potential risks associated with CBDCs that opponents frequently reference, chief amongst them is privacy concerns. A CBDC would essentially give the central bank and federal government access to all users' financial information related to transactions and banking, resulting in a massive invasion of privacy. Additionally, the central bank would now be the ultimate honeypot, which we mentioned earlier, and it would become a massive target for hackers who could attempt to steal customer funds. In a world where a majority of dollars are stored through a CBDC, this could have disastrous effects on the economy and national security of the United States. Furthermore, a CBDC can impact the overall financial system and negatively impact existing financial intermediaries. If individuals and businesses can hold accounts with the central bank, this could reduce the role of traditional banks, potentially disrupting lending and destabilizing banks altogether. A CBDC can also increase the risk of bank runs by disintermediating banks. This means that during times of crisis or instability, customers may shift their funds from commercial banks into a CBDC that

they perceive as safe, this could exacerbate liquidity shortages and further destabilize the banking system (Nelson, 2023).

The chances that the United States and the Federal Reserve will move towards creating a Central Bank Digital Currency at any point in the near future seem to be slim to none. While there are certainly advocates for the United States, most notably Senator Warren, the idea has not caught on widely, and even those who are somewhat interested want there to be studies or pilot programs conducted first before rushing into it. There have been several Democratic members of Congress attempting to work a provision into the stablecoin legislation that would direct the Treasury and Federal Reserve to conduct a study on a CBDC, however it seems like this will not go anywhere. That is because a CBDC is essentially a nonstarter for a vast majority of Republican members, who have also passed a bill through committee that would bar the Fed from ever creating one. Additionally, Chairman Jerome Powell has repeatedly stated that the Federal Reserve has no authority to create a CBDC without approval from Congress and will not begin any work on developing one unless approval through legislation is granted (Schroeder, 2024). Finally, currently, no other major central bank across the world has issued a CBDC (Nelson, 2023).

Recommendation

The United States should not create a CBDC and should stay far away from doing so. Due to all of the privacy concerns previously stated, there seems to be no reason to create one in the first place, and its creation would only create more problems than any problems it could solve. The creation of a CBDC would bring about the world that the Cypherpunks were afraid of. The payment services that a CBDC would provide can already be provided through private stablecoins, rendering any benefit for a CBDC

unnecessary. Additionally, a CBDC is not something the American public is asking for, with only 16% saying they support one (Ekins & Gygi, 2023). Reviewing the evidence seems to suggest that a CBDC is a solution in search of a problem.

Senator Elizabeth Warren, the chief proponent of a CBDC, said this in an interview with NBC's Chuck Todd:

> "If the problem you are trying to solve is a fast, almost frictionless ability to send money across the country, do it rapidly, send it around the world. Be able to send it to your cousins in Argentina. You don't need a Bitcoin to do that. So then the question becomes what problem is it solving for?"

This is an apparent misreading of the Cypherpunks and Satoshi. Indeed, low-cost, high-speed transactions that can send payments across the globe are frequently brought up as a feature and use for cryptocurrencies and one of the use cases for something like a stablecoin. However, nowhere in either Eric Hughes's, *Cypherpunk Manifesto*, or Satoshi Nakomato's writings is this brought up as the problem they were trying to solve or the purpose of this innovation. At the heart of the Cypherpunk movement was ensuring that the right to privacy remained in the digital age; for Satoshi, it was building a decentralized financial system that removed third parties and trust from the system. Warren completely ignores the foundation of that problem these developers were trying to solve to focus on the one use case that might also be applicable to a CBDC, when a CBDC is inherently anti-privacy, as centralized as the system can get and requires massive amounts of trust in the central bank. In other words, a CBDC is the exact future the Cypherpunks were working to prevent. It is also evident through Senator Warren's statements and her DAAMLA legislation that she is incredibly against the use of cryptocurrency and would prefer to see Bitcoin eradicated, "A well-designed CBDC

could serve as a public alternative to these cryptocurrencies and potentially crowd out their usage."

CBDC might introduce significant risks to the broader banking system because they can be viewed as safe, and there is no reason to believe that the central bank will not have the dollars on hand. This is because rather than being a claim on a dollar, like a deposit in a checking account at a commercial bank, a CBDC account represents a physical dollar. This less risky nature of a CBDC may make them attractive to people during times of instability, where they may run a bank to move their funds into a CBDC, leading to the disintermediation of banks (Hendrickson, 2022). One study on this potential risk found this:

> "A one-dollar introduction of CBDC replaces bank deposits by around 80 cents on the margin. Bank lending falls by one-fourth of the drop in deposits because banks partially replace lost deposits with wholesale funding. This substitution raises banks' interest-rate risk exposure and lowers their resilience to negative equity shocks. If CBDC bears interest or is intermediated through banks, it captures a greater deposit market share, amplifying the impact on lending. The effect on lending is amplified for small banks, for which wholesale funding is more expensive" (Whited et al., 2022).

However, many advocates of a CBDC have stated that a potential solution would be to offer no or extremely low rates of interest on holding CBDC to disincentive people from turning to them. This represents a massive contradiction, as the claim is that a CBDC is a superior financial product. However, in order to make it stable for the broader financial system, it must be designed so that no one uses it. This is one of many questions about why anyone would use a CBDC. As Senator Warren suggests, a CBDC would eliminate the need for anyone to use Bitcoin, but that does not make sense. The main reason why people invest in or use Bitcoin is because of the decentralized ledger technology and the ability to maintain their financial privacy. Why would any people who use Bitcoin for

this now want to use the exact opposite product in the form of a CBDC? It is also claimed that a CBDC will provide financial services to the unbanked. While it is possible that this may be true for some, the FDIC survey found that the second most cited reason why people remain unbanked is that they do not trust banks (FDIC, 2023). I find it hard to believe that the same people who do not trust banks and resort to hiding money under their mattresses have a vast amount of trust in the federal government or the central bank.

A CBDC also has massive privacy concerns associated with it. Once again placing it at direct odds with what the Cypherpunks were trying to accomplish.

> "The real danger in CBDCs is that there is no limit to the level of control that the government could exert over people if money is purely electronic and provided directly by the government. A CBDC would give federal officials full control over the money going into–and coming out of–every person's account" (Michel, 2022).

A CBDC essentially eliminates any resemblance of financial privacy. In a world where a CBDC is the only option for money and financial services, there is nothing stopping the government from seeing everything you do. It makes freezing the accounts of citizens, similar to what occurred in Canada, incredibly easy. Finally, a CBDC represents the final form of the government taking over the supply and control of money. This stands in opposition to many of the economists' views of the monetary system that we reviewed earlier in the paper and against the history of the development of money.

For all of these reasons, the United States should stay far away from creating a CBDC. A report from the Economic Affairs Committee in the UK Parliament found the same thing, saying that a CBDC did not have answers to the various questions posed and did not provide any particularly valuable use without having significant cost, ultimately

determining that it is a solution in search of a problem (Economic Affairs Committee, 2022). In conclusion, a CBDC is just a bad idea.

Stablecoins

Stablecoin regulation is the area that has seen the most advanced bipartisan discussion between lawmakers. However, there was a major breakdown in July 2023 when, right before a markup on the bill, there was a breakdown in bipartisan talks. This led to a hectic and contentious markup hearing after the White House and Ranking Member of the Financial Services Committee, Maxine Waters (D-CA), backed out of the bipartisan negotiations. The Chairman of the committee, Patrick McHenry (R-NC), decided to move forward with the legislation regardless. The bill H.R. 4766, The Clarify for Payments Stablecoins Act of 2023, passed the Financial Services Committee by a vote of 34-16 with support from all Republicans and five Democrats. While the bill has received no action yet since being reported out of committee, there is still optimism that 2024 will be the year that a consensus is struck on stablecoin legislation. Jeremy Allaire, CEO of stablecoin issuer Circle, said that there is a "very good chance" that a deal is struck, "I think what you're seeing is a desire from the administration, a desire from the Treasury, from the [Federal Reserve], by both chambers of Congress, and certainly on a bipartisan basis" (Browne, 2024).

Clarity for Payment Stablecoins Act

The bill is centered on "payment stablecoins" which is defined as a digital asset which is issued for the use of payments and which the issuer is required to redeem at predetermined fixed amount (Tierno & Scott, 2023). This bill places requirements on issuers designed to protect consumers. The bill requires issuers to hold reserves on a 1:1 basis, meaning for every dollar issued, one must be held in reserve in the form of

acceptable assets. There are also requirements placed on the types of acceptable reserves such as currency, treasury bills, insured funds at banks and central bank deposits. Issuers have capital liquidity requirements placed on them to prevent them from manipulating the reserves except for when needing liquidity to meet redemptions.

Additionally, the bill requires that issuers publicly announce the redemption process and publish monthly reports about their financials, such as outstanding issuance and the composition of their reserves. These reports must also be audited by registered CPAs and the bill contains criminal penalties for issuers knowingly producing false reports (Tierno & Scott, 2023). These requirements create the distinction of "permitted payment stablecoin issuer" that must be approved by regulators in order to issue stablecoins.

This bill makes it clear that payment statements are neither commodities nor securities and that the SEC or the CFTC have no authority over them. The bill actively goes in and makes amendments to four existing securities laws in the U.S. Code to further clarify that they are not securities. The bill also doesn't prohibit stablecoins from offering interest to holders, so issuers may be able to offer interest without violating securities laws. The bill also creates a system for the regulation of these stablecoin institutions that sets up a dual system with a federal and state option for issuers who could be both banks or nonbanks. "Banks and credit unions would be subject to federal regulation, while nonbanks would have the option to be subject to state or federal regulation" (Tierno & Scott, 2023). At the federal level the Federal Reserve would handle oversight and enforcement of bank issuers whereas the Office of the Comptroller of the Currency (OCC) would be the regulator for nonbanks. The bill still, however, treats nonbank issuers with bank-like regulation. "Bank-like requirements include capital,

liquidity, and risk management requirements; application of the Bank Secrecy Act and the Gramm-Leach-Bliley Act's customer privacy requirements; certain activities limits; and broad supervision and enforcement authority" (Polk, 2024). The Federal Reserve also has authority over custodians and wallet providers, who are subject to standard customer protection requirements.

State regulators have a robust role in the framework set by the bill. If an issuer chooses to follow the state path and become a state stablecoin issuer, then generally state regulators have primary enforcement, with the Federal Reserve having secondary authority for what the bill calls "exigent" circumstances, which the Fed would define after the enactment of the law. While the Federal Reserve does not have the primary oversight and enforcement of state issuers, it would be responsible for writing rules for them.

A section of the bill also relates explicitly to the Terra / Luna collapse and its loss of $16 billion in value. The bill places a two-year ban on issuing new algorithmic stablecoins, which the bill refers to as "endogenously collateralized stablecoins". It also directs the U.S. Treasury, in coordination with other federal agencies, to produce a report for Congress on the algorithmic stablecoins and nonpayment stablecoins, including their risks and possible policy options (Tierno & Scott, 2023).

There seems to be broad consensus that the overall approach to this bill is correct. A vast majority of this bill is agreed to by all the major stakeholders. It is also clear that this bill, regardless of minor disagreements, represents a massive step in the right direction for regulating stablecoin in the United States and is certainly better than the status quo. This bill will increase regulatory clarity for everyone involved in the

stablecoin space, allowing for clear rules that might bring more customers and institutional actors off the sidelines. This bill's increased requirements for issuers, including reserve requirements, greatly enhances customer protections. This bill accomplishes the goals of providing clarity, stability, transparency and protection to the stablecoin market.

The main argument against this bill has been related to the division of power between state and federal regulators. Opponents to the bill argue that it does not give the Federal Reserve enough authority over stablecoin regulation, fearing that this will create a "race to the bottom". Congressman Stephen Lynch, who is a Ranking Member of the Digital Asset Subcommittee, said this:

> "A race to the bottom is a practice, is the custom of this industry, you know, to go offshore and seek areas of least regulation. My feeling is that if we directed this to 50 states, and territories perhaps, that that practice would continue and that cryptocurrencies would seek out those area, those jurisdictions, that offer the best opportunity for them to maximize their profit and avoid cumbersome and costly regulation and disclosure"

This viewpoint is not entirely off base; there has been a frequent trend of blockchain companies wanting to escape stricter regulations, as some companies have decided to flee the United States or stop operating in states such as New York that have stricter standards. The primary concern is that the Federal Reserve does not have the authority to reject an application of a state-based issuer that it deems inadequate and has limited enforcement power over those institutions.

These disagreements are truly at the core of what is preventing a bipartisan compromise (Leonardo, 2023). In the Senate, Senators Kirsten Gillibrand (D-NY) and Cynthia Lummis (R-WY), announced in December, 2023 that they would be working on a standalone stablecoin bill separate from their proposal in their broader crypto bill,

Responsible Financial Innovation Act (RFIA). This new proposal will attempt to find a compromise on the federal vs state question with Sen. Gillibrand saying "We think we have a nuanced position that might be the sweet spot". The proposal in the RFIA has many similarities to the Clarity for Payment Stablecoin bill. Many of the requirements, such as the 1:1 reserve requirements, transparency requirements, basic regulations, and making issuers subject to the Bank Secrecy Act, are all the same.

The key difference is that under the RFIA, only "depository institutions" are allowed to issue stablecoins. "Depository institutions" must be approved by the OCC or a state regulator with a "substantially similar State law." These institutions should get permission from both a federal agency and a state agency as well as become a member bank of the Federal Reserve System. This is the other side of the debate to the Clarity for Payment Stablecoins Act, which does not limit issuer to being depository institutions and allows for non bank entities to seek approval. State issuers do not need approval from a federal regulator, do not need to become members of the Federal Reserve System, as the Fed will only serve as a secondary authority. However, these state issuers will still need to comply with some minimum standards set by federal regulators. The "sweet spot" for a compromise could lie in between these two visions of regulation and could be provided by this new Gillibrand-Lummis proposal (Leonardo, 2023).

Recommendation

The *Clarity for Payment Stablecoins Act* should be passed. The framework that is lays out provides the necessary clarity to issuers, sets clear rules of the road that allow them to seek approval through various mechanisms, sets strict requirements and guardrails to ensure that their is proper oversight, stability added to the market, and provides significant customer protections through reserve requirements, liquidity

standards and enhanced transparency. This bill represents a massive leap forward from the current status quo, which has no standards.

It is certainly possible that a compromise could be struck that will still allow a role for state regulators while increasing the responsibility of federal regulators in overseeing stablecoin issuers. If a compromise is reached then it would be wholly adequate as well to handle the challenges. However, the current framework in the *Clarity for Payment Stablecoins Act* is also acceptable. While there are concerns that the Federal Reserve does not have enough authority over state-regulated issuers, these state issuers are still subject to a set of minimum requirements that will provide protections. The concern over a "race to the bottom" does not seem to be as salient when there is a federal minimum and backstop. The concern is that issuers will flee overseas to seek less burdensome requirements, with these standards however, any issuer who does this will not be able to operate in the US. Additionally, with this federal minimum, issuers will have less opportunity to find states with friendly regulations.

Concerns have been raised on a bipartisan basis that the bill would allow giant companies like Amazon or Facebook to issue stablecoin. There are concerns over these massive companies having their own payment systems, essentially consolidating their power and adding to privacy concerns. This concern arises from the fact that this bill does not explicitly ban these types of stablecoin issuers, and the pathway to becoming a qualified issuer would allow nonbank entities. This concern doesn't seem to hold up, however, as Facebook went through their Libra/ Diem project to issue their own token but ended up scrapping the project in 2022 due to all the regulatory scrutiny that was

coming their way, even without any sort of regulatory framework in the first place (Choudhar, 2022).

Stablecoins actually resemble a known financial product as they are just stable value products that are implementing blockchain technology. These types of stable products have been the preference of financial market reforms following the 2008 financial crises that were partly generated by risky and speculative financial products. This means that it is known how to construct a stable regulatory environment for products that resemble stablecoins that does not allow for systemic threat to markets.

Not passing a comprehensive stablecoin bill does not make them go away, other countries around the world have begun to recognize their value and have frameworks for them. This will continue to happen regardless of the United States actions. If the United States does not act, it is possible to see the standard currency of crypto no longer being the dollar. This could have massive national security and economic consequences in the long run for the country if there is a world where the financial system is built on blockchain technology and was developed outside of the United States.

This bill clarifies the regulatory environment surrounding stablecoins. It sets for the necessary operational requirement to protect customers, addresses concerns over the quality of stablecoin issuers reserves and distinctly assigns authority between state and federal regulators. This bill is massively better than the status quo and would prevent any long-term negative consequences from keeping stablecoins outside of the US financial system. Stablecoins represent an innovation to our payment system, allowing for improved cross-border transactions and empowering disadvantaged people with access to digital dollars. Stablecoins also support the position of the US dollar as the reserve

currency in the world and amplify Fed monetary policy. For these reasons, the *Clarity for Payments Stablecoins Act* should be passed, and stablecoins should be incorporated into our financial system.

Illicit Uses

A lot of attention has been paid to the use of cryptocurrencies for illicit or criminal purposes. However, as previously investigated the amount of criminal activity that occurs with cryptocurrencies is minimal and that by far the preference for criminals is to continue to use physical cash. Given this, there is still valid reason to be concerned about the potential use of cryptocurrency for criminal activity, and a multitude of policies have been proposed to curtail it. Some of these proposals have received massive bipartisan support, while others have been viewed as nothing less than attempts to outright ban crypto entirely.

Financial Technology Protection Act

This would create a Financial Technology Working Group to study and work to "combat terrorism and illicit financing", titled the "Independent Financial Technology Working Group to Combat Terrorism and Illicit Financing." The group would consist of representatives from The US Treasury, FinCen, IRS, Office of Foreign Assets Control, DOJ, FBI, DEA, DHS, State Department, CIA, along with members of industry such as financial institutions, blockchain companies and research organizations. The purpose of this group is "conduct research on terrorist and illicit use of new financial technologies including digital assets" and "develop legislative and regulatory proposals". The group would operate for four years and would produce a yearly report to the Secretary of the Treasury detailing any findings and proposals. Additionally, before the termination of the group, they would submit a final report to Congress.

Furthermore, Section 3 of this act is exclusively dedicated to studying digital assets and their potential use by any entity, state or non-state actors "to evade sanctions, finance terrorism, or launder monetary instruments" that would threaten US national security along with ways to mitigate these uses. This bill has received a high amount of support, both bipartisan and bicameral. The bill is sponsored by Senators Ted Budd (R-NC) and Kirsten Gillibrand (D-NY) in the Senate and has also been introduced in the House by Reps. Zach Nunn (R-IA) and Jim Himes (D-CT). In July the bill passed the House Financial Services Committee unanimously and it has passed the House unanimously in both 2018 and 2019.

Combating Money Laundering in Cyber Crime Act

This bill makes minor updates to Section 3056(b) of title 18 in the United States Code to better improve and expand the authority of the US Secret Service when it comes to investigating financial crimes, particularly related to digital assets. These changes were written based on the recommendation of the 2024 National Money Laundering Risk Assessment Report and in coordination with federal authorities. This bill has received bipartisan support and passed the House Financial Services Committee unanimously.

Establishing an Office of Innovation at FinCEN

There has been a discussion in Congress of a piece of legislation that would simply create an Office of Innovation within FinCEN that would be tailored towards finding solutions that deal with financial technology such as digital assets. The office would be required to hold monthly meetings which would be open to the public, specifically members of the industry, who could come and share concerns or ideas with the agency and or showcase what they are doing to better ensure the safety of their

products. This is another relatively bipartisan proposal that is geared towards increasing the amount of cooperation between the government and industry leaders.

Recommendations

These three proposals should all be adopted and implemented and represent a good first step towards addressing concerns over the illicit uses of digital assets. We know things to be true, first that the use of cryptocurrencies for criminal activities is incredibly low, according to Chainalysis numbers, only somewhere between 0.12 percent and 0.24 percent of total crypto transactions are uses for illicit purpose (Chainalysis, 2023) Furthermore, we know that criminal still prefer cash and that the vast majority of financial crime is carried out with cash and will remain that way for the foreseeable future (Butler, 2019). Second, we know that the existing AML regime is one of the most ineffective policies that is implemented by the government (Pol, 2020). These three proposals strike a necessary balance towards working towards real solutions and addressing concerns while not hastily applying ineffective frameworks in a way that can hurt innovation and the broader uses of cryptocurrency. “Overstating crypto’s criminal use and overlooking other applications will not yield sound policy on either front” (Schulp et al., 2023).

Given that the amount of crypto crime is low, policymakers have the time to develop sound policy. This is the approach of the *Financial Technology Protection Act*, which will bring all of the relevant stakeholders together in a working group to produce studies and report on the uses of crypto for illicit means. It will primarily focus on the issues of terrorism financing and evasion of sanctions. This working group will also have the time to develop a set of proposals that might have the potential to be much more

suitable for the technology and more effective. Establishing an Office of Innovation within FinCEN would have a similar effect, bringing together government and industry to work together in a collaborative fashion to find solutions and policies that can actually work. Finally, the *Combating Money Laundering in Cyber Crime Act* is a simple tweak to existing law that will grant the Secret Service the additional tools that it needs to be able to investigate criminals and has been crafted in coordination with all relevant stakeholders.

Crypto-Asset National Security Enhancement and Enforcement (CANSEE) Act

This bill is sponsored by a cohort of bipartisan Senators, Senators Jack Reed (D-RI), Mike Rounds (R-SD), Mark Warner (D-VA) and Mitt Romney (R-UT). While it does have a basis for bipartisan support it has received massive backlash from crypto enthusiasts on the Hill. The overarching purpose of this bill is to apply much of the AML and KYC framework to cryptocurrency.

This bill requires anyone who "controls" either directly or indirectly the code of the blockchain blockchain protocol or "makes available an application to facilitate transactions" to comply with Office of Foreign Asset Control regulations. These individuals are termed "digital asset transaction facilitators" and are given this distinction by the Secretary of the Treasury" If it is deemed that nobody controls the protocol then it will levy penalties on "protocol backers" who is someone with $25,000,000 invested into that protocol. The $25 million total can come from cash, token holdings, or a combination. Additionally these two groups will also have the AML rules from the Bank Secrecy Act applied to them. The Secretary of the Treasury may exempt protocol backers from these requirements if it finds that there is someone who controls it.

Additionally, this bill would allow the Treasury to prohibit any US financial institution from transferring funds to or from another jurisdiction or account if it deems it is of "primary money laundering concern". The bill also contains a provision related to crypto kiosks, which are stand alone ATMs that facilitate crypto transactions. It requires that these kiosks verify users' names and addresses by collecting photo ID. This requirement applies to both parties of a transaction.

Digital Asset Anti-Money Laundering Act (DAAMLA)

The *Digital Asset Anti-Money Laundering Act* is the toughest of the proposals on crypto crime and is being led by its key champion, Senator Elizabeth Warren (D-MA). This bill is the scorn of the crypto industry, labeling it an effective "ban on crypto". This bill also stands virtually zero chance of becoming law as it would be a nonstarter in the current House and also has many other opponents, including Chairman of the Senate Banking Committee, Sherrod Brown. This bill broadly aims to close loopholes and bring the digital asset ecosystem into compliance with the AML, KYK and countering the financing of terrorism frameworks.

The bill expands the definition of money service businesses (MSBs) to include miners, validators, wallet providers and virtually all other blockchain participants that validate or secure transactions. This expanded definition applies the Bank Secrecy Act responsibilities in addition to Know-Your-Customer requirements would be extended to all included actors. The bill also targets what is call "unhosted digital wallets" which is a more pejorative name for self-hosted wallets or self-custody. This bill requires all MSBs and banks to verify the identities of customers and counterparties, keep record and file reports for transactions that contain at least one party who is self-custodying. Another section of DAAMLA requires the Treasury to implement rules which would force

financial institutions, which now includes essentially all participants of the blockchain under this act, to protect against the potential risks of privacy "anonymity-enhancing" technologies and digital assets.

Another massive component of this bill is that it would massively expand the scope of AML/CFT both with regard to digital assets and blockchain companies, but also in regards to all financial institutions. Under this act, the Treasury Department would have to create a process to examine and review all MSBs. Additionally, the SEC and CFTC would be required to establish AML/CFT standards and review all of the entities it regulates for compliance.

The DAAMLA also contains virtually the same policy when it comes to digital assets ATMs / kiosks in regards to verifying customer ID, via government issued ID. Finally, the bill would instruct the DEA to provide recommendations for rulemaking or legislation on how to reduce money laundering and drug trafficking that is being carried out with the use of digital assets.

Recommendations

Both the CANSEE Act and the DAAMLA Act are bad pieces of legislation that represent a massive evasion of financial privacy and fundamentally don't understand the underlying technology of cryptocurrencies. A letter led by the Blockchain Association against these bills amassed over 80 signatories coming from the crypto industry, former government officials, military and intelligence officers and financial crime experts.

"To be clear, the digital asset industry strongly supports U.S. efforts to address illicit activities within the blockchain space. To achieve this effectively, it's crucial for the industry to develop within the United States, governed by domestic laws and regulations. Sen. Warren's DAAMLA legislation, however, would inadvertently hinder law enforcement and national security efforts by driving the majority of the digital asset industry overseas. This shift could also lead to increased liquidity in unregulated offshore

exchanges and a loss of valuable expertise and visibility for the U.S. in the blockchain realm" (Korver et al., 2023).

These bills would drive the development of cryptocurrencies and blockchain companies overseas, effectively eliminating any ability for the United States to monitor them for criminal uses. It would also have disastrous impacts on the overall economic and national security of the United States

As a society, we have agreed that having a free, open internet provides more benefits than harm. This was a decision that was made from the outset of the internet and in the long run it has proven to be correct. There are many bad actors on the internet today, using it for illegal and bad purposes, but imagine all of the benefits that the development of the internet through an open and public process would not have been achieved had the United State government regulated access. We are posed with a similar question today when it comes to blockchain technology: should the government restrict access to the good actors due to the fear of bad actors? (Smith, 2023). We also know that the criminal actors are low, even the Treasury report that proponents of this bill cite for evidence that action is needed emphasizes that "the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods" (Anthony, 2023).

In terms of just the CANSEE Act, it is an overly broad, poorly written piece of legislation. The bill attempts to get around the fact that there are no third parties in a decentralized blockchain by instituting the term "control"; however they define control as essentially anything that the Treasury department deems to be. This grants the Treasury Department way too much power and authority to enact enormous requirements on essentially anybody. Furthermore, the definition of "digital asset transaction facilitator"

in the act can apply to anybody who develops software code. This means that someone can design a software that is later used by someone for a criminal purpose, and the designer will be held criminally liable, which is a violation of the First Amendment in which courts have consistently found the computer code is an expression of speech (Anthony, 2023). Finally, the definition of "crypto kiosks" is incredibly broad that it can easily apply to any individual who has downloaded a crypto wallet onto their phone. That means these users may be subject to the same requirements to verify ID every time they transact with someone (Anthony, 2023).

DAAMLA suffers from many of the flaws of CANSEE in that it does not understand the technology or how something like Bitcoin works. It would designate miners and people who just use cryptocurrency software as "financial institutions," subjecting them to the same requirements of AML and KYC that are placed upon banks. This fundamentally does not make sense. It would essentially end the ability of people to mine and use Bitcoin in the United States. However, the Bitcoin network would not go away; it is global and would continue to operate without the influence of the United States, solving none of the international problems that this bill claims to want to address.

Furthermore, this bill takes a direct shot at limiting the ability to maintain an "unhosted wallet." This is another term for self-custodying your digital assets, which essentially means that you own your own property. This is the equivalent of saying that people aren't allowed to own physical cash and that all of their dollars must be held at some form of a financial institution. This represents a massive breach of financial privacy and property rights.

Both CANSEE and DAAMLA would subject decentralized ledger technology to the requirement of the Bank Secrecy Act. This would completely undermine the entire purpose of the innovation in the first place. These technologies are built on privacy and decentralization and this policy would turn them into something that resemble much more traditional financial intermediaries. This is the exact thing that the Cypherpunks and Satsoshi were working to get rid of in their new decentralized financial system and it is another example of how they are being proven right. These bills would be wholly ineffective and represent the wrong approach to dealing with these issues, "Should cybercriminals successfully tempt the United States to abandon the human right to privacy and the U.S. Constitution, everyone will lose" (Anthony, 2023).

Energy and Commerce Committee (E&C) and FTC Proposals

When it comes to the regulation of digital assets and crypto, most of the attention has been placed upon the financial regulators. However, the Energy and Commerce has been working in a bipartisan fashion to proactively expand the Department of Commerce and the FTC's role in both crypto tokenization and blockchain technology broadly. The committee has held several hearings on "Web3" and the potential proliferation of blockchain technology throughout the internet and the economy. In December, 2023 the E&C Committee passed their first two blockchain bills out of committee, both unanimously.

Deploying American Blockchains Act

This bill places the Secretary of Commerce as the chief advisor to the President when it comes to blockchain policy and calls upon the Secretary to promote the development, use and competitiveness of blockchain in the United States. The bill specifies certain actions the Secretary of Commerce should take. This includes creating a

"Blockchain Deployment Program", developing a set of best practices to support blockchain operations, reduce cyber risk and quantify the potential value of building apps on blockchain. They should also examine how federal agencies benefit from blockchain technology. Two key uses highlighted were fortifying supply chains and protecting against cyber attacks. Additionally, the Secretary should develop policies for utilizing blockchains for decentralized ID, AI, e-commerce and healthcare. Finally, this bill also calls for a report from the Department of Commerce, which would recommend legislation to strengthen US competitiveness and describe emerging risks and trends in blockchain, including apps and tokenization.

Consumer Safety Technology Act

This bill is specifically tailored toward increasing the role of the FTC in exploring and regulating blockchain technology and digital tokens. It directs the FTC to study the "current and potential use of blockchain technology in commerce and the potential benefits of blockchain technology for limiting fraud and other unfair or deceptive acts or practices." The FTC should provide a report to Congress that contains recommendations that would better allow the FTC to protect consumers from deceptive and fraudulent practices and "promote competition and innovation in the global digital token sector." The bill's language also included several explicitly pro-crypto sentiments, stating that the US must remain a leader in innovation and blockchain technology is a leader of innovation. The bill also highlighted the fact that digital assets and blockchains are only becoming more common and there is a need to have our federal agencies ahead of this trend.

Recommendations

These are both good bills that represent a proactive approach to regulation that was missing from financial regulators when it came to the onset of cryptocurrencies. These broader uses of blockchain technology are currently more of hypothetical rather than realities and it is certainly possible that perhaps blockchain can be as revolutionary as the advent of the internet. It is also possible that it won't be. However, it makes sense for the government and federal regulators to take a proactive approach to investigate potential uses, risks, and possible policies to implement rather than waiting to be reactive after the fact.

In particular, the *Consumer Safety Technology Act* is a significant development for consumer safety. The FTC is responsible for protecting consumers from bad business practice. There have been a plethora of blockchain projects that operate much more similar to this and have implemented manipulative or deceptive marketing schemes. Placing the FTC in a better position to respond to this is necessary. One form of digital assets that seem to fit much better under the regulation of the FTC would be NFTs. However, if we are to accept the argument that at least some cryptocurrencies are more akin to collectibles than they are to either securities or commodities, this necessarily means that the FTC needs to increase their oversight of these markets.

Other Proposals

Taxation

The debate surrounding the taxation of digital assets and what a taxing regime could like is incredibly complex. It is also an issue that has seemingly been placed on the backburner compared to focusing on the financial regulators. However, the issue is only going to continue to become more important as the trend of people using cryptocurrency increases. It is also clear that the current taxing structure could be more efficient. The

approach of the IRS to make rules based on existing tax rules is not working. Their proposals have been missing the mark and drawing massive amounts of baclask from the public with a recent proposal amassing over 100,000 public comments (Hamilton, 2023). There has also been an overemphasis on preventing tax evasion over making a functional tax regime that serves the needs of the vast majority of people who use digital assets. The reporting and tracking requirements are also incredibly burdensome for a user, making compliance incredibly challenging. It is only further complicated by the constant changing of requirements (Smith, 2023). There are two things that Congress can do right now. While not establishing a full tax regime, it will provide significant fixes and be a huge step in the right direction.

First, create a working group to study digital asset taxation and potential policies. This is very similar to the *Financial Technology Protection Act* and its approach to tackling illicit uses. Creating a group of all the important stakeholders from various positions in government, research organizations, large crypto companies and the general public will allow the tax debate to move forward in a much more efficient and productive way than the current approach.

There is also a very simple legislative tweak that Congress can approve that would massively ease the burden on people who use cryptocurrencies for transactions. This would be instituting a De Minimis Exemption for personal crypto transactions. This would be creating an exemption from taxes for small everyday transactions involving cryptocurrencies. Under the current rules, a user must track, record, and report even the smallest transactions for taxation. This is incredibly complicated and burdensome. The government already implements this type of exemption for foreign currency transactions,

because due to exchange rates between currencies you may receive a small gain (Agrawal, 2023). There is already a proposal in Congress, *The Virtual Currency Tax Fairness Act*, which would create a $200 de minimis exemption for cryptocurrency transactions. This proposal is also included in the larger *Responsible Financial Innovation Act*.

Keep Your Coins Act

The *Keep Your Coins Act* (H.R., 4841) is a piece of legislation designed to protect the rights of individuals to use cryptocurrencies. The bill prohibits the federal government from preventing users from using virtual currency for purchases of goods and services. Additionally, it prohibits the federal government from restricting users' ability to self-custody their digital assets or use self-hosted wallets. The bill is sponsored by Rep. Warren Davidson (R-OH) and did not receive bipartisan support when it passed the House Financial Services Committee by a vote of 29-21 in July, 2023.

This bill is a must pass piece of legislation for anyone who believes in the promise of Bitcoin and the Cypherpunks. The ability to self-custody or self-host your own tokens is not only just allowing people to have control over their property; it is the fundamental tenet of cryptocurrency. What it means to be a self-custodian is that you are in control of your own tokens and the only one who can access the private keys to your assets. It is the functional equivalent of saying that people have the right to keep some or all of their money in the form of physical cash in their wallets. The ability to self-wallet is a major contributor to what makes Bitcoin and other digital assets decentralized, because there does not have to be a third party that holds everyone's assets. This is also what makes them private, allowing for uncensored transactions. This bill was created in direct response to the Canadian government freezing peoples bank accounts and calling on

crypto custodians to freeze users accounts. It is the ability to be your own custodian that prevents those types of actions from the government and is at the core of what Satoshi and the Cypherpunks were working to create.

The opponents to this bill are people who do not believe in the promise of Bitcoin, allowing individuals to maintain their financial privacy, create a decentralized financial system and allow for a form of digital cash that is free from censorship. Rep. Brad Sherman said in opposition that this bill allows people to "hide their identity" and that they are doing so because they want to engage in illicit activities with crypto. It has already been covered all the multitude of reasons why someone might not want their money stored on a centralized server, fear or theft or fear of censorship of these transactions. Sherman is essentially arguing against the presence of cash in our society and against the right to privacy. Rep. Bill Foster has said that we should not allow self-custody without them having federal identities tied to them (Foster, 2023). This defeats the entire purpose of self-custodying in the first place and is just a precursor to the government being able to monitor individuals' transactions and put an end to them if they would like too.

Blockchain Regulatory Certainty Act

This bill is designed to provide clarity to blockchain participants by making it clear that certain developers and providers who never have control over consumer funds are exempt from financial reporting and licensing requirements. The bill exempts noncustodial blockchain providers and developers, such as miners, nodes, and wallet providers, from being deemed money transmitters under state or federal law. The bill is sponsored by Rep. Tom Emmer (R-MN) and Rep. Darren Soto (D-FL). Despite the

bipartisan sponsorship, the bill did not receive bipartisan support in its vote in the Financial Services Committee where it was passed by a vote of 29-21.

This is another good piece of legislation as it just ensures that something like a Bitcoin miner is treated in the nature of what they are doing. Miners on the blockchain are not money transmitters because they are not an intermediary taking control of funds to facilitate a transaction. They are a group of users who compete for the right to write the peer-to-peer transactions into the decentralized ledger when it is then verified by all the blockchain participants. These miners never have access to the private keys that go to the coins that are being transacted between the two parties.

CHAPTER IX: CONCLUSION

A study of the history of cryptography and the cypherpunk movement showcases that Bitcoin is not a fad. There is a wrong assumption that Bitcoin was just randomly created one day out of thin air, but history shows that this is not the case. Bitcoin represented the culmination of decades of work. The lineage of Bitcoin can be traced to the Diffie-Hellman key exchange in 1976, to David Chaum in the 1980s and the Cypherpunks in the 1990s, through Hal Finney's Reusable Proof of Work, Adam Back's Hashcash and other early attempts, and finally Satoshi Nakamoto's revolutionary white paper. Bitcoin is a legitimate innovation, it is built on sound computer science and sound economics. The blockchain technology and proof of work system in Bitcoin solved not only the problems the early attempts at digital currency faced, but it also revolutionized how we can view a private commodity money. Throughout human history, private commodity money was the overarching norm, but in each instance you had to trust the issuer. The invention of Bitcoin removed the problem of the issuer, making private commodity money even more accessible. The study of the history of the cryptocurrency market also reveals that Bitcoin is here to stay. The price pattern of Bitcoin can be called the "Bitcoin Cycle." The price of Bitcoin has gone through a series of peaks and valleys, yet every single peak has been higher than the last and every valley is also higher than the last. This seems to indicate that Bitcoin has staying power amongst the financial system. Bitcoin has also been the driving force behind this rise, either due to increased acceptance of it as a form of payment, inflation in fiat currency causing a demand for a sound

commodity money, or increased institutional support through something like the approval of Bitcoin ETFs. Yet, virtually every time the price of Bitcoin has crashed it has been unrelated to the underlying technology of Bitcoin and rather associated with the broader crypto industry. For example, in 2014 the collapse of the Mt.Gox exchange caused volatility, in 2018 the ICO bubble burst tanking the market and finally in 2022 the FTX disaster.

Bitcoin was born out of the desire to bring privacy to the digital age. This was the problem that the Cypherpunks were most concerned with. They wanted to construct a form of digital currency that would protect people's financial privacy and serve as a form of digital cash in a society that was becoming increasingly cashless. Bitcoin represented the solution to these problems through a private/public key pairing that could protect users' identities. Satoshi also wanted to revolutionize the financial system removing the need to trust anyone in the system. Bitcoin does this by creating a peer-to-peer transaction system which removes the need of a middleman or financial intermediary to process transactions. Bitcoin also serves as a refuge from inflation that can be caused by the bad monetary policy of central banks that has led to inflation. There are also ample reasons why these applications represent legitimate use cases and provide value to users. Whether it be fear of having your information stolen from the centralized databases that financial institutions keep or from the predation of the government attempting to spy on or even censor your transactions.

Bitcoin and the concept of cryptocurrencies are also economically sound. The origins for the idea of a competing system of private currencies can be seen during the period of Free Banking in the United States. Ever since the US government switched

away from the gold standard and toward a fiat currency with the government having a monopoly on the supply of money, monetary economists have asked if this is the best path forward. Milton Friedman wrote that leaving monetary policy up to Central Bankers alone could be a grave mistake and that a system of predictable monetary policy based on computers would be preferred. Some could argue that Bitcoin and its issuance schedule can represent this concept. Benjamin Klien wrote that a system of competing private monies would be stable as long as they could prevent counterfeiting and cryptocurrencies are virtually impossible to counterfeit. Finally, F.A Hayek was a harsh critic of the government having a monopoly on money and advocated for a system where private money issuers competed in a market. The proliferation of cryptocurrencies in our financial system can represent this "Hayekian escape" as they all compete with each other, offering a variety of different uses or benefits and customers are able to decide which provides them the most value.

As Bitcoin has become more popular amongst the mainstream there has been a significant shift in the broader crypto market place. What started as a group of activists who were focused on privacy concerns in the digital age or by genuine innovators who wanted to create a better financial system, has turned into an entirely different concept that pushes a get rich quick scheme. The broader "crypto" industry has been rotten with fraud from the collapse of the Terra stablecoin, the fall of Celsius, the ICO boom, or the fiasco that was FTX. This has resulted in trillions of dollars lost. The crypto industry has morphed itself into a Silicon Valley adjacent with many blockchain and crypto projects closely resembling tech firms. They have sought massive investment from venture

capitalists and have pushed ideas that don't entirely make sense. This has resulted in the promise and purpose of the Cypherpunks and Satoshi being lost in the shuffle.

Much of the problems that have been associated with cryptocurrencies have been allowed to fester due to the lack of regulation and the incompetence of federal regulators. The current regulatory regime highlighted by the "regulation by enforcement" method of the Securities and Exchange Commission has resulted in an utter lack of transparency in the market. There has not been clear guidance given on what tokens represent a security and which tokens represent a commodity. This has led to confusion for all parties involved, crypto companies, regulators and investors. The current lack of a regulatory framework for digital assets is wholly inadequate and it is time for Congress to take action to fill the regulatory gaps that have emerged.

There have been a wide variety of legislative proposals dealing with digital asset policy across an array of issues. Beginning with market structure legislation or the distinction between security and commodity. The *Financial Innovation and Technology for the 21st Century Act (FIT Act)* is the most promising piece of legislation on thai front and represents a remarkable improvement in the status quo. The legislation provides clear rules to the road offering a set of criteria that if a digital asset is "decentralized" and "functional" it will be deemed a commodity. The proposal also provides the CFTC with the additional authority that it needs in order to adequately regulate the digital asset spot market and requires crypto businesses such as exchanges to register with the regulator. There are also significant requirements placed on crypto companies which will increase the overall transparency and oversight of the market and include significant customer protections. The bill however is not perfect, the criteria for "decentralized" is far too

broad encompassing tokens that are most likely not significantly decentralized. The bill also lacks a hybrid asset distinction that may be needed in order for the SEC and CFTC to share regulatory authority over digital assets that share aspects of both securities and commodities.

The United States should not create a central bank digital currency as it is a solution in search of a problem. It is not clear what the use case for a CBDC is or exactly who would want to use it. CBDCs represent a significant concern for financial privacy and also provide a significant risk to the banking sector through disintermediation of banks. The only use case for a CBDC, the ability to send money across borders easily, can already be provided with private stablecoins. That is why Congress should pass the *Clarity for Payment Stablecoins Act* which would fully regulate the stablecoin market.

There has been a lot of talk about the potential for bad or criminal actors to take advantage of the anonymity provided by cryptocurrencies for illicit uses. However, the data indicates that this is not a widespread concern. Additionally, it seems clear that in the eyes of criminals physical cash is still far superior than a cryptocurrency because crypto is not a perfect substitute for cash. Furthermore, most of the proposed policies surround limiting the illicit uses of cryptocurrencies, The *DAAMLA Act or CANSEE Act*, has been expand the existing AML frameworks to digital assets. The existing AML regulations are incredibly ineffective and costly.

In conclusion, Bitcoin represented a legitimate innovation that was able to solve the problems that early Cypherpunks were attempting to solve as they aimed to create a digital form of cash. In the years following Bitcoin many good faith innovators have attempted to expand upon the promise of Bitcoin to build a better financial system.

However, due to the success of Bitcoin and other cryptocurrencies a variety of bad actors have entered the market. The rise of scams in the market and the inability of regulators to effectively handle the situation has showcased that it is time for Congress to take action to finally create a regulatory framework surrounding cryptocurrency.

REFERENCES

Abrams, R., & Popper, N. (2014, March 4). *Trading site failure stirs ire and hope for bitcoin*. DealBook. https://archive.nytimes.com/dealbook.nytimes.com/2014/02/25/trading-site-failure-stirs-ire-and-hope-for-bitcoin/?_php=true&_type=blogs&_r=0

Agrawal, N. (2023, October 2). A simple legislative fix to complicated tax rules for personal cryptocurrency transactions. *Coin Center*. https://www.coincenter.org/a-simple-legislative-fix-to-complicated-tax-rules-for-personal-cryptocurrency-transactions/

Ahlstrand, G. (2023, May 11). Elizabeth Warren Calls for US to Create a CBDC. *Coindesk.* https://www.coindesk.com/policy/2022/04/01/elizabeth-warren-calls-for-us-to-create-a-cbdc/

Allaire, J. (2024, March 21). Payment Stablecoins Support the Dollar & U.S. Economic Competitiveness. *Circle*. https://www.circle.com/executiveinsights/payment-stablecoins-support-the-dollar-and-u.s.-economic-competitiveness

Anthony, N. (2023a, May). *The Right to Financial Privacy*. CATO Institute. https://www.cato.org/policy-analysis/right-financial-privacy

Anthony, N. (2023b, July 25). *More Senators Target Financial Privacy with "CANSEE Act."* CATO Institute. https://www.cato.org/blog/more-senators-target-financial-privacy-cansee-act

Anthony, N. (2024, January 3). *The Right to a Self-Hosted Wallet? Crypto Laws Congress Should Pass in 2024*. CATO Institute. https://www.cato.org/commentary/right-self-hosted-wallet-crypto-laws-congress-should-pass-2024

Arthur, C. (2020, April 16). PlayStation Network: hackers claim to have 2.2m credit cards. *The Guardian*. https://www.theguardian.com/technology/blog/2011/apr/29/playstation-network-hackers-credit-cards

Ashford, K. (2023, February 16). What is cryptocurrency? *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/

Ashmore, D. (2022a, August 17). An introduction to stablecoins. *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/stablecoins/

Ashmore, D. (2022b, October 11). Bitcoin price history 2009 to 2022. *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-price-history/

Aswal, P. (2024, March 15). *What are Blockchain nodes? Detailed Guide [UPDATED] - Blockchain Council*. Blockchain Council. https://www.blockchain-council.org/blockchain/blockchain-nodes/#:~:text=In%20virtual%20money%2C%20however%2C%20a,laptops%2C%20and%20a%20file%20server

Atlantic Council. (2024, February 9). *Cryptocurrency Regulation Tracker - Atlantic Council*. https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker/

Auxier, B., Raine, L., Anderson, M., Perrin, A., & Turner, E. (2019, November 15). *Americans and Privacy in 2019 - concerned, confused and feeling lack of control over their personal*

information | Pew Research Center. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Back, A. (2002). *Hashcash- A Denial of Service Counter-Measure*. http://www.hashcash.org/papers/hashcash.pdf

Barefoot, J. A. (2020). *Digitizing Financial Regulation: Regtech As A Solution for Regulatory Inefficiency and Ineffectiveness*. Harvard. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_150_final.pdf

Baydakova, A. (2023, June 6). Gary Gensler's Evolving Position on Crypto – in Quotes. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/06/06/gary-genslers-evolving-position-on-crypto-in-quotes/

BBC News. (2014, February 28). MtGox bitcoin exchange files for bankruptcy. *BBC News*. https://www.bbc.com/news/technology-25233230

BBC News. (2022, February 15). Trudeau vows to freeze anti-mandate protesters' bank accounts. *BBC*. https://www.bbc.com/news/world-us-canada-60383385

Best, R. D. (2024a, January 9). *Number of cryptocurrencies 2013-2024 | Statista*. Statista. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Best, R. D. (2024b, January 29). *Bitcoin market cap 2013-2024 | Statista*. Statista. https://www.statista.com/statistics/377382/bitcoin-market-capitalization/

Best, R. D. (2024c, March 26). *Crypto market cap 2010-2024 | Statista*. Statista. https://www.statista.com/statistics/730876/cryptocurrency-maket-value/

Blockchain Regulatory Certainty Act. (2022). Congress. https://www.congress.gov/bill/118th-congress/house-bill/1747/text

Blumenfeld, M., & Talvitie, L. (2023). *PWC Global Crypto Regulation Report 2023*. PWC. https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf

Borden, M. (2023, July 25). U.S. Congressional Leaders Introduce Two Landmark Bills to Create a Digital Assets Regulatory Scheme. *Insights | Sidley Austin LLP*. https://www.sidley.com/en/insights/newsupdates/2023/07/us-congressional-leaders-introduce-two-landmark-bills-to-create-a-digital-assets-regulatory-scheme

Bosker, B. (2013, April 17). Gavin Andresen, bitcoin architect: Meet the man bringing you bitcoin (And getting paid in it). *HuffPost*. https://www.huffpost.com/entry/gavin-andresen-bitcoin_n_3093316

Brady, E. (2023, July 28). *Statement on Digital Asset Anti-Money Laundering Act*. The Digital Chamber. https://digitalchamber.org/statement-on-digital-asset-aml-act/

Browne, R. (2024, January 15). "Very good chance" that U.S. passes stablecoin laws this year, Circle CEO says. *CNBC*. https://www.cnbc.com/2024/01/15/good-chance-us-passes-stablecoin-laws-this-year-circle-ceo-says.html#:~:text=Circle%20CEO%20Jeremy%20Allaire%20said,for%20the%20most%20part%20unregulated

Bryan, B. M. (2013, November). *The Great Inflation*. Federal Reserve History. https://www.federalreservehistory.org/essays/great-inflation

Buchwald, E. (2023). *As PacWest shares dive, are we seeing the 2008 financial crisis all over again?* CNN. https://www.cnn.com/2023/05/11/business/2008-banking-crisis-comparison/index.html#:~:text=Banks%20failed%20in%202008%20because,pay%20it%20back%20on%20time

Buterin, V. (2014). *Ethereum Whitepaper | Ethereum.org*. ethereum.org. https://ethereum.org/en/whitepaper/

Butler, S. (2019). *Criminal use of cryptocurrencies – a great new threat or is cash still king?* Royal Holloway. https://pure.royalholloway.ac.uk/ws/files/42792707/Accepted_Manuscript.pdf

Campbell, A. (2023, July 31). Pass the Stablecoin Bill Now. *Coindesk.* https://www.coindesk.com/consensus-magazine/2023/07/31/pass-the-stablecoin-bill-now/

Carbone, C. (2024, February 20). *Cryptocurrency under threat: Urgent call to stop Senate bill banning crypto*. The Digital Chamber. https://digitalchamber.org/cryptocurrency-under-threat-urgent-call-to-stop-senate-bill-banning-crypto/

Casey, M. (2023, September 28). Crypto Industry Needs More FTC, Less SEC. *Coindesk.* https://www.coindesk.com/consensus-magazine/2023/02/24/crypto-lobbying-needs-a-reset-more-ftc-less-sec/

Chainanalysis. (2023a, July 12). *Crypto Crime mid-year update: Crime down 65% overall, but ransomware headed for huge year thanks to return of big game hunting*. Chainalysis. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/#:~:text=Inflows%20to%20illicit%20addresses%20are,%241.0%20billion%20on%20the%20year

Chainanalysis. (2023b, August 17). *24% of new tokens launched in 2022 bear On-Chain characteristics of pump and dump schemes*. Chainalysis. https://www.chainalysis.com/blog/2022-crypto-pump-and-dump-schemes/

Chamanara, S., Ghaffarizadeh, S. A., & Madani, K. (2023). The environmental footprint of Bitcoin mining across the globe: call for urgent action. *Earth's Future*, *11*(10). https://doi.org/10.1029/2023ef003871

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044. https://doi.org/10.1145/4372.4373

Chaum, D. L. (1983). Blind signatures for untraceable payments. In *Springer eBooks* (pp. 199–203). https://doi.org/10.1007/978-1-4757-0602-4_18

Chervinsky, J. & Blockchain Association. (2023). Understanding stablecoins' role in payments and the need for legislation. In *United States House of Representatives Committee on Financial Services Subcommittee on Digital Assets, Financial Technology and Inclusion* (p. 2) [Report]. https://docs.house.gov/meetings/BA/BA21/20230419/115753/HHRG-118-BA21-Wstate-ChervinskyJ-20230419.pdf

Chilson, N. (2018, March 16). *It's time for a FTC Blockchain Working Group*. Federal Trade Commission. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2018/03/its-time-ftc-blockchain-working-group

Choudhar, V. (2022, January 27). *Zuckerberg's Facebook Dropping Plans to Have its Own Currency*. The Street. https://www.thestreet.com/crypto/investing/facebook-about-to-abandon-diem-it-could-be-a-death-kiss-for-stablecoins

Cointelegraph. (n.d.). *History of ETH: The rise of the Ethereum blockchain*. https://cointelegraph.com/learn/history-of-ethereum-blockchain

Combating Money Laundering in Cyber Crime Act. (2024). Congress. https://www.congress.gov/bill/118th-congress/house-bill/7156/text

Consensys. (2018). *The Decade in Blockchain — 2010 to 2020 in review | Consensys*. https://consensys.io/blog/the-decade-in-blockchain-2010-to-2020-in-review

Consumer prices up 9.1 percent over the year ended June 2022, largest increase in 40 years. (2022, July). https://www.bls.gov/opub/ted/2022/consumer-prices-up-9-1-percent-over-the-year-ended-june-2022-largest-increase-in-40-years.htm#:~:text=FONT%20SIZE%3A%20PRINT%3A-,Consumer%20prices%20up%209.1%20percent%20over%20the%20year%20ended%20June,largest%20increase%20in%2040%20years

Conti, R. (2023, March 17). What is an NFT? Non-Fungible tokens explained. *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

Cross, J., Hou, C., & Trinh, K. (2021). Returns, volatility and the cryptocurrency bubble of 2017–18. *Economic Modelling*, *104*, 105643. https://doi.org/10.1016/j.econmod.2021.105643

Cryptopedia. (2021, December 2). *Crypto regulations in New York*. Gemini. https://www.gemini.com/cryptopedia/new-york-cryptocurrency-regulations

Cryptopedia. (2023). *The DAO: What was the DAO hack? | Gemini*. Gemini. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

Dai, S. N. W. (2017, September 14). *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails*. https://gwern.net/doc/bitcoin/2008-nakamoto#section

Dale, B. (2023a, March 6). *The few crypto firms that have registered with the SEC*. Axios. https://www.axios.com/2023/03/06/crypto-register-sec-securities-exchange-commission

Dale, B. (2023b, November 15). *New York releases new rules for crypto exchange listings*. Axios. https://www.axios.com/2023/11/15/cryptocurrency-new-york-exchange-listing-nydfs

De, N. (2024, March 8). SEC Chair Gary Gensler: "Far Too Many Frauds and Bankruptcies." *Coindesk*. https://www.coindesk.com/policy/2023/12/22/sec-chair-gary-gensler-far-too-many-frauds-and-bankruptcies/

Dewey, J. N., & Patel, S. (2023, October 30). *Blockchain & Cryptocurrency Laws and Regulations 2024 | USA*. GLI - Global Legal Insights - International Legal Business Solutions. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/tit.1976.1055638

Disparte, D. & Circle. (2023). Understanding stablecoins' role in payments and the need for legislation. In *United States House Committee on Financial Services, Subcommittee on Digital Assets, Financial Technology and Inclusion*. https://docs.house.gov/meetings/BA/BA21/20230419/115753/HHRG-118-BA21-Wstate-DisparteD-20230419.pdf

Dowlat, S., & Hodapp, M. (2018). *CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION*. Satis Research Group. https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

Duggan, W. (2023, June 30). How does the SEC regulate crypto? *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/sec-crypto-regulation/

Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. In *Springer eBooks* (pp. 139–147). https://doi.org/10.1007/3-540-48071-4_10

Economic Affairs Committee. (2022, January 13). *Central bank digital currencies: a solution in search of a problem?* UK Parliament. https://committees.parliament.uk/committee/175/economic-affairs-

committee/news/160221/central-bank-digital-currencies-a-solution-in-search-of-a-problem-report-published/
Ekins, E., & Gygi, J. (2023, May 31). *Only 16% of Americans Support the Government Issuing a Central Bank Digital Currency*. CATO Institute. https://www.cato.org/survey-reports/poll-only-16-americans-support-government-issuing-central-bank-digital-currency
FDIC. (2023, July 24). *2021 FDIC National Survey of Unbanked and Underbanked Households*. Federal Deposit Insurance Corporation. https://www.fdic.gov/analysis/household-survey/index.html
Federal Deposit Insurance Corporation. (1996). *The Banking Crises of the 1980s and Early 1990s: Summary and Implications*. FDIC. https://www.fdic.gov/bank/historical/history/3_85.pdf
Financial Innovation and Technolgoy for the 21s Century Act. (2023, July 20). House of Representatives. https://www.congress.gov/bill/118th-congress/house-bill/4763/text?s=1&r=1&q=%7B%22search%22%3A%5B%22Financial+Innovation+and+Technology+for+the+21st+Century+Act.%22%5D%7D
Financial Services and Agriculture Committee. (2023a). *The Future of Digital Assets: Closing the Regulatory Gaps in the Digital Asset Ecosystem*. https://docs.house.gov/meetings/BA/BA21/20230510/115885/HHRG-118-BA21-20230510-SD002.pdf
Financial Services and Agriculture Committee. (2023b). *FIT for the 21st Century Act Section by Section*. https://agriculture.house.gov/uploadedfiles/market_structure_bill_section_by_section.pdf
Financial Services Committee. (2023a). *The Future of Digital Assets: Identifying the Regulatory Gaps in Digital Asset Market Structure*. https://docs.house.gov/meetings/BA/BA21/20230427/115821/HHRG-118-BA21-20230427-SD008.pdf
Financial Services Committee, M. S. (2023b). *MEMORANDUM*. https://docs.house.gov/meetings/BA/BA21/20230419/115753/HHRG-118-BA21-20230419-SD002.pdf
Foster, B. (2023, June 22). *Democratic Rep says Self-Custody wallets should have federal digital identities | Congressman Bill Foster*. Congressman Bill Foster. https://foster.house.gov/media/in-the-news/democratic-rep-says-self-custody-wallets-should-have-federal-digital-identities
Friedman, M. (1962). VIII SHOULD THERE BE AN INDEPENDENT MONETARY AUTHORITY? In *Harvard University Press eBooks* (pp. 219–243). https://doi.org/10.4159/harvard.9780674434813.c9
Gensler, G. (2021, September 13). Even if a Thousand Projects Don't Make It, Blockchain Is Still a Change Catalyst. *Coindesk*. https://www.coindesk.com/tech/2019/12/15/even-if-a-thousand-projects-dont-make-it-blockchain-is-still-a-change-catalyst/
Gensler, G. (2022, April 4). *Prepared remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference*. Securities and Exchange Commission. https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422
Gilbert, J., & Quigley, J. (2023, March 28). *What is Proof-of-Stake (POS)? The investor's guide*. Blockworks. https://blockworks.co/news/proof-of-stake-investors-guide

Grewal, P. (2023, March 22). *We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead*. Coinbase. https://www.coinbase.com/blog/we-asked-the-sec-for-reasonable-crypto-rules-for-americans-we-got-legal

Griffin, A. (2019, September 4). Bitcoin price latest: Cryptocurrency plunges as traders in South Korea forced to identify themselves | The Independent. *The Independent*. https://www.independent.co.uk/tech/bitcoin-latest-price-value-south-korea-regulation-a8173506.html

Grobys, K. (2020, December 6). Did you fall for it? 13 ICO scams that fooled thousands. *Cointelegraph*. https://cointelegraph.com/news/did-you-fall-for-it-13-ico-scams-that-fooled-thousands

Hamilton, J. (2023a, March 29). U.S. CFTC Chief Behnam Reinforces View of Ether as Commodity. *Coindesk*. https://www.coindesk.com/policy/2023/03/28/us-cftc-chief-behnam-reinforces-view-of-ether-as-commodity/

Hamilton, J. (2023b, August 9). Fed Starts New Program to Oversee Crypto Activity in U.S. Banks. *Coindesk*. https://www.coindesk.com/policy/2023/08/08/fed-starts-new-program-to-oversee-crypto-activity-in-us-banks/#:~:text=The%20U.S.%20Federal%20Reserve%20is,any%20rules%20for%20crypto%20banking

Hamilton, J. (2023c, November 15). IRS "Raided" by Crypto Investors as Industry Puts Up Fight Against U.S. Tax Proposal. *Coindesk*. https://www.coindesk.com/policy/2023/11/13/irs-raided-by-crypto-investors-as-industry-puts-up-fight-against-us-tax-proposal/

Hamilton, J., & Schickler, J. (2023, July 28). U.S. Stablecoin Bill Takes Big Step Despite Fight From Democrats, White House. *Coindesk*. https://www.coindesk.com/policy/2023/07/28/us-stablecoin-bill-takes-big-step-despite-fight-from-democrats-white-house/

Hayek, F. A. (1976). *Denationalisation of money: An Analysis of the Theory and Practice of Concurrent Currencies*. Ludwig von Mises Institute.

Hayek, F. A., & Von Hayek, F. A. (1976). *Choice in currency: A Way to Stop Inflation*. Ludwig von Mises Institute.

Hendrickson, J. (2022a, May 12). When a dollar isn't a dollar. *Economic Forces*. https://www.economicforces.xyz/p/when-a-dollar-isnt-a-dollar

Hendrickson, J. (2022b, October 20). Who is going to use CBDCs? *National Review*. https://www.nationalreview.com/2022/10/who-is-going-to-use-cbdcs/

Hendrickson, J. (2022c, November 10). What is an FTX? *Economic Forces*. https://www.economicforces.xyz/p/what-is-an-ftx

Hendrickson, J. (2022d, November 21). *Opinion | How Bitcoin is being ruined by scammy crypto scandals like FTX*. NBC News. https://www.nbcnews.com/think/opinion/bitcoin-vs-ftx-crypto-king-sam-bankman-fried-problem-rcna57964

Hendrickson, J. (2024, February 8). Why does the state have a monopoly on money? *Economic Forces*. https://www.economicforces.xyz/p/why-does-the-state-have-a-monopoly

Hern, A. (2017, February 21). Mt Gox CEO charged with embezzling £1.7m worth of bitcoin. *The Guardian*. https://www.theguardian.com/technology/2015/sep/14/bitcoin-mt-gox-ceo-mark-karpeles-charged-embezzling

Hetler, A. (2022, August 1). *Proof of work vs. proof of stake: What's the difference?* WhatIs. https://www.techtarget.com/whatis/feature/Proof-of-work-vs-proof-of-stake-Whats-the-difference

Hicks, C. (2023, March 16). Different types of cryptocurrencies. *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/different-types-of-cryptocurrencies/#:~:text=How%20Many%20Cryptocurrencies%20Are%20There,market%20capitalization%20of%20%241.1%20trillion

Hicks, C. (2024, January 25). What are crypto wallets? *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/crypto-wallets/

Hileman, G. (2014). *A History of Alternative Currencies*. https://www.hillsdale.edu/wp-content/uploads/2016/02/FMF-2014-A-History-of-Alternative-Currencies.pdf

Hooper, A. (2023, April 5). Debunking the myth: Cryptocurrency is used for criminal activity. *Cointelegraph*. https://cointelegraph.com/news/debunking-the-myth-cryptocurrency-is-used-for-criminal-activity

Huang, K. (2022, November). *Why Did FTX Collapse? Here's What to Know*. New York Times. https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html

Hughes, B. (2023, February 22). 4 Reasons Why US Lawmakers Shouldn't Back Sen. Warren's Latest Crypto Bill. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/02/15/4-reasons-why-lawmakers-shouldnt-back-sen-warrens-latest-crypto-bill/

Hughes, E. (1992). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

Hyperinflation in Argentina. (n.d.). https://www.citeco.fr/10000-years-history-economics/contemporary-world/hyperinflation-in-argentina#:~:text=Inflation%20started%20rising%20prior%20to,300%25%20between%201975%20and%201990

Investopedia. (2023, August 27). *DigiCash: Meaning, history, implications*. https://www.investopedia.com/terms/d/digicash.asp#:~:text=By%201995%2C%20the%20company%20had,Bank%2C%20and%20the%20Bank%20Austria

IRS. (2024, February). *Digital Assets*. Internal Revenue Service. https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets

Ivanova, I. (2021, October 22). U.S. Treasury amends proposal to monitor bank accounts and report to IRS, raising threshold to $10,000. *CBS News*. https://www.cbsnews.com/news/irs-bank-account-update-change-treasury-10000-dollars/

Jabotinsky, H. (2020, November 29). *The Regulation of Cryptocurrencies: Between a Currency and a Financial Product*. The Fordham Law Archive of Scholarship and History. https://ir.lawnet.fordham.edu/iplj/vol31/iss1/2/

Jaikaran, C. (2018). *Blockchain: Background and Policy Issues*. Congressional Research Service. https://sgp.fas.org/crs/misc/R45116.pdf

Jakobsson, M., & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols. In *Springer eBooks* (pp. 258–272). https://doi.org/10.1007/978-0-387-35568-9_18

Jasperse, J. (2023, May 30). *50-State Review of Cryptocurrency and Blockchain Regulation - Stevens Center for Innovation in Finance*. Stevens Center for Innovation in Finance. https://stevenscenter.wharton.upenn.edu/publications-50-state-review/

Johnson, L., & Pozza, D. (2023, July 21). *The FTC is targeting crypto too - with a significant new enforcement action*. JD Supra. https://www.jdsupra.com/legalnews/the-ftc-is-targeting-crypto-too-with-a-9740039/

Jones, B. J. M. (2022, August 25). Americans Using Cash Less Often; Foresee Cashless Society. *Gallup.com*. https://news.gallup.com/poll/397718/americans-using-cash-less-often-

foresee-cashless-society.aspx#:~:text=The%20latest%20Federal%20Reserve%20payment,for%203%25%20of%20all%20transactions
Kaloudis, G. (2023, May 22). Celebrating Bitcoin Pizza Day: the Time a Bitcoin User Bought 2 Pizzas for 10,000 BTC. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/05/22/celebrating-bitcoin-pizza-day-the-time-a-bitcoin-user-bought-2-pizzas-for-10000-btc/
Kapilkov, M. (2021, September 14). Previously Unpublished Emails of Satoshi Nakamoto Present a New Puzzle. *Coin Desk*. https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle/
Karimov, B., & Wójcik, P. (2021). Identification of scams in initial coin offerings with machine learning. *Frontiers in Artificial Intelligence, 4*. https://doi.org/10.3389/frai.2021.718450
Keep Your Coins Act. (2023). Congress. https://www.congress.gov/bill/118th-congress/house-bill/4841/text#:~:text=To%20prohibit%20Federal%20agencies%20from,use%2C%20and%20for%20other%20purposes
Kessler, C. (2021, October 20). A banking app has been suddenly closing accounts, sometimes not returning customers' money. *ProPublica*. https://www.propublica.org/article/chime
Kharpal, A. (2017, April 12). Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency. *CNBC*. https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html
Kharpal, A. (2022, July 8). Embattled crypto lender Celsius is a "fraud" and "Ponzi scheme," lawsuit alleges. *CNBC*. https://www.cnbc.com/2022/07/08/crypto-lender-celsius-is-a-fraud-and-ponzi-scheme-lawsuit-claims.html
Klein, A. (2020, December 9). 3 steps to improve anti-money laundering regulation. *Brookings*. https://www.brookings.edu/articles/3-steps-to-improve-anti-money-laundering-regulation/
Klein, B. (1974). The competitive supply of money. *Journal of Money, Credit and Banking, 6*(4), 423. https://doi.org/10.2307/1991457
Korver, M., Andreessen Horowitz, Shirzad, F., Coinbase, Palmer, D., Anchorage Digital Bank, Coldebella, G., True Ventures, Schneps, K., Veterans for Energy and Technology Solutions, Pruden, A., Aleo Network Foundation, Gebner, A., MIT, Grieco, C., Davison, W., Viglione, R., Horizen Labs, Inc., Bridge, J., . . . Kinca, B. (2023). *Letter from Blockchain Association and National Security Signatories to Members of Congress*. https://theblockchainassociation.org/wp-content/uploads/2024/02/NatSecLettertoCongress_2_13_24-1.pdf
Kost, E. (2023, August). *10 biggest data breaches in finance*. Upguard. https://www.upguard.com/blog/biggest-data-breaches-financial-services
Kuhn, D. (2023a, May 24). The Blocksize Wars Revisited: How Bitcoin's Civil War Still Resonates Today. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/05/17/the-blocksize-wars-revisited-how-bitcoins-civil-war-still-resonates-today/
Kuhn, D. (2023b, July 14). Why Did Celsius Go Up in Flames? Alex Mashinsky Built Celsius a House of Cards. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/07/13/celsius-sold-lies-to-sell-cel-tokens/

Kuhn, D. (2024, March 21). Why the SEC Shouldn't Classify ETH as a Security. *Coindesk*. https://www.coindesk.com/consensus-magazine/2024/03/20/why-the-sec-shouldnt-classify-eth-as-a-security/

Ledger Insights & Ledger Insights. (2023, November 7). *Fed Governor Barr: stablecoins borrow the trust of Federal Reserve*. Ledger Insights - Blockchain for Enterprise. https://www.ledgerinsights.com/stablecoins-borrow-trust-federal-reserve-barr/

Leonardo, G. (2023a, July 14). *RFIA 2.0, XRP, NDAA*. Cap Hill Crypto. https://ckarchive.com/b/k0umh6hdnx0qdalh7

Leonardo, G. (2023b, July 21). *FIT for 21st Century; AML in Senate*. Cap Hill Crypto. https://ckarchive.com/b/qdu8h7h7ogn46clhk

Leonardo, G. (2023c, July 28). *Crypto Bills Advance*. Cap Hill Crypto. https://ckarchive.com/b/gkunh5hd6o57gbrh9

Li, T., Shin, D., & Wang, B. (2019). *Cryptocurrency Pump-and-Dump Scheme*. https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:2bfa23c4-a21a-4c18-a052-63cd44b4e2b5

Liao, S. (2017, December 6). Steam no longer accepting bitcoin due to 'high fees and volatility.' *The Verge*. https://www.theverge.com/2017/12/6/16743220/valve-steam-bitcoin-game-store-payment-method-crypto-volatility

Lopp, J. (2016, April 9). *Bitcoin and the Rise of the Cypherpunks*. Coin Desk. https://www.coindesk.com/markets/2016/04/09/bitcoin-and-the-rise-of-the-cypherpunks/

Lucking, D., & Aravind, V. (2022). *Cryptocurrency as a Commodity: The CFTC's Regulatory Framework*. Global Legal Insight. https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:2278ce96-15bd-41bb-a77c-f29ff18c79bc

Lummis, Ms., & Gillibrand, Mrs. (2023). Lummis-Gillibrand Responsible Financial Innovation Act. In *United States Senate*. https://www.lummis.senate.gov/wp-content/uploads/Lummis-Gillibrand-2023.pdf

Lummis-Gillibrand. (2023). *Lummis-Gillibrand Responsible Financial Innovation Act of 2023 Section by Section*. https://www.lummis.senate.gov/wp-content/uploads/Lummis-Gillibrand-2023-Section-by-Section-Final.pdf

Maheshwari, R. (2024, January 10). What are crypto exchanges and how do they work. *Forbes Advisor INDIA*. https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-a-crypto-exchange/

Majority Staff, F. S. C., Fennie Wang, Matt Homer, David Portilla, Robert Morgan, & Delicia Reynolds Hand. (2023). *Putting the "Stable" in "StableCoins:" How legislation will help stablecoins achieve their promise*. https://docs.house.gov/meetings/BA/BA21/20230518/115973/HHRG-118-BA21-20230518-SD002.pdf

Malwa, S. (2024, March 8). Solana Back Up Following Major 5-Hour Outage. *Coindesk*. https://www.coindesk.com/markets/2024/02/06/solana-network-suffers-brief-outage-sol-steady/

Manfredi, R. (2023, August 22). *Lummis-Gillibrand Responsible Financial Innovation Act: An overview of new provisions in the reintroduced bill*. Gibson Dunn. https://www.gibsondunn.com/lummis-gillibrand-responsible-financial-innovation-act-an-overview-of-new-provisions-in-the-reintroduced-bill/

Marr, B. (2022, October 12). A short history of Bitcoin and crypto currency everyone should read. *Forbes*. https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=1148c4c83f27

MCHENRY, M. (2023). *H.R. 4766 Clarity for Payment Stablecoins Act*. https://docs.house.gov/meetings/BA/BA00/20230727/116295/BILLS-118-HR4766-M001156-Amdt-3.pdf

Meyer, A. (2023, April). *Banks Are Closing Customer Accounts, With Little Explanation*. New York Times. https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html

Michel, N. (2022, July 18). *Central Bank Digital Currencies and Freedom Are Incompatible*. CATO Institute. https://www.cato.org/commentary/central-bank-digital-currencies-freedom-are-incompatible

Michel, N. (2023a, February 22). *The Risks of CBDCs*. CATO Institute. https://www.cato.org/visual-feature/risks-of-cbdcs#:~:text=By%20programming%20a%20CBDC%2C%20money,%5Bpeople%20can%20do.%5D%E2%80%9D&text=A%20CBDC%20could%20undermine%20both,challenging%20the%20rise%20of%20cryptocurrency

Michel, N. (2023b, September 14). *Digital Dollar Dilemma: The Implications of a Central Bank Digital Currency and Private Sector Alternatives*. CATO Institute. https://www.cato.org/testimony/digital-dollar-dilemma-implications-central-bank-digital-currency-private-sector

Mitchelhill, T. (2023, May 24). ETH can be both a security and a commodity, former CFTC commissioner says. *Cointelegraph*. https://cointelegraph.com/news/eth-can-be-security-and-commodity-says-former-cftc-commissioner

Mitchell, D. (2016, October 11). *Money Laundering Laws: Ineffective and Expensive*. CATO Institute. https://www.cato.org/blog/money-laundering-laws-ineffective-expensive#:~:text=There%27s%20no%20evidence%20that%20these,financial%20services%20for%20poor%20people

Mola, S. (2024, January 24). *SEC enforcement of cryptocurrency reaches a new high | Cornerstone Research*. Cornerstone Research. https://www.cornerstone.com/insights/press-releases/sec-enforcement-of-cryptocurrency-reaches-a-new-high/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. In *Bitcoin.org*. https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2009, February 11). *Bitcoin Open Source Implementation of P2P Currency*. Satoshi Nakamoto Institute. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1

Napolitano, E. (2022, November 18). *Sam Bankman-Fried and the FTX collapse, explained*. NBC News. https://www.nbcnews.com/tech/crypto/sam-bankman-fried-crypto-ftx-collapse-explained-rcna57582

Napolitano, E. (2023, July 20). SEC Chair Gensler Cites “Wild West” of Crypto in Case to Increase Agency’s Budget. *Coindesk*. https://www.coindesk.com/policy/2023/07/19/sec-chair-gensler-cites-wild-west-of-crypto-in-case-to-increase-agencys-budget/

Nebraska Department of Banking and Finance. (2023). *Digital Assets*. https://ndbf.nebraska.gov/industries/digital-assets#:~:text=The%20Act%20authorizes%20a%20new,the%20blockchain%2Fdigital%20asset%20industry

Nelson, R. (2023). *Central Bank Digital Currencies*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11471

Nessi, H. (2023, December). *Argentina inflation tops 160% spotlighting challenge for Milei*. Reuters. https://www.reuters.com/world/americas/argentina-inflation-tops-160-spotlighting-challenge-milei-2023-12-13/

Nguyen, H. (2021, December 7). Why Ethereum Architecture is Flawed - Hugo Nguyen - Medium. *Medium*. https://hugonguyen.medium.com/why-ethereum-architecture-is-flawed-d4eefd15db3e

Nunn, Z. (2023, September 7). *Financial Technology Protection Act*. Representative Nunn. https://nunn.house.gov/SL/Financial-Technology-Protection-Act#:~:text=The%20Financial%20Technology%20Protection%20Act%20aims%20to%20protect%20emerging%20digital,government%20and%20crypto%20industry%20leaders

NYDFS. (2022). *Virtual currency businesses*. New York Department of Financial Services. https://www.dfs.ny.gov/virtual_currency_businesses#:~:text=NYCRR%20Part%20200.-,History,currency%20business%20activity%20since%202013

O'Neill, J. (2021, February 5). Calls for Bank of America boycott grow after data given to FBI. *New York Post*. https://nypost.com/2021/02/05/calls-for-bank-of-america-boycott-grow-after-data-given-to-fbi/

Orcutt, M., & Manoylov, M. (2022, May 12). Terra, Luna and UST: How we got here. *The Block*. https://www.theblock.co/post/146444/terra-luna-and-ust-how-we-got-here

Pair, S. (2018, May 10). The Bitcoin fee market - Stephen Pair - medium. *Medium*. https://medium.com/@spair/the-bitcoin-fee-market-4df1857d12b7

Palmer, D. (2021, September 13). More than half of ICOs fail within 4 months, study suggests. *CoinDesk*. https://www.coindesk.com/markets/2018/07/10/more-than-half-of-icos-fail-within-4-months-study-suggests/

Patterson, M. (2018, September 12). *Crypto's 80% Plunge Is Now Worse Than the Dot-Com Crash*. Bloomberg. https://www.bloomberg.com/news/articles/2018-09-12/crypto-s-crash-just-surpassed-dot-com-levels-as-losses-reach-80

Peirce, H., & Roisman, E. (2021, July 14). *In the Matter of Coinschedule*. Securities and Exchange Commission. https://www.sec.gov/news/public-statement/peirce-roisman-coinschedule

Perez, Y. B. (2021, September 11). Mt Gox: The History of a Failed Bitcoin Exchange. *Coindesk*. https://www.coindesk.com/markets/2015/08/04/mt-gox-the-history-of-a-failed-bitcoin-exchange/

Peterson, A. (2021, December 6). Hal Finney received the first Bitcoin transaction. Here's how he describes it. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/

Pham, S. (2019, March). *Former Mt. Gox chief Mark Karpeles acquitted of most charges in major bitcoin case*. CNN. https://www.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html#:~:text=The%20man%20who%20oversaw%20the,cryptocurrency%20exchange%20in%20the%20world

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice*, *3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Polk, D. (2024, March 12). *Chairman McHenry's Clarity for Payment Stablecoins Act approved by the House Financial Services Committee*. Davis Polk. https://www.davispolk.com/insights/client-update/chairman-mchenrys-clarity-payment-stablecoins-act-approved-house-financial

Porter, D. (2023, March 6). Bitcoin Mining Is Good for the Energy Grid and Good for the Environment. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/03/06/bitcoin-mining-is-good-for-the-energy-grid-and-good-for-the-environment/

Pritzker, Y. (2019). *Inventing Bitcoin: The Technology Behind the First Truly Scarce and Decentralized Money Explained*.

Quigley, J., & Gilbert, J. (2024, April 24). *What is proof-of-work (POW)? All you need to know*. Blockworks. https://blockworks.co/news/what-is-proof-of-work

Quinn, G. (2022, February). *Stablecoins are a national security asset in the digital age*. Law 360. https://www.law360.com/articles/1463286/stablecoins-are-a-national-security-asset-in-the-digital-age

Qureshi, H. (2021, December 8). The ICO bubble explained in three moments - HackerNoon.com - medium. *Medium*. https://medium.com/hackernoon/3-moments-in-history-that-explain-the-ico-bubble-e7c42896ca6f

Radmilac, A., & Van Straten, J. (2022, August 17). Research: Ethereum is neither decentralized nor deflationary. *CryptoSlate*. https://cryptoslate.com/research-ethereum-is-neither-decentralized-nor-deflationary/

Ramos, J. (2024, February 13). Elizabeth Warren Bill may kill crypto in US: Blockchain Association. *Watcher Guru*. https://watcher.guru/news/elizabeth-warren-bill-may-kill-crypto-in-us-blockchain-association#google_vignette

Reuters. (2022, October 14). *SEC's Gensler says CFTC authority over stablecoins should be bolstered*. https://www.reuters.com/technology/secs-gensler-says-cftc-authority-over-stablecoins-should-be-bolstered-2022-10-14/

Rizzo, J. (2023, May 22). Elizabeth Warren's Bill Won't Stop Money Laundering, but It Could Ban Crypto. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/05/18/elizabeth-warrens-bill-wont-stop-money-laundering-but-it-could-ban-crypto/

Robinson, T., & Fanusie, Y. (2018). *BITCOIN LAUNDERING: AN ANALYSIS OF ILLICIT FLOWS INTO DIGITAL CURRENCY SERVICES*. Elliptic. https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf

Rockoff, H. (1974). The Free Banking Era: A reexamination. *Journal of Money, Credit, and Banking/Journal of Money, Credit and Banking*, *6*(2), 141. https://doi.org/10.2307/1991023

Rolnick, A., & Weber, W. (1983). New evidence on the free banking era on JSTOR. *The American Economic Review*. https://www.jstor.org/stable/1814673

Romney, Reed, Rounds, & Warner. (2024). *Crypto-Asset National Security Enhancement and Enforcement Act of 2023*. https://www.romney.senate.gov/wp-content/uploads/2023/07/SIL238651.pdf

Rowe, N. (2024, January 24). *Hitting a record high in 2023, SEC enforcement actions against crypto firms have nearly doubled since 2021—the year Gensler took over*. Fortune Crypto. https://fortune.com/crypto/2024/01/24/crypto-enforcement-actions-sec-gary-gensler-new-report/

Sapkota, N., Grobys, K., & Dufitinema, J. (2020). How much are we willing to lose in cyberspace? On the tail risk of scam in the market for initial coin offerings. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3732747

Schroeder, P. (2024, March 7). *Powell says Fed not "remotely close" to a central bank digital currency*. Reuters. https://www.reuters.com/markets/us/powell-says-fed-not-remotely-close-central-bank-digital-currency-2024-03-07/

Schulp, J., Solowey, J., Anthony, N., & Thielman, Ni. (2023, January 27). *Overstating Crypto Crime Won't Lead to Sound Policy*. CATO Institute. https://www.cato.org/blog/overstating-crypto-crime-wont-lead-sound-policy

Scott, A., Sykes, J., Su, E., & Tierno, P. (2022). *How the Lummis-Gillibrand Responsible Financial Innovation Act (S. 4356) Would Alter the Crypto Regulatory Landscape*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11971

Schwinger, R. (2018, March 14). *Federal court holds that CFTC can regulate virtual currencies as commodities*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-us/knowledge/publications/6c7bcc30/federal-court-holds-that-cftc-can-regulate-virtual-currencies-as-commodities

SEC. (2023a, June 5). *SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao*. US Securties and Exchange Commission. https://www.sec.gov/news/press-release/2023-101

SEC. (2023b, June 6). *SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency*. US Securities and Exchange Commission. https://www.sec.gov/news/press-release/2023-102

Sekharan, T. (2022, September 20). Blocksize Wars- When Bitcoin split in 2. *Medium*. https://tiena-sekharan.medium.com/blocksize-wars-when-bitcoin-split-in-2-b790e6c97693

Sigalos, M. (2021, July 20). Bitcoin mining isn't nearly as bad for the environment as it used to be, new data shows. *CNBC*. https://www.cnbc.com/2021/07/20/bitcoin-mining-environmental-impact-new-study.html

Sigalos, M. (2022, January 7). Crypto scammers took a record $14 billion in 2021. *CNBC*. https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html

Smith, J. (2017, August 11). *The Bitcoin cash hard fork will show us which coin is best*. Fortune. https://fortune.com/2017/08/11/bitcoin-cash-hard-fork-price-date-why/

Smith, K. (2023a, August 16). The FIT Act Is the Most Comprehensive Crypto Regulation Ever Voted on by Congress. *Coindesk*. https://www.coindesk.com/consensus-magazine/2023/08/16/the-fit-act-is-the-most-comprehensive-crypto-regulation-ever-voted-on-by-congress/

Smith, K. (2023b, November 15). *Washington shouldn't give in to crypto panic*. Blockworks. https://blockworks.co/news/washington-crypto-panic-congress

Smith, S. (2023, November 29). 2 More reasons why crypto tax compliance is increasingly difficult. *Forbes*. https://www.forbes.com/sites/digital-assets/2023/11/28/two-more-reasons-why-crypto-tax-compliance-is-increasingly-difficult/?sh=950084473903

Snakai. (2023, July 13). *Lummis, Gillibrand Reintroduce comprehensive legislation to create regulatory framework for crypto assets*. Kirsten Gillibrand | U.S. Senator for New York. https://www.gillibrand.senate.gov/news/press/release/lummis-gillibrand-reintroduce-comprehensive-legislation-to-create-regulatory-framework-for-crypto-assets/

Steven. (2023, August 17). *Bank of America hit by data breach affecting 11K customers*. IDStrong. https://www.idstrong.com/sentinel/bank-of-america-suffers-another-data-breach/

Stevens, R. (2024, March 9). Securities vs. Commodities: Why It Matters For Crypto. *Coindesk*. https://www.coindesk.com/learn/securities-vs-commodities-why-it-matters-for-crypto/

Studenski, P., & Krooss, H. E. (2003). *Financial history of the United States*. Beard Books.

Su, E. (2021). *Stablecoins: Background and Policy Issues*. Congressional Research Service. https://sgp.fas.org/crs/misc/IF11968.pdf

Szabo, N. (2005). *Bit gold*. https://unenumerated.blogspot.com/2005/12/bit-gold.html

Thales. (2023, February 1). *A brief history of encryption (and cryptography)*. Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption#:~:text=Modern%20cryptography%20(computer%2Dbased%20encryption,until%20it%20cracked%20in%201997.

The Economist. (2018, April 30). Crypto money-laundering. *The Economist*. https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

Tierno, P. (2023a). *Cryptocurrency: Selected Policy Issues*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47425

Tierno, P. (2023b). *Introduction to Cryptocurrency*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12405

Tierno, P. (2023c). *Stablecoin Policy Issues for the 118th Congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12450#:~:text=Regulatory%20Framework&text=Today%2C%20stablecoin%20issuance%20remains%20the,for%20anti%2Dmoney%20laundering%20purposes

Tierno, P., & Scott, A. (2023). *An Overview of H.R. 4766, Clarity for Payment Stablecoins Act*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN12249

Tierno, P., & Su, E. (2023). *An Overview of H.R. 4763, Financial Innovation and Technology for the 21st Century Act*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN12223

Tobey, J. S. (2024, March 26). The Federal Reserve's folly: an inflation rate of 20%. *Forbes*. https://www.forbes.com/sites/johntobey/2024/03/26/the-federal-reserves-folly-an-inflation-rate-of-20/?sh=b55a06b51de5

Top 50 cryptocurrency prices, coin market cap, price charts and historical data | Crypto.com. (n.d.). crypto.com. https://crypto.com/price

Tucker, J. A. (2023, February 3). *Bitcoin and Mises's Regression Theorem*. Free the People. https://freethepeople.org/bitcoin-and-misess-regression-theorem-2/

Verma, P., & Bogage, J. (2023, March 13). Signature Bank's collapse spells trouble for cryptocurrency industry. *Washington Post*. https://www.washingtonpost.com/technology/2023/03/13/signature-bank-collapse-crypto/

Vidal, A. (2023, December 8). *Digital currency's Titanic: Ethereum's sinking ship of flawed technology exposed*. CoinGeek. https://coingeek.com/digital-currency-titanic-ethereum-sinking-ship-of-flawed-technology-exposed/

Von Mises, L., & Batson, H. E. (1912). *The theory of money and credit*. http://cyber.sibsutis.ru:82/Monarev/docs/nauka/PROBABILITY/MVspf_Stochastics%20i

n%20finance/Ludwig%20von%20Mises.%20Theory%20of%20Money%20and%20Credit(302s).pdf
Wagner, C. (2023a, July 18). *Rep. Torres asks SEC to reconsider "crusade against crypto" in wake of Ripple*. Blockworks. https://blockworks.co/news/rep-torres-sec-reconsider-regulation-by-enforcement
Wagner, C. (2023b, November 30). *SEC's Hester Peirce doesn't know what her agency is trying to accomplish*. Blockworks. https://blockworks.co/news/hester-peirce-sec-endgame
Warren, E., & Marshall, R. (2021). *The Digital Asset Anti-Money Laundering Act of 2022 Overview*. https://www.warren.senate.gov/imo/media/doc/Crypto%20National%20Security%20One-Pager%20draft_12.13.22.pdf
What is Ethereum? | ethereum.org. (2023). ethereum.org. https://ethereum.org/en/what-is-ethereum/
White, L. H. (2023). *Better money: Gold, Fiat, or Bitcoin?* Cambridge University Press.
Whited, T. M., Wu, Y., & Xiao, K. (2022). Central bank digital currency and banks. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4112644
Whittaker, M. (2023, April 12). How does bitcoin mining work? *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-mining/
Whittaker, M. (2024, March 8). Top 10 Altcoins of 2024. *Forbes Advisor*. https://www.forbes.com/advisor/investing/cryptocurrency/best-altcoins/
Wilson, T. (2023, October 23). *Crypto's role in terrorist financing*. Reuters. https://www.reuters.com/technology/cryptos-role-terrorist-financing-2023-10-23/
Wolf, T. (2023, June 29). *Chair Gensler must recuse himself from digital asset enforcement decisions*. Blockchain Association. https://theblockchainassociation.org/chair-gensler-must-recuse-himself/
Wolf, T. (2024, February 13). *Former U.S. Military and National Security Professionals Warn Against Enacting Proposed Legislation that Threatens Digital Asset Development*. Blockchain Association. https://theblockchainassociation.org/former-u-s-military-and-national-security-professionals-warn-against-enacting-proposed-legislation-that-threatens-digital-asset-development/
Wright, T. (2023, April 5). 'Ludicrous' to think Signature Bank's collapse was connected to crypto, says NYDFS head. *Cointelegraph*. https://cointelegraph.com/news/ludicrous-idea-that-signature-bank-s-collapse-was-connected-to-crypto-says-nydfs-head
Yaffe-Bellany, D. (2023, June 7). *Crypto Firms Start Looking Abroad as U.S. Cracks Down*. Axios. https://www.nytimes.com/2023/06/07/technology/crypto-firms-start-looking-abroad-as-us-cracks-down.html
Yakovenko, A. (2017). *Solana: A new architecture for a high performance blockchain v0*. https://solana.com/solana-whitepaper.pdf
Yeltekin, D. S. (2023, March 29). 5 lessons to learn from the collapse of FTX. *Simon Business School*. https://simon.rochester.edu/blog/deans-corner/5-lessons-learn-collapse-ftx
Yoaquim. (2023, January 23). I'm a Bitcoin Maximalist — Here's Why It's Dangerous. *Medium*. https://medium.com/coinmonks/im-a-bitcoin-maximalist-yes-it-s-disgusting-ed320999d6f5
Zuluaga, D. (2018, June 25). *Should Cryptocurrencies Be Regulated like Securities?* CATO Institute. https://www.cato.org/cmfa-briefing-paper/should-cryptocurrencies-be-regulated-securities