Luke Marushack, Tiantian Wei , Yuchen Yang , Yutan Zhang , Jenna Zhao

Professor Himonas

Mathematical Methods in Financial Economics

1 May 2023

Cryptocurrency and the Cryptocurrency Crisis

1. Introduction to Cryptocurrency

Before currency was prevalent in human societies, individuals and communities traded with each other using the Barter system. Barter describes the system in which different parties trade with each other using direct goods and services, without an intermediary (Chapman). However, as the need for trade increased over time, the barter system became inefficient due to its limitations, such as the difficulty to find someone to exchange goods with. Therefore, some intermediaries of trade emerged. At first, paper currency acted as a promise of payment later, but over time people started to agree on the value of such a medium of exchange (Ritter). However, throughout the history of expansion of paper currency, there were skepticisms about why a piece of paper is worth anything. Commodity money, a type of currency that has values derived from the commodity (such as gold or silver) it's made out of, emerged as a more widely accepted currency. Later on, when commodity money became incompatible with the efficiency and quantity required by the society, it evolved into representation money, which is a type of currency that's much easier to carry but is backed by the value of certain commodities (Andrei). Eventually, fiat money, a "money without intrinsic value that is used as money because of government decree", became the most widely used system (Mankiw). There has always been skepticism about the value of fiat money, because why does fiat money worth anything just because the government says so? Like fiat money, crypto money doesn’t have any intrinsic value. Evenmore, cryptocurrencies don't depend on any government backing. Hence there is even more skepticism about cryptocurrency. What is cryptocurrency and why is it worth anything?

Before going into the details of how cryptocurrency works, let’s draw an analogy between cryptocurrency and an ancient currency on Yap Island in Micronesia. The Yapese used a currency made out of stone which they referred to as Fei. Fei was made out of heavy stones they got from Palau island, which made the process of making Fei complicated and costly. Fei was often too big or too heavy to carry for the individuals to walk around with it to trade. Therefore, when the Yapese needed to make a trade, they made marks on the stone without moving the stone itself. As long as the majority of the villagers acknowledged the trade, the ownership of the stone was established. The richest family on the island had never seen their most valuable Fei. Their ancestors found a gigantic stone in Palau, and the stone was so big that it made their family the richest on the Island. However, they lost it to the ocean on their way back to Yap. However, because many villagers witnessed them getting the stone and the ownership was established, it did not matter where the stone was and it was still considered their property (Fitzpatrick, 2001). Much like Fei, the value and transaction of bitcoin also relies on “consensus”. On some level, one could say that Fei is the original crypto.

Cryptocurrency, or crypto is a digital currency designed to serve as a transaction medium which is decentralized, meaning that it is not controlled by or reliant on any central authority, such as a government or bank. It is based on a network of computers that collectively maintains a public ledger to eliminate the need for traditional intermediaries such as banks. Another interpretation of cryptocurrency is a form of digital currency run on a technology named blockchain. It is an easier way to complete transactions without dealing with online wallets, banks and third party applications, immune to counterfeiting, and is protected by strong and complex encryption algorithms.

The motivation of cryptocurrency can be explained by an easy example. Imagine four friends having dinner at a restaurant, and friend A pays the whole bill. They decide to split the expense with each other via online money transfer. However, when B is transferring money to A, there is a possibility that the transaction doesn't go through. Reasons behind the failed bank transactions would be related to the bank as an avoidable intermediary. Technical issues, one of their accounts getting hacked (security issues), transfer limit being exceeded, or high transaction costs would all impact the transaction. Moreover, whether the transaction is successful is not visible to the general public, thus a friend C would not be able to see the record of a transaction between A and B. The concept of cryptocurrency came into existence to solve these problems.

Go back to the previous example, if A requires all three other friends to send her two bitcoins as contributions to the dinner, and imagine A has five bitcoins in stock while others have two. First, when B sends two bitcoins to A, a record is created in the form of a block. The transaction record between them is permanently inscribed in the block. This record also holds the number of bitcoins that each of the friends own. Then C and D transferred bitcoins to A in the same way, and their transaction records are inscribed in blocks as well. These blocks are linked to each other as each of them takes reference from previous ones for the number of bitcoins each friend owns. This chain of blocks or records is called a ledger. This ledger is shared by all friends and is publicly distributed. A hacker will not be able to alter data in a blockchain because each user has a copy of the ledger and the data within the blockchain are encrypted by complex algorithms.

2. Speculative Bubbles

A speculative bubble is a situation where the prices of assets, such as stocks, real estate, or cryptocurrencies, rise to unsustainable levels due to the perception that the asset will continue to increase in value. This perception is often driven by a frenzy of buying activity, fueled by the fear of missing out (FOMO), and is not supported by the underlying fundamentals of the asset.

Speculative bubbles can be caused by various factors, such as excessive investor optimism, easy access to credit, and low interest rates, among others. However, the bubble eventually bursts when the demand for the asset declines, and investors rush to sell their holdings, causing a sharp drop in prices. This can lead to widespread panic selling, financial instability, and economic downturns. Examples of historical speculative bubbles outside of the cryptocurrency bubble include the dot-com bubble in the late 1990s, the housing bubble in the mid-2000s, and the tulip mania in the 17th century. It is important for investors to be aware of speculative bubbles and exercise caution when investing in assets that may be subject to such market conditions.

The Tulip Mania was a speculative bubble that occurred in the Netherlands during the 17th century, specifically in the early 1630s. The Dutch were introduced to the tulip flower in the late 16th century, and its exotic and beautiful appearance quickly made it a popular status symbol among the wealthy. As demand for tulips increased, so did the price of bulbs, and by the early 1630s, tulip bulbs had become a highly sought-after commodity, with prices reaching exorbitant levels. At the peak of the bubble, a single tulip bulb could be sold for the price of a house, or more.

The speculation was driven by a number of factors, including a rapidly expanding middle class with disposable income, a desire for luxury goods, and a growing market for trading goods. Additionally, the tulip market was largely unregulated, which allowed for rampant speculation and manipulation. However, the bubble burst in February 1637, when prices plummeted, leaving many investors with worthless bulbs and significant financial losses. The collapse of the tulip market had a significant impact on the Dutch economy, leading to widespread bankruptcies and financial instability.

The dot-com bubble was a speculative bubble that occurred in the late 1990s and early 2000s, primarily in the United States. The bubble was driven by the rapid growth of the internet and the emergence of many new internet-based companies, commonly referred to as dot-coms. Investors were excited about the potential of these new companies to disrupt traditional business models and create new opportunities for growth. As a result, many dot-coms received significant investments, even if they were not yet profitable or had no clear path to profitability.

The bubble reached its peak in March 2000, when the NASDAQ stock market, which was heavily weighted towards technology stocks, reached an all-time high. However, the bubble burst shortly after, and the NASDAQ lost nearly 80% of its value by the end of 2002. The collapse of the dot-com bubble had a significant impact on the U.S. economy, leading to widespread bankruptcies, job losses, and a decline in consumer confidence. Many investors who had put their money into dot-com companies lost large amounts of money.

Like the dotcom bubble and the tulip bubble, the crypto bubble had a significant impact on many individuals and companies. The cryptocurrency bubble was fueled by low interest rates and easy access to capital. Many consumers borrowed money in order to buy cryptocurrency, and were levered to a point at which a small decrease in crypto prices could result in a margin call.

3. How Does the System Work

We will use Bitcoin as a concrete example for how cryptocurrency works. Traditionally, to make the finance system work, people have to trust certain individuals or institutions. For example, one has to trust banks to secure their deposits and make transactions. They need to trust exchanges or dealers to execute their trades. However, with virtual currencies, a centralized system incurs risks. Many had attempted to create virtual currencies before bitcoin emerged, and most of them required some level of centralization and led to different levels of complexities. Some of them were logistic issues, such as who would be responsible for the "central bank" of the currency; and some of them were safety problems, such as the possibility of attracting hackers to attack the central system.

In October 31, 2008, a person (or group of people) using the pseudonym Satoshi Nakamoto released an article describing a technology that is essential to the existence and development of cryptocurrencies (Nakamoto). The technology would allow an anonymous, decentralized trust from "proof-of-work" consensus. In responding to the trust issue in the traditional financial system, what Nakamoto suggests is to replace the concept of "trust" by cryptographic proof.

In order to understand how the bitcoin system works, we first need to introduce the four essential components of the bitcoin system:

1. A decentralized peer-to-peer network (the Bitcoin protocol)
2. A public transaction ledger (the blockchain)

3. A set of rules for independent transaction validation and currency issuance (consensus rules)
4. A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

2.1 A decentralized peer-to-peer network

One of the main protocols in cryptocurrency transactions is that the participants are all on a decentralized, peer-to-peer network. A decentralized peer-to-peer network, (also known as P2P network), refers to a system in which peers have equal capabilities and authority without a central control. That means, all users in the network would act as equal agents and no one is more superior than the others, so each user could operate and contribute equally to the system. It's also anonymous, so it protects the identity of each individual node.

2.2 Blockchain

Blockchain is a decentralized, distributed public transaction ledger built on a peer-to-peer network. It is a growing list of records that is available for all the nodes in the system at all times. It stores all historical records of transactions in which one user sends some digital asset to another user. P2P allows all nodes to have access to the public information in the blockchain and update the information with equal access. Due to the nature of the "chain-like" blocks, once a clock is added to the chain, it cannot be altered or deleted without altering all subsequent blocks, making the blockchain a secure and tamper-resistant system.

In this way, the idea of "trust" is decentralized in cryptocurrencies. Much like the Yapeses, the P2P system makes sure the public ledger, blockchain, is visible to all villagers (nodes). Once a transaction is updated to the blockchain, it is accepted by the whole village, and hence it’s valid.

Rather than trusting an individual or a central authority, people trust the decentralized system and everyone who contributes to the system. They trust that the blockchain is authentic and true, because they trust the amount of work that went into verifying and recording the transactions which makes it impossible to be duplicated and modified. The network collaboratively adds and verifies blocks faster than any individual can, so it’s difficult for one person to outrun the entire network. Additionally, the system considers the longest chain as the most secure because it has the most collective work. To modify the chain, one has to redo all the work that the network has done collectively, and add blocks faster than the entire work - an almost impossible task. The exact method of making this decentralized trust secured is by proof-of-work, which will be expanded in later sections.

2.3 Rules for independent transaction validation and currency issuance

For each transaction, their information gets sent to the P2P network, and each node can pick up the data and bundle them into a block. For bundling the data, the miners would use a hash function to output a hash value that corresponds to the transaction information. To put their block onto the blockchain, the miners will first need to identify the block that goes before their block, and grab certain information from that previous block. Then, they will produce a block header which includes information about the previous block, all the transactions they have in their block, and a key to a random puzzle. If they are fast enough to solve the puzzle before everyone else, they have a good chance of successfully appending their block to the chain.

Calculation power and speed are the most important components of the competition. However, due to the large number of miners joining the contest and the decentralized nature of P2P, there could be many blocks being added to the blockchain at the same time. This is known as forking. The system therefore uses the longest chain to decide which block is the most valid one, because it has the most accumulated proof-of-work. The valid block is then added to the blockchain, and the miner who contributed the block is rewarded.

The reward is a randomly generated amount of bitcoins the system awards to the miner who successfully contributes a new block to the chain. At this moment, the block reward is 6.25 bitcoins, but it is halved approximately every four years. There is an upper bound to how many bitcoins will be provided, and prediction is that in 2140, the bitcoin “mine” will be dried up. The system also restricts new blocks to show up only every 10 minutes. With more miners, more computers, and more calculation power in the system, the random puzzles will become harder to make sure it takes the miners roughly 10 minutes to solve. Each block also has a roughly constant size, which restricts the number of transactions it contains.

Other than rewards, individuals who put their transactions onto the network will include commissions to motivate miners to pick up their transactions. However, the miner could only collect their commission if their block is uploaded to the blockchain successfully. Currently, the value of bitcoin outweighs the commissions by a lot, and most of the profits for miners come from bitcoin rewards. However, as the bitcoin reward starts to decrease, eventually commission will become the main motivation for miners to maintain the system.

Both the rewards and commission act as a motivation for miners to maintain and contribute to the system. Because the calculation power needed for mining bitcoins is high, professional miners require a lot of hardware and engineering support. They also require equipment that allow them to outperform their competitors. They use a specific tool, the Application-Specific Integrated Circuits (ASICs) chips to get optimal computational speed. Therefore, the cost of mining is high, thus creating a rough lower bound to the value of bitcoins. The miners have a probability of successfully uploading a block every so often, and their reward plus commission should be able to cover their costs, otherwise they wouldn’t have an incentive to mine.

2.4 Proof of Work

Proof of Work (PoW) is a consensus algorithm that is used to verify transactions and add new blocks to a blockchain. The PoW algorithm requires nodes on the network to solve a complex mathematical problem in order to validate a block of transactions and add it to the blockchain.

The basic idea behind PoW is that to add a new block to the blockchain, a miner (or node) must solve a cryptographic puzzle for uploading the block to the blockchain. The puzzle is designed to be difficult to solve, but easy to verify. Once a miner solves the puzzle, they can submit the block to the network for verification. The other nodes can quickly verify if the solution is correct and that the new block is valid. The puzzle is typically a mathematical algorithm that requires a large amount of computational power to complete. This is what makes PoW an effective consensus algorithm, as it ensures that the work required to add a new block to the blockchain is significant enough to discourage malicious actors from attempting to disrupt the network.

Bitcoin uses a PoW algorithm called SHA-256 (Secure Hash Algorithm 256-bit) to validate and secure transactions, and to add new blocks to its blockchain. A hash function takes input data of arbitrary length and outputs a fixed-length string of bits, called a hash digest or hash value. The output is a unique representation of the input data, meaning that any change in the input data will produce a different hash value.

SHA-256 works by padding the input data with zeros to ensure its length is a multiple of 512 bits, breaking the padded data into 512-bit blocks, initializing a set of hash values to constant values, and applying a compression function that takes the 512-bit input block and the previous hash value as inputs and outputs a new hash value. The compression function uses bitwise logical operations and modular arithmetic to generate the new hash value. This process is repeated for each block of input data until all blocks have been processed. Finally, the final hash value is the concatenation of the hash values generated for each block. The output of the SHA-256 algorithm is a fixed-length hash digest of 256 bits. This hash value serves as a unique fingerprint of the input data and is used to ensure the integrity and authenticity of the data.

To illustrate how logical operations work, we provide two concrete examples: right rotation and right shift. Take a block as an example: 00001111011110100111101001011111.

1. If we were to perform rotation on it, for instance, we could right rotate it by 7 places, the block will go over the transformation::

   0000111101111010011110100**1011111**→**1011111**0000111101111010011110100

2. If we were to perform shift on it, for instance, we could right shift it by 3 places, the block will have the transformation:

   00001111011110100111101001011**111**→**000**00001111011110100111101001011

Shift is different from rotation in the sense that shift will move the block right or left depending on the operation, and 0’s at the remaining places. The logical operation introduces randomness to the process. Unless one knows which logical operations were performed on the blocks, it would be very difficult to reverse the operations, and decryption would mostly be a process of guess and check, which is nearly impossible due to the large number of possible operations.

SHA256 is a widely used cryptographic hash function that offers several benefits in securing data. It is deterministic, meaning that the same input data will always produce the same output hash value. Thus, it is ideal for verifying data integrity and ensuring that the input data is not altered or corrupted. Additionally, SHA256 is collision-resistant, which means that it is very difficult to find two different input values that produce the same hash output. This property ensures that it is difficult for anyone to manipulate the data without getting caught. SHA256 also provides excellent diffusion properties, meaning that even small changes in the input data will produce a completely different output hash value. This makes it ideal for ensuring data confidentiality and integrity, as any unauthorized change to the data will result in a different hash output. Additionally, SHA256 is non-reversible, meaning that it is practically impossible to determine the input data from the output hash value. This property makes it useful in protecting sensitive information such as passwords, credit card numbers, and other personal data.

In the Bitcoin network, miners need to include a correct block header in order to upload their block to the blockchain. The block header will include the block hash from the previous block, the Merkle root, timestamp, difficulty target, and a nonce. Merkle root is the hash output that summarizes all transactions included in this block, and nonce is a random number of leading zeros on the block hash. The miners need to repeatedly change the nonce value in the block header and apply the hash function until they find a nonce that produces a hash value that meets the difficulty requirement. This means that miners must essentially guess and check until they find the correct nonce value, which can take a significant amount of time and computational power. Overall, the benefits of SHA256 make it a highly secure and reliable method for hashing and securing data.

To maintain a consistent block time of approximately 10 minutes, the system is adjusted every 2016 blocks to change the difficulty, and it determines the amount of computational power required to solve the puzzle. Some miners use specialized hardware called ASICs (Application-Specific Integrated Circuits) to generate hashes as quickly as possible, and the first miner to solve the puzzle collects reward and transaction fees. Once a miner solves the puzzle, they broadcast the solution to the rest of the network, and other nodes verify that the solution is correct.

By requiring miners to expend significant computational resources to solve the cryptographic puzzle, and by using the longest chain to determine the valid block, the PoW algorithm makes it economically infeasible for malicious actors to attack the network. A 51% attack in Bitcoin is a hypothetical scenario in which an entity or a group of entities control more than 50% of the network's mining hash rate, giving them the ability to manipulate the Bitcoin blockchain's transactions. If an entity or group of entities control more than 50% of the network's mining power, they have the ability to manipulate the blockchain's transactions by excluding or reversing them. They can also prevent new transactions from being added to the blockchain, resulting in a halt in the entire Bitcoin network.

This type of attack can allow the attacker to double-spend their own coins or block transactions of other users, effectively disrupting the normal functioning of the network. It is considered a significant threat to the security and integrity of the Bitcoin network. However, executing a 51% attack in Bitcoin would require a massive amount of computational power and resources. With the longest-chain validation, they would also need to modify all subsequent blocks in the chain as well and outcompete all other miners on the network. The difficulty in acquiring such computational power and outcompeting all opponents makes it impractical and costly to execute.

The security of this algorithm and its difficult to hack makes Bitcoin one of the few decentralized systems that is resistant to attack. If some entity does not want to use a centralized currency, then Bitcoin is useful because it gives the anonymity and security that modern fiat currency cannot.

4. Advocations and Criticisms

The decentralization of cryptocurrency is the source of its most advocacies and criticisms. It provides freedom from associations to any government agencies, but also raises problems including the reliance on exchanges, criminal activities, potential system failing, and its failure to function as a currency.

One important advocating voice is that cryptocurrency revolutionizes remote transactions and enhances efficiency for global payments. Currently, any remote payments would need the intervention of some private infrastructure - the most common example is that one needs an account in the bank in order to pay and receive money. However, corporate intermediaries are getting fewer, larger and more powerful due to economies of scale. These features also make their failure increasingly grave. Bank failures will lead to serious financial problems; information leakage can happen on the scale of billions of people. Also, since financial corporations are inescapably closely monitored by governments, there are more difficulties transacting money around the globe. In contrast, the blockchain used for cryptocurrencies creates a public digital payment infrastructure that is available to all without the need of any intermediaries. Therefore, the use of cryptocurrency will allow resources to move around the world in easier and cheaper ways.

Moreover, since transacting agencies are not needed, cryptocurrency was used by people without bank accounts for transactions. According to the 2021 Fed Survey of Household Economics and Decisionmaking, people who used cryptocurrency for transactions were more likely to be unbanked than those who did not use cryptocurrency at all. Thirteen percent of transactional cryptocurrency users lacked a bank account, compared to six percent of people who did not use cryptocurrency, while 27 percent of cryptocurrency transactors did not have any credit cards, compared to 17 percent of non-users. (Fed) Another example is in El Salvador. 20% of the country comes from remittance from foreign countries, while 70% of the population doesn't have a bank account, causing up to 30%-50% wastes on the cost of transacting money. (PwC) The government tries to promote Bitcoin as a low-cost way of receiving remittances without banks. On the other hand, for businesses, one reason for using cryptocurrency is to attract more investors who value anonymity. It was reported that up to 40% of customers who pay with crypto are new customers of the company, and their purchase amounts are twice those of credit card users. (Bitpay)

However, there are also criticisms about cryptocurrencies. Although crypto transactions are decentralized, the challenge of transacting cryptocurrency is that one has to find a merchant/buyer that is willing to accept the crypto currency in exchange for the goods wanted. Such buyers are hard to find due to people's unfamiliarity of crypto currency and the high volatility. For example, in El Salvador, a street test showed that most merchants won't accept Bitcoin as a payment, and those who accept it have trouble verifying the transaction since it takes 10 minutes to add each block (NBC News). Thus, most people have to rely on exchanges to convert their crypto currencies into fiat money to use in the real world. The reliance on exchanges means that people using cryptos have to involve a centralized financial institution, thus lose their anonymity, all of which undermines the reason crypto currencies were created.

Also, there are security and regulation issues from the decentralization of cryptocurrencies. Cryptocurrencies operate in a largely unregulated environment, which can make them vulnerable to scams and criminal activities. In a 2018 report, Foley et al argued that "approximately one-quarter of bitcoin users are involved in illegal activity…around $76 billion of illegal activity per year involves bitcoin (46% of bitcoin transactions), which is close to the scale of the US and European markets for illegal drugs." By nature, crypto currencies can be favored by drug dealers, money laundering, and other illegal or highly taxed goods. This can cause problems for the government to regulate criminal activities. Additionally, the lack of oversight can lead to market instability and manipulation, as shown in the crypto crisis below in later sections.

There are dangers of cryptocurrency from lack of third party protection. Since only one's public key is needed for sending transactions, the receiver cannot block the payment. In the blockchain, there is no way of reverting a transaction. Thus, if the crypto is accidentally sent to the wrong recipient, there is no recourse. Also, if one loses their private key, they can't access their cryptocurrency because they cannot digitally sign the transactions. Since the private key is very complicated, a 256-bit number, the chance of losing the private key is high, and people have lost millions of dollars because of this.

Finally, another criticism questions the prosperity of using cryptocurrencies as a new form of money. While there is the ambitious vision of using cryptocurrencies as a "global currency," one might argue that cryptocurrencies don't satisfy the three fundamental functions of money at all. The functions of money states that (1) money is a medium of exchange, which is a widely accepted way of payment that could facilitate trades; (2) Money is a storage of value - it can allow for exchange across time, facilitate savings, accumulation, and investments; and (3) It is a unit of account - money allows people to compare values of different goods and services. Since cryptocurrencies have very high volatility, it is unlikely that people will be able to use it as a reliable storage of value or as a unit of account for everyday payments.

There also are problems associated with cryptocurrency as a medium of exchange. Given the immutable nature of transactions, and the irreversible nature of sending money, one can imagine potential problems associated with sending cryptocurrency in exchange for a good or service, then not receiving said good or service. One way cryptocurrency advocates have developed solutions for this problem is with smart contracts.

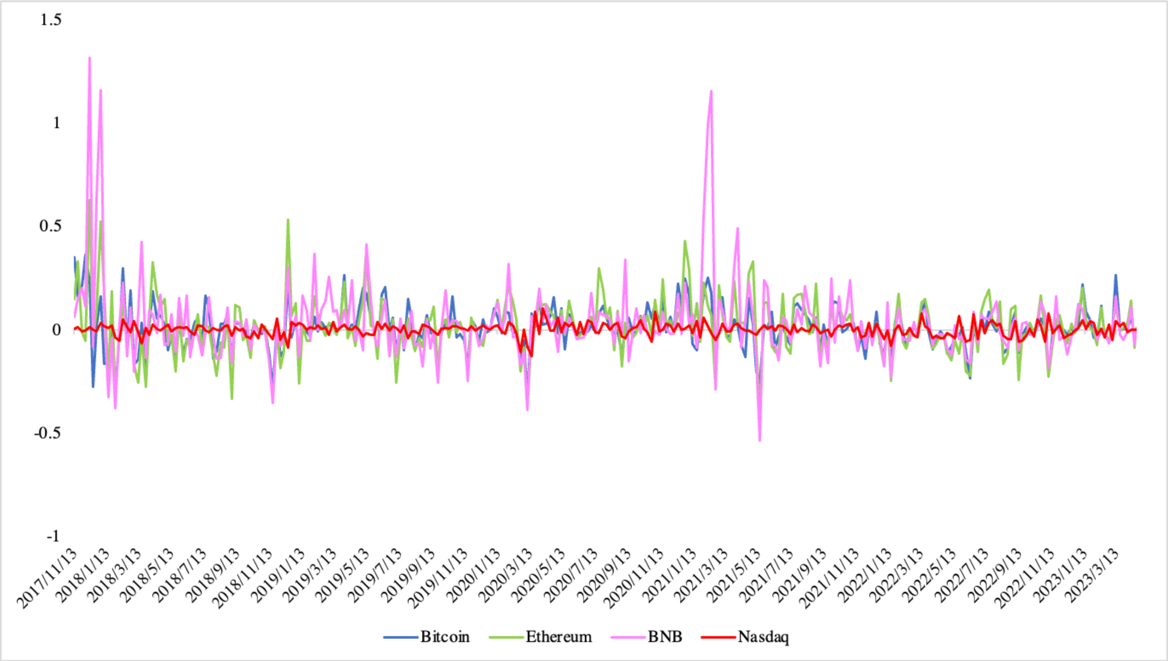
Smart contracts are self-executing digital contracts that allow parties to execute transactions without intermediaries such as banks, lawyers, or other third parties. They are typically programmed on a blockchain platform such as Ethereum, and they operate according to pre-specified rules and conditions. Smart contracts work by utilizing computer code that defines the rules and obligations of the contract. Once the contract is deployed on the blockchain, it becomes immutable and cannot be altered. The code in the smart contract will then automatically execute the terms of the contract when certain conditions are met.

For example, imagine a smart contract between two parties that involves the transfer of funds upon completion of a specific task. The contract would include specific conditions that must be met for the funds to be released. For instance, the contract may specify that the funds will be transferred to the recipient's account once the task has been verified by a third-party service. The smart contract would then automatically execute the transaction once the conditions have been met. This means that the funds will be transferred automatically, without the need for intermediaries to verify or process the transaction. Smart contracts can be used for a wide range of applications, including supply chain management, voting systems, and insurance policies, among others. They offer several benefits, including increased transparency, security, and efficiency, as well as lower costs due to the elimination of intermediaries.

In conclusion, although the cryptocurrencies give an innovative idea of decentralizing the current transacting system, there are multiple challenges to its full implementation into the real world.

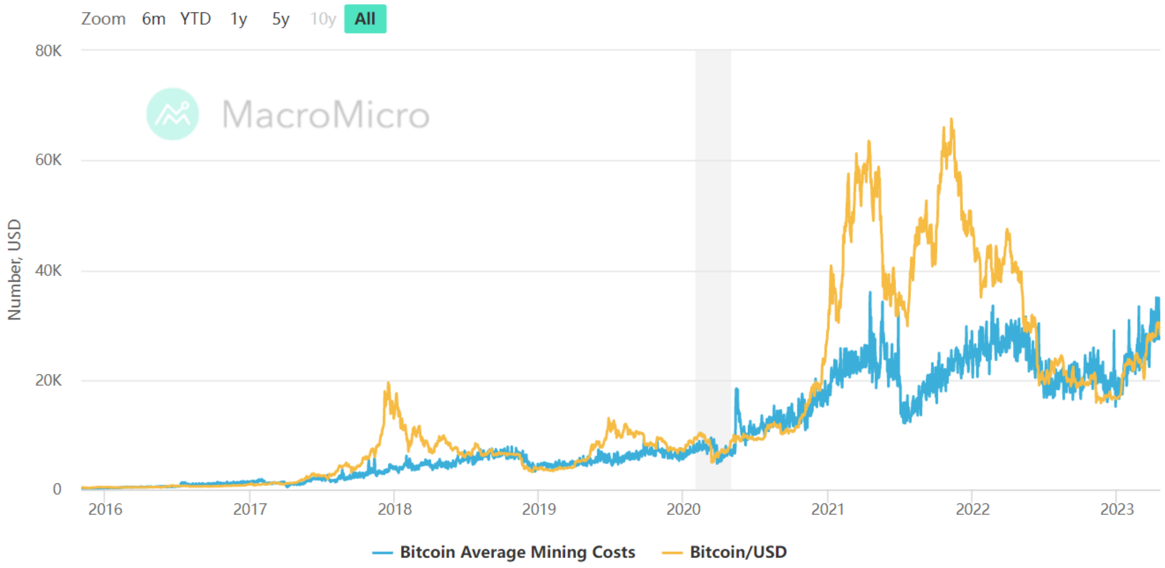
5. Crypto Valuation

Crypto assets and blockchain defines a brand new ecosystem that is conceptually different from the traditional finance system for which valuation reflects the value of underlying assets, economics, policies changes, etc. In the cryptocurrency world, market participants are still debating on whether they behave like currencies, commodities, or financial securities, or are something else. The shifting perceptions from market participants reflects in the high volatility of crypto prices. The recent crypto crisis is an example for which market participants' valuation for crypto suddenly decreased due to concerns about regulations issues. In general, with the exception of certain stablecoins, cryptocurrencies are known for their significant price fluctuations compared to conventional financial instruments like stocks and bonds. Below is a visual demonstration of the weekly returns of three types of cryptocurrencies versus the Nasdaq stock index (the red line). Compared to bonds and equities, the graph shows that cryptocurrencies may experience sudden declines in value, but also have the potential for substantial gains. Due to the high volatility of crypto currencies, their demand can be linked with economic situations. During economic downturns, people would seek safer assets and trend away from highly volatile equities including crypto currencies, causing its price to drop.



(Weekly Returns of Three Cryptos Verses that of Nasdaq Index)

However, the fundamental valuation of crypto currencies is dependent on the mining costs. This is because the only way of creating new cryptos is through mining. Although miners would receive commission from users for adding their transactions to the chain, currently the main income still comes from new crypto rewards. Mining depends on using computer power to solve algorithmic problems. Moreover, since there's only one winning miner at each time a block is added, the competition is intense and increasing when more participants enter the mining. The more participants, the harder to mine, and the more computing power needed to win the competition. To increase the computing power, more powerful equipment is needed. The energy cost and equipment cost, therefore, gives a floor of valuation for the crypto. Miners would have very limited motivation to mining if the cost is lower than prices of crypto.



(reference: https://en.macromicro.me/charts/29435/bitcoin-production-total-cost)

Above is the graph of Bitcoin average mining costs versus USD valuation of Bitcoin. We can observe that there is a slightly delayed correlation between Bitcoin price and mining cost. When the value of Bitcoin goes above mining cost, more miners would join and push the cost up. On the other hand, when Bitcoin price is significantly higher than mining cost, it symbolizes a bubble. In an ideal scenario, by perfect market competition theory, the prices of crypto currencies and the mining costs of them would converge.

6. The Cryptocurrency Crisis of 2022

The crypto market is highly volatile and can experience sharp fluctuations in value. The current crypto crisis captured public attention with the collapse of FTX this past November and the arrest of the exchange's founder, Sam Bankman-Fried. FTX Trading was formerly a cryptocurrency exchange and crypto hedge fund. The crypto industry's troubles began months earlier and have continued to spread. Here is a look at the timeline of the crisis.

In February, 2022, Bitcoin traded back down at $42,259.28 as the market started to price in the Federal Reserve's interest rate hikes. As reference, Bitcoin had peaked at $67,802 as investors rushed into riskier assets. In May, the Fed raised its benchmark interest rate by 50 bps to tame soaring inflation, making the sharpest increase since 2000. This led to a selloff in speculative investment, including bitcoin. The cryptocurrency TerraUSD, a stablecoin that is supposed to keep its value at $1, fell below its fixed value, and its sister coin, Luna, TerraUSD lost $40 billion in value. In June, the crypto lender Celsius and Babel Finance freezed all account withdrawals because of liquidity pressures and extreme market conditions. Later that month, the hedge fund Three Arrows Capital, which had invested heavily in TerraUSD, defaulted on loan payments to the crypto lender Voyager. In July, Voyager filed for bankruptcy protection.

In November of 2022, FTX experienced a sudden collapse due to a series of events that occurred earlier that month. On November 8th, users began withdrawing funds and cryptocurrency from their FTX accounts, causing a liquidity crisis for the company. FTX attempted to be rescued by rival Binance, but the deal fell through, and FTX subsequently filed for bankruptcy a few days later. The fallout was significant, with more than 100,000 creditors and tens of billions of dollars in assets and liabilities across a network of affiliates. This event marked the largest cryptocurrency-related bankruptcy to date, both in terms of its swiftness and its magnitude. To compound matters, FTX's founder, Sam Bankman-Fried, was arrested in the Bahamas on criminal charges filed by federal prosecutors in New York a month later.

7. Comparison to Subprime Lending Crisis

The cryptocurrency crisis and the subprime mortgage crisis are related in many ways. Both have resulted in significant financial loss for institutions as well as individuals. There are a number of similarities in both the causes as well as the effects of these two crises, including failure to properly evaluate counterparty risk, incorrect risk and volatility management, and misaligned incentives between conflicting parties. However, the cryptocurrency crisis and the subprime crisis are different in the nature of the response by the Federal Reserve as well as the fundamental belief in the security of the assets by both institutions and individuals.

One of the key risks new traders are taught about in the modern world is counterparty risk. This risk refers to the ability of one party to make payments to another party over the course of a transaction. An example of this is expressed in the options market. If I buy a European call option, but the difference between the strike price and market price is greater than my counterparty's wealth at expiration, then I might not get paid the full amount that my option is worth. In the mortgage backed securities market, when housing prices dropped and homeowners were unable to make the mortgage payments, they defaulted on their loans. This counterparty risk, the idea that homeowners were not able to pay back their loans, combined with the systemic risk of the market when that same default risk was reproduced in MBS, caused bank failures across the country and decimated the US economy, plunging us into recession.

In the cryptocurrency markets, consumers are subject to a similar type of counterparty risk. Exchanges like FTX are often wrought with liquidity issues, as there is a finite amount of cryptocurrency on the exchange at any given time. Because of the difficulties with on-chain computing and the delay of transferring cryptocurrency between two wallets, the liquidity pool available on crypto exchanges is subject to run out when multiple parties try to withdraw large balances simultaneously. In essence, this is similar to a bank run. A similar phenomena happened in 2008 when $193 billion was removed from money market funds over a short period of time after the failure of Lehman Brothers. The counterparty risk, in both cases, was devastating to consumers and caused significant financial losses.

Another similarity between the subprime crisis and the cryptocurrency crisis is the decay from investment towards speculation. In the years leading up to the subprime crisis, housing prices rose at a surprisingly high rate for no apparently evident reason. People thought the housing market would never drop and that it was immune to collapse. The purpose of buying a house, in many cases, was disfigured from buying a necessary shelter into purchasing a speculative, risky investment because it was believed to go up over time. A similar phenomenon occurred in cryptocurrency markets. Originally valued at approximately the cost of the processing power to ensure the validity of the transaction, cryptocurrencies like Bitcoin skyrocketed as investors thought "it could only go up." It quickly deviated from this price and climbed to new heights. As there is no fundamental backing of the value of cryptocurrency, the price of Bitcoin and other coins fluctuated wildly based on demand. Speculation rather than investment became the fundamental driving force of Bitcoin's price.

As the speculative bubble grew, people began using leverage to increase the variance of their trades and hopefully generate massive profits. Platforms like Robinhood began allowing users to get cheap leverage in the pursuit of returns. When the bubble burst, small drops in the Bitcoin price caused some investors to get margin calls due to their leverage ratios. Similarly, in the financial crisis of 2008, use of leverage caused banks to fail after small deviations in the price of their mortgage-backed securities. During this time, Lehman Brothers was levered at a ratio of approximately 30-to-1. When MBS valuations fell 3%, Lehman Brothers went bankrupt. The decay of investment towards speculation, in both of these cases, was highly detrimental to investors and caused the loss of billions of dollars.

One of the major differences in the cases of the cryptocurrency crisis and the subprime crisis is the involvement of the Federal Reserve. The Federal Reserve is known as the “lender of last resort” and is the final backstop in the case of financial ruin. The Federal Reserve has significant control over fiat currency, and can use monetary policy in order to control inflation and unemployment.

To combat inflation, the Federal Reserve may use contractionary monetary policy, which involves reducing the money supply and raising interest rates. This makes borrowing more expensive, which in turn can lead to a decrease in consumer spending and business investment. With less money in circulation, inflationary pressures may ease. On the other hand, to combat unemployment, the Federal Reserve may use expansionary monetary policy, which involves increasing the money supply and lowering interest rates. This makes borrowing cheaper, which can encourage consumer spending and business investment. With more money in circulation, economic activity may increase, leading to more job creation.

The Federal Reserve also uses other tools, such as open market operations (buying and selling government securities), reserve requirements (the amount of money banks must keep in reserve), and discount rates (the interest rate at which banks can borrow from the Federal Reserve), to influence the economy and achieve its policy goals. Cryptocurrency does not allow for these same types of actions, as the supply is fixed or is a function of some decentralized systems. Although proponents of cryptocurrency argue that this is beneficial as it doesn’t allow for money to be created, devaluing the cryptocurrency, opponents argue that monetary policy allows for the government to assist in times of financial ruin. The latter is impossible to do with Bitcoin and other cryptocurrencies.

The Federal Reserve has acknowledged the emergence of cryptocurrencies and is closely monitoring their development. However, its official stance on cryptocurrencies is that they are not considered legal tender, and the Federal Reserve does not endorse any particular cryptocurrency. The Federal Reserve has also expressed concerns about the potential risks associated with cryptocurrencies, such as their high volatility, lack of consumer protection, and potential use for illicit activities such as money laundering and terrorist financing.

During the cryptocurrency crash of 2022, the Federal Reserve did not intervene in order to bolster the cryptocurrency market. On the contrary, in the case of the subprime lending crisis, the Federal Reserve lowered the federal funds rate, which is the interest rate at which banks lend money to each other overnight. By lowering this rate, the Federal Reserve hoped to make borrowing cheaper and stimulate economic activity. The Federal Reserve also lowered the discount rate, which is the interest rate at which banks can borrow money directly from the Federal Reserve. In addition, the Federal Reserve provided liquidity to the financial system by lending money directly to banks and other financial institutions, as well as purchasing mortgage-backed securities and other assets. The Federal Reserve also worked with other government agencies to establish programs aimed at preventing foreclosures and supporting the housing market.

References

[1] Ritter, Joseph A. "The Transition from Barter to Fiat Money." *The American Economic Review*, vol. 85, no. 1, 1995, pp. 134–49. *JSTOR*, http://www.jstor.org/stable/2118000. Accessed 27 Mar. 2023.

[2] Chapman, Anne. "Barter as a Universal Mode of Exchange." *L'Homme*, vol. 20, no. 3, 1980, pp. 33–83. *JSTOR*, http://www.jstor.org/stable/25131676. Accessed 27 Mar. 2023.

[3] Andrei, Liviu. (2011). Fiat versus Representative Money under Debate, or How Right Keynes Was Once (!). Theoretical and Applied Economics. XVIII(2011). 45-58.

[4] Mankiw, N.G. *Principles of Economics*, 7th edn. (Cengage Learning, Stamford, CT, 2015)

[5] Antonopoulos, Andreas M. 2014. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies* (1st. ed.). O'Reilly Media, Inc.

[6] Fitzpatrick, Scott M. "Archaeological Investigation of Omis Cave: A Yapese Stone Money Quarry in Palau." *Archaeology in Oceania*, vol. 36, no. 3, 2001, pp. 153–62. *JSTOR*, http://www.jstor.org/stable/40387204.

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

[8] Choi, Candice. n.d. “Crypto Crisis: A Timeline of Key Events.” WSJ. https://www.wsj.com/articles/crypto-crisis-a-timeline-of-key-events-11675519887.

[9] “Economic Well-Being Of U.S. Households in 2021.” *Federal Reserve Board Publication*, 2022.

[10] “Forrester Study Shows Accepting Crypto Attracts New Customers & Boosts AOV.” Bitpay, 6 Aug. 2020, bitpay.com/resources/forrester-report-says-bitpay-adds-new-sales-and-2x-aov/.

[11] “El Salvador’s law: a meaningful test for Bitcoin.” PwC, October 2021, https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf.

[12] “El Salvador Adopted Bitcoin As A National Currency. Here’s How It’s Going.” NBC News, 13 Apr 2022.

[13] Foley, Sean, et al. “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?” SSRN Electronic Journal, 2018, https://doi.org/10.2139/ssrn.3102645.