Crypto: A Currency for The People?

The founders of cryptocurrency promised revolution.
What they got fell far short of their lofty goals.

By Noel Anderson

Bitcoin. Dogecoin. Bored Apes. Blockchain. Meme coins. Crypto mining. NFTs. The onslaught of *crypto-verse* jargon is confusing and inaccessible to most of us. Few people understand what this terminology means, and even fewer understand how the underlying technology works, and yet it is common to hear people expound upon the amazing investment opportunity crypto offers *and* its potential to revolutionize nearly every aspect of our capitalist system — usually in that order.

So what *are* cryptocurrencies and NFTs, and how do they work? Will these technologies decentralize the internet, fundamentally challenge global banking, and put the power of currency back in the hands of "the people?" And more importantly, for some, should *you* be investing? Is this a once in a lifetime opportunity, or is it simply the latest bubble that, like a tulip, will flower then quickly die?

To answer these questions, we need to go back to the origins of cryptocurrency – to 2008, just before the recession.

Bitcoins and Bailouts

In 2008, the global economy was teetering on the edge of a precipice, as a direct result of the 1999 repeal of portions of the 1933 Banking Act, known as the Glass-Steagall Act.[1] These repeals allowed financial institutions to engage in more lucrative and riskier speculative operations, such as “predatory lending.”[2] Predatory lending is the making of loans to low income families who could not pay the interest. These loans were often mortgages that leveraged the family's house as collateral; because of the housing bubble, the price of homes and thus the size of the loans could be huge.[3]

---

[1] Maverick, J.B. (October 22, 2019). “Consequences of The Glass-Steagall Act Repeal.” Investopedia. Retrieved 16 May 2021. https://www.investopedia.com/ask/answers/050515/did-repeal-glasssteagall-act-contribute-2008-financial-crisis.asp

[2] O'Connell, Brian (May 9, 2019). “What Is Predatory Lending?” TheStreet. https://www.thestreet.com/personal-finance/mortgages/what-is-predatory-lending-14953861

[3] According to a 2020 paper, “Arguably the largest contributor to the conditions necessary for financial collapse was the rapid development in predatory financial products which targeted low-income, low-information homebuyers who largely belonged to racial minorities,”

These "subprime mortgages" were risky and likely to default. But the banks had colluded with credit rating agencies like Standard & Poor's, to deceptively give the mortgages the most favorable risk rating: AAA. By falsely categorizing these loans as low-risk, the banks could now aggregate the loans and sell them to investors as "mortgage-backed securities." The investor would purchase the mortgage debt from the bank and then slowly make a profit as the mortgage was paid off with interest. When the housing bubble burst and the mortgages began to default, the investors lost their money, the homeowners lost their homes, and the financial crisis ensued.[4]

In the immediate aftermath of the financial collapse, the Obama administration rushed to pass legislation designed to help the US economy recover. This legislation included enormous bailouts for the banks. Rather than punish the organizations and people that caused the financial crisis, the Obama administration decided that these banks were "too big to fail." The bailouts were seen by many, on both the left *and* right wings of the political spectrum, as a clear sign of corruption in the global economic and political system.

On the political left, the financial crisis and the bailouts were explained as the product of unchecked capitalism, the revolving door between regulators and private business, and regulatory capture. The bailouts were a classic example of the collectivization of risk and privatization of profit: the bankers make money and the taxpayers bail them out when the economy crashes. This sentiment was dramatically expressed through the Occupy Wall Street movement, which focused attention on income and wealth inequality in the US with the slogan "we are the 99%."

On the political right, similar complaints took on a more libertarian bent. The financial collapse was not caused by too *little* regulation, they argued. Rather, it was caused by too much. A truly free capitalist market would have let the banks crash and burn. When the Obama administration decided to bail out the banks, it was preventing the free market from punishing the bad actors. As Conservapedia, *The Trustworthy Encyclopedia, s*tates when describing the bailouts,

> "Rather than investing in corrupt and inefficient businesses due to political considerations, given the relative greater efficiency and dynamism of capitalism, the Obama administration should have allowed capitalist forces to cause a more rapid and efficient allocation of economic resources. Allowing market forces to allocate resources instead of government bureaucrats to allocate economic resources due to political considerations would have caused the United States economy to recover more rapidly."[5]

Sarra, Janis; Wade, Cheryl L. (July 2020). *Predatory Lending Practices Prior to the Global Financial Crisis*. *Predatory Lending and the Destruction of the African-American Dream*. pp. 23–68. doi:10.1017/9781108865715.004. Retrieved 18 May 2022.

[4] While this is admittedly an oversimplification, it is more than adequate for our purposes.

[5] "Obama administration corporate bailouts," Conservapedia: The Trustworthy Encyclopedia, Accessed 16 May. https://www.conservapedia.com/Obama_administration_corporate_bailouts

It was into this stew of anti-bank, anti-establishment sentiment that Bitcoin emerged, promising a decentralized alternative to the international monetary system that had failed so dramatically.

The proponents offered Bitcoin as a new kind of monetary system, with a different kind of currency – cryptocurrency – which would exist outside of the traditional financial institutions. It would be controlled not by big banks and the government but by the users themselves. It would be anonymous, free from taxes, regulation, corporate corruption, and government manipulation.[6] As the UK software engineer Stephen Diehl documents, a distrust of government interference in financial markets, resulting from the bailouts, makes up the fundamental ideological justification underpinning cryptocurrencies.[7]

Cryptocurrencies, advocates declared, had the potential to be a revolutionary force. A cryptocurrency built on a decentralized Blockchain would be untraceable and immune to the influence of meddling governments, who would be unable to devalue the currency, enforce trade laws or collect taxes. Banks would become redundant and unnecessary, because transactions could be made peer to peer, across any border. The power of a decentralized currency could be used to threaten corrupt governments, by denying them income from taxation. And as decentralized Blockchain technologies grew more advanced, they could fundamentally restructure society by challenging big business, providing funding to the arts, and solving climate change.[8] The possibilities were endless.[9] [10]

With all these advantages, it was clear to crypto supporters that Bitcoin would soon replace the dollar. “Bitcoin is definitely more than a get-rich scheme. I think it's the next big technology that will revolutionize our society. It's as big as the internet – or maybe bigger,” one early investor told a reporter.[11] But in order to understand how all of this was supposed to work, we need to understand the underlying technology: the Blockchain.

---

[6] Garcia, Evan. “Bigger than Bitcoin: The Revolutionary Potential of Blockchain Technology.” WTTW News, January 16, 2018. Retrieved May 23, 2022, from https://news.wttw.com/2018/01/16/bigger-bitcoin-revolutionary-potential-blockchain-technology.

[7] Diehl, Stephen. “The Intellectual Incoherence of Cryptoassets.” stephendiehl. Accessed May 23, 2022. https://www.stephendiehl.com/blog/crypto-absurd.html.

[8] A recent blockchain-based platform Celo even claims to be capable of offsetting “nearly 20% of all US emissions.” The Celo Foundation. “A Carbon Negative Blockchain? It's Here and It's Celo.” Medium. The Celo Blog, May 28, 2021. Retrieved May 23, 2022, from https://medium.com/celoorg/a-carbon-negative-blockchain-its-here-and-it-s-celo-60228de36490.

[9] Gibbons, S. (2022, January 17). *10 ways cryptocurrency will make the world a better place*. DUE. Retrieved May 23, 2022, from https://due.com/blog/cryptocurrency-will-make-world-a-better-place/#6_Keep_companies_and_individuals_accountable

[10] Russo, Camila. *The Infinite Machine: How an Army of Crypto-Hackers Is Building the next Internet with Ethereum*. HarperBusiness, 2020.

[11] Ball, James. “Silk Road: The Online Drug Marketplace That Officials Seem Powerless to Stop.” The Guardian. Guardian News and Media, March 22, 2013. Retrieved May 23, 2022, from https://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace

BlockChain: Crowd-Sourced Accounting

A Blockchain is basically a public ledger book, an agreed-upon record that everyone can look at. The technology allows a decentralized group of individuals (a network of peers) who do not necessarily know or trust each other to agree on the state of the common ledger. Blockchains are also immutable; once something has been written in a blockchain, it cannot be erased.

For cryptocurrencies, the blockchain acts as a complete history of every transaction ever made. If you want to pay seven crypto coins to another account, you simply add a line to the ledger book stating the transaction. Then everyone else on the network will know that you have seven fewer coins and the account you paid has seven more. Using this blockchain history, everyone on the network can determine how many coins each account has, without having to rely on actual physical coins.

You might be imagining the ledger book, or Blockchain, as a shared document on the cloud that everyone has access to. But this would require the network to trust whatever database was storing the document. Instead, there is no central storage of the blockchain. Each user keeps their own copy of the blockchain and updates it privately. To make a payment, you must broadcast the new transaction to the network of users, and each user must then append it to the end of their own copy of the blockchain.

You might worry that this allows bad actors to make payments from accounts that are not theirs. What prevents Bob from broadcasting to the network that “Alice pays Bob 10 coins?” A simple piece of cryptography prevents this type of fraud. When you create a blockchain account, also known as a wallet or crypto wallet, you are given a public key/private key pair. This pair allows users to uniquely sign transactions with a “digital signature.” A payment that does not carry the appropriate digital signature is considered invalid. This ensures that only someone who knows the private key can make payments from the associated wallet.

You might also be wondering how we can ensure that everyone on the network is updating their own copy of the ledger, their own blockchain, in the same way. With no central ledger, this process is almost guaranteed to run into problems. Maybe one part of the network does not hear a particular transaction, someone might forget to add a transaction, two dependent transactions could be recorded in different orders by different parts of the network, or one of the broadcast messages could simply become corrupted as it traverses the internet. How do you reconcile conflicting ledgers?

This is the central problem that blockchains address: how to choose between conflicting ledgers so that everyone can agree on the same ledger. This is where the second piece of cryptography comes into play. Rather than adding single transactions to the Blockchain one at a time, transactions are added in groups known as blocks. Anyone on the network can listen for transactions and gather them together into a block. But the block is not considered “valid” until they find the solution to a very difficult computational problem.

The computational problem is based on a cryptographic hash function and depends on the contents of the new block and all the previous blocks. Slight changes in the contents of any block drastically change the solution. Once someone on the network finds a solution to a new block, they broadcast the block along with the solution to the network. While it takes a lot of computational work to find a solution, it is quite easy to check that a solution is valid. So, when a user receives a new block, they can easily check that the solution is valid. If it is, they add the new block to their record, and it becomes the next segment of the immutable blockchain.

This process of gathering together transactions into a block, solving the associated computational problem, and broadcasting the block and solution is called mining. As a reward for their work, miners are allowed to add a bonus transaction at the end of each block they mine which adds a small amount of cryptocurrency to their own wallet. As soon as the new block is mined, the miners all begin mining the next block, competing to be the first to find a solution and earn the reward.[12]

Finally, if there is a conflict between two different versions of the blockchain, the rule is that the network defers to the longer chain. This rule provides a way to choose between conflicting versions of the blockchain.

To see why this system works, it is helpful to imagine what it would take to trick the system. Imagine Bob wants to trick Alice into thinking that he has paid her 50 coins when he hasn't. If Bob actually wanted to pay Alice, he would broadcast to the network “Bob pays Alice 50 coins.” As soon as Alice received a valid block containing the transaction, she would know the transaction had gone through and the rest of the network had acknowledged Bob's payment to her.

But if Bob was trying to be tricky, rather than broadcasting the transaction to the entire network, he could instead privately mine his own block, including the fake payment to Alice. After finding a solution, Bob could send the new block to Alice, hoping to convince her that he had paid her. But since no one else on the network would know about the transaction, they would all think Bob still had the 50 coins. Bob would be free to spend them on the rest of the network.

While this may initially trick Alice, in order to continue the deception, Bob would have to keep adding new blocks to the end of his fraudulent chain and sending them to Alice. If he did not, the blockchain being worked on by the rest of the network would soon grow longer than Bob’s, and Alice would defer to it instead. And the longer blockchain would not include Bob's payment to Alice, so she would (eventually) know that she had been tricked. The purpose of all the computational effort that goes into mining new blocks is to prevent Bob from creating a long enough blockchain to trick Alice. Because it takes so much computational work to mine each new block, Bob would never be able to keep his fraudulent chain longer than the real chain,

[12] If you have heard of the large CO2 emissions associated with cryptocurrencies, this competition to mine blocks is the source: computers use a lot of energy and because crypto mining is a winner take all game, bigger faster more energy intensive computers are always better at making money.

which is being worked on by the rest of the entire network. If Alice simply waited for a few more blocks to be added after the block containing Bob's payment to her, she would be able to tell whether the payment was real.

Forcing the network to spend lots of computational power to mine each new block ensures that no individual can trick the system. The longest chain will always be the chain with the most computational power being put into it. So by choosing the longest chain, you are deferring to the blockchain that the vast majority of the network has agreed upon.

Early Crypto: Ecstasy and Extortion

So with all the revolutionary potential of crypto, how has it turned out? Initially, one Bitcoin cost nine cents, but there was basically nothing you could do with it and it was virtually useless.[13] This changed in 2011 with the creation of the Silk Road, an online marketplace that accepted Bitcoin. Much like Amazon, the Silk Road allowed buyers to purchase items and rate and review sellers. But unlike Amazon, the Silk Road was located on the dark web. According to the website's terms of service, written by the founder, the pseudonymous *Dread Pirate Roberts*, the Silk Road prohibited the sale of anything that would "harm or defraud" customers. This included "stolen credit cards, assassinations… weapons of mass destruction," and child pornography.[14] Items *not* prohibited by the Silk Road were sold under the headings of "Books," "Opioids," "Art," "Stimulants," "Apparel," "Ecstasy," "Home & Garden," "Psychedelics," "Fake IDs," and others.[15] [16] Now that Bitcoin could be used to buy drugs, its price rose to over $200 per coin.[17]

Some crypto enthusiasts supported this use of Bitcoin, arguing that it was supporting a true open market:

> "People want drugs. The drug war is probably a failed war [and] I want to get rid of cartels. The way to do that is for people to buy their drugs straight from the producer. That's what's cool about things like Silk Road – you can bypass gangs."[18]

---

[13] Edwards, John. "Bitcoin's Price History." Investopedia, May 13, 2022. Retrieved May 23, 2022, from https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.
[14] Gayathri, Amrutha. "From Marijuana to LSD, Now Illegal Drugs Delivered on Your Doorstep." International Business Times, December 11, 2012. Retrieved May 23, 2022, from https://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021.
[15] Norrie, Justin, and Asher Moses. "Drugs Bought with Virtual Cash." The Sydney Morning Herald. The Sydney Morning Herald, June 11, 2011. https://www.smh.com.au/technology/drugs-bought-with-virtual-cash-20110611-1fy0a.html.
[16] Ball. "Silk Road." The Guardian.
[17] Edwards. "Bitcoin's Price History." Investopedia.
[18] Ball. "Silk Road." The Guardian.

But in 2013 the FBI shut down the website and arrested its founder Ross Ulbricht, aka the *Dread Pirate Roberts.* The price of Bitcoin, and other cryptocurrencies, plunged.[19]

During the next few years, one of the primary uses for cryptocurrencies, especially Bitcoin, was in facilitating ransomware attacks. In a ransomware attack, the attacker gains access to your computer before locking all your files. They then refuse to unlock the files or threaten to publish them on the internet unless a ransom is paid, usually payable only in Bitcoin. Total ransomware payments increased 311% in 2020, reaching a total of $360 million in cryptocurrencies.[20] These numbers are projected to continue rising.[21]

Then in late 2020, as the economy shut down due to Covid, interest in cryptocurrencies saw a resurgence. Egged on by the IPO[22] of Coinbase, a popular cryptocurrency exchange platform, the price of Bitcoin hit an all-time high of $68,789.[23] Other cryptocurrencies also saw their prices increase. Ether, the second most popular cryptocurrency after Bitcoin, reached a price of $4,426.[24]

But even as the price rose and interest around these coins increased, cryptocurrencies still had very few real world uses. Most stores simply won't accept crypto, so the average user can't buy coffee or groceries with crypto. Additionally, the price of most cryptocurrencies is far too volatile for daily use: Your Bitcoin might be valued at $100 in the morning but by the time you're ready to buy groceries in the afternoon, the value could have dropped to $30.

In addition to the fluctuations in price, the technology underlying crypto is self-limiting. Crypto users realized relatively early on that Bitcoin and other decentralized cryptocurrencies could never handle the scale of transactions needed for them to become a *real* usable currency. Currently, it takes six hours of continuous mining for Bitcoin to process the number of transactions that Visa processes in one minute – and Visa is just one of many credit card companies operating globally. Bitcoin simply can't accommodate the volume of global financial transactions.[25]

---

[19] Edwards. "Bitcoin's Price History." Investopedia.
[20] "Cryptocurrency Based Ransomware Attacks Went up in 2020: Report." MSN. The Financial Express, May 14, 2021. https://www.msn.com/en-in/news/world/cryptocurrency-based-ransomware-attacks-went-up-in-2020-report/ar-AAXgcjX.
[21] Clark, Mitchell. "US Treasury Says Ransomware Payouts in 2021 Could Top Entire Past Decade." The Verge. The Verge, October 15, 2021. https://www.theverge.com/2021/10/15/22728765/us-treasury-ransomware-payout-numbers-reports-2021-first-half-cybercrime.
[22] An IPO or Initial Public Offering is when a company first sells stocks on the stock market.
[23] Edwards. "Bitcoin's Price History." Investopedia.
[24] Best, Raynor de. "Ethereum Price History 2015-2022." Statista, May 19, 2022. https://www.statista.com/statistics/806453/price-of-ethereum/.
[25] Olson, Dan. "Line Goes up – the Problem with Nfts." Folding Ideas, January 21, 2022. https://www.youtube.com/watch?v=YQ_xWvX1n9g&t=1381s.

But these issues didn't stop investors from continuing to pour money into crypto. We now enter the modern era of crypto, one dominated by fraudsters, scammers, and grifters.

Current Crypto: A Playground for Grifters and Scammers

In the early days, crypto touted lofty goals of democratizing finance and decentralizing economic power. But crypto in its current form leaves these goals behind. Cryptocurrencies are not actually currencies. Almost no stores will accept them, and after the FBI shut down the Silk Road you can't even use them to buy drugs. This is not a hidden aspect of crypto: "[No one is actually buying Bitcoin] because they expect to be able to go to the store and spend it. [They are buying Bitcoin] because they expect it to hold its value," the Director of Data and Indexes at the crypto reporting agency CoinDesk said in an interview with Time.[26] Rather than functioning as a currency, cryptocurrencies have become financial assets: investors purchase cryptocurrencies for the sole purpose of selling them later for more money. This is known as a "bigger fools" game: in order to make money, each investor must find a "bigger fool" who will buy the asset off them for more money. The new investor must then find an even bigger fool who in turn must find a yet bigger fool. It's like a game of hot potato, where the potato is passed from person to person as fast as possible until the music stops and one unfortunate player is left holding the potato, which (metaphorically) burns their hands. In crypto, it all ends when the last fool, the biggest fool, can find no one else to sell it to. Without a buyer, they are left with a meaningless, valueless asset. The system works somewhat like a pyramid scheme. In fact, some commentators have described cryptocurrency as a "pyramid scheme for men," noting that while pyramid schemes typically target women, crypto scams primarily target men.[27]

Much of the hype around crypto is a product of grifters trying to pull this type of scam. An entrepreneur, or scammer, creates a cryptocurrency and purchases advertisements and celebrity endorsements in order to hype up their coin.[28] The early investors also help hype the coin. If they don't, they will be unable to find anyone to buy the coins from them and they will lose their investment. All the hype generates interest around the coin, and when the price begins to rise, the early investors begin to sell. But as soon as the hype train comes to a stop — either because the celebrity endorsements are no longer generating publicity or because everyone has realized that the coins are entirely useless — the price crashes because the crypto assets have no underlying value. As long as the grifters can get out before the crash, they make a profit, but the gullible buyers are left with nothing.

There are a number of common ways that scammers pump up the price of a cryptocurrency. One of these involves setting up multiple accounts and then trading the currency back and forth

---

[26] Haar, Ryan. "Should You Buy Things with Crypto? Here's Why You Shouldn't." Time, May 3, 2022. https://time.com/nextadvisor/investing/cryptocurrency/should-you-use-crypto-like-cash/.

[27] "An Honest Conversation on the Problem with Nfts & Cryptocurrency." YouTube. The Financial Diet, February 7, 2022. https://www.youtube.com/watch?v=8St36RjHd2E&t=1604s.

[28] Usually, these schemes also rely on portraying the new coin as somehow unique. It might employ slightly different design choices and other coins or it might be associated to some up-and-coming business. In either case this helps the coin stand out from the crowd.

between the accounts. Each time the scammer transfers the crypto, he raises the price. To an outside observer seeing all this activity, it looks like there is a lot of interest in the coin; since the price keeps going up, they should definitely invest. But as soon as others begin to buy, the scammer sells all his crypto, and the price tanks because there was never any real demand for the currency. Luckily for the scammer, they have already made their money. This is called wash trading; in standard asset markets, wash trading is a form of securities fraud, made illegal in 1936.[29] But the crypto market is not a standard asset market. Cryptocurrencies have escaped regulation. The whole point is that it is a market free from regulations and government interference. So grifters are free to wash trade as much as they want. In fact, a 2021 study by Cornell, researchers estimated that 70% of the total volume in cryptocurrency trading was wash trading.[30] [31]

Wash trading is not the only method crypto scammers use to scam less knowledgeable investors. They also hype up technologies, usually somehow related to the Blockchain, and by the time later investors realize that the technology is going nowhere, the crypto grifters have already made off with a bucket load of money. A perfect example of this is NFTs. NFTs, or non-fungible tokens, are marketed as a way for people to own digital *things* and for artists to make money off digital art. But as soon as you begin to dig into NFTs you realize they do almost nothing that they claim to and usually are just another way for crypto scammers to take your money. Let me explain.

NFTs primarily rely on the Ethereum blockchain. While the Bitcoin blockchain can only store information about Bitcoin transactions, the Ethereum blockchain is more advanced. It can store almost any kind of information in its immutable ledger. When it was first constructed, its developers imagined the Ethereum blockchain acting as an immutable public library, storing everything from land deeds and government documents to news articles and medical records. It was supposed to form the backbone of a new, freer internet: a place where information could be stored permanently, secure from government censorship and interference, where free speech was enshrined in the fundamental architecture of the system. Luckily for the privacy of our medical records, this never came to pass. Instead, like the Bitcoin blockchain, the Ethereum blockchain is mainly used to record cryptocurrency transactions. However, this more advanced form of blockchain does allow for the creation, or minting, of NFTs.[32]

The way that NFTs are usually described is that they take advantage of the data storage ability of modern blockchains to place an image on the blockchain. The image can then be traded and sold between accounts, leaving a record of who owns it, just like with cryptocurrencies. But unlike cryptocurrencies, the image is *non-fungible*. Bitcoins are *fungible*: it doesn't matter which

---

[29] Chen, James. “Wash Trading Definition.” Investopedia, May 11, 2022. https://www.investopedia.com/terms/w/washtrading.asp.

[30] Cong, Lin W. “Crypto Wash Trading: Crypto and Blockchain Economics Research Forum.” CBER Forum. Crypto and Blockchain Economics Rezearch Forum. Accessed May 23, 2022. https://www.cber-forum.org/cryptowashtrading.

[31] Cong, Lin William, Xi Li, Ke Tang, and Yang Yang. "Crypto wash trading." *arXiv preprint arXiv:2108.10984* (2021). https://doi.org/10.48550/arXiv.2108.10984

[32] Russo, 2020.

Bitcoin you have, because they all have the same value (or lack thereof). But an NFT is nonfungible; each NFT is unique. While a description like this is common to hear, it is not how NFTs actually work.

It turns out that it is actually very expensive to put something on the blockchain. Just recording a cryptocurrency transaction can incur fees of over $100.[33] The fees required to put an entire image onto the Blockchain would be astronomical, and because of this, it's never done. Instead, the images are stored on private websites, and a URL that points to the page is placed on the blockchain. An NFT is not an image; it is a URL that links to an image.

This ushers in a whole new set of problems for digital ownership. First, anyone can go to the URL and look at the image. They can even right-click and copy the image. In addition, owning an NFT does not ensure that the link will continue to work. If the website or database that stores the image neglects to register its domain name, goes out of business, or simply stops displaying the image, then your NFT is gone. In addition, owning an NFT on one blockchain in no way prevents someone from owning the same NFT (a URL pointing to "your" image) on a different blockchain. It's not even clear if owning an NFT grants any legal rights to the image. In 2021, Christie's auction house sold a piece of digital art by the artist Beeple for $69 million.[34] In the 30-page terms of sale that accompanied the purchase, they acknowledged that owning the NFT did not grant any legal rights to the image:

> "You acknowledge that ownership of an NFT carries no rights, express or implied, other than property rights for the lot (specifically, digital artwork tokenized by the NFT).
>
> … You acknowledge and represent that there is substantial uncertainty as to the characterization of NFTs and other digital assets under applicable law."

In their very terms of sale, Christie's acknowledges that "buying" an NFT does not transfer ownership of the linked image. When you own an NFT, all you own is an entry on a blockchain that links to an image stored on a private server. It does not prevent other people from copying the image, removing the image, or even creating the same NFT on a different blockchain.

While some artists have actually made money off NFTs, the vast majority do not and instead are left owning a virtually useless URL stored on a Blockchain. But the grifters promote the few large sales, like the Christie's auction, to entice other artists to get into NFTs.[35] To add an NFT to the blockchain, the artist must pay a fee and the grifters are quick to gobble up this money. The

---

[33] "Gas Fees." Ethereum Gas Fees Tracker | Crypto.com DeFi Dashboard. Accessed May 23, 2022. https://crypto.com/defi/dashboard/gas-fees.
[34] Thaddeus-johns, Josie. "Beeple Brings Crypto to Christie's." The New York Times. The New York Times, February 24, 2021. https://www.nytimes.com/2021/02/24/arts/design/christies-beeple-nft.html.
[35] Gerard, David. "NFTs: Crypto Grifters Try to Scam Artists, Again." Attack of the 50 Foot Blockchain, March 11, 2021. https://davidgerard.co.uk/blockchain/2021/03/11/nfts-crypto-grifters-try-to-scam-artists-again/.

crypto exchanges that facilitate these interactions also take a cut of each transaction, and so everyone makes money – everyone *except* the artist.[36] [37]

In addition to being almost entirely a scam, cryptocurrencies have also left behind many of the lofty promises they made about decentralizing economic power. As investing in cryptocurrencies has become more popular, crypto exchanges like CoinBase have sprung up. These platforms make the process of interacting with the underlying blockchain more streamlined and allow less tech-savvy users to trade cryptocurrencies. However, they are almost entirely unregulated and are notorious for their questionable business practices. As Investopedia states,

"Cryptocurrency exchanges work similarly to a stock exchange, except crypto exchanges typically charge much higher transaction fees and lack reputable customer service. The exchanges have also been victims of cybercrime, sometimes in the billions of dollars."[38]

These exchanges also do away with any idea that trading crypto is anonymous. While it has always been possible to link crypto wallets to individuals or institutions, these crypto exchanges store lots of information about their users and make it far easier to connect individuals with accounts. In addition, as cryptocurrencies like Bitcoin became more expensive, miners were incentivized to build more and more powerful mining operations in order to claim the reward for mining the next block. This set off an "arms race" between miners. Today, crypto mining is dominated by the select few who can afford to build massive multi-million dollar mining operations.

One anecdote illustrates how today's cryptocurrency market replicates the same consolidation of power it was originally designed to challenge. In 2016, a number of wealthy investors attempted to set up a decentralized investment group using the Ethereum blockchain. To create the investment group, the founders wrote a set of rules which were recorded as computer code and put on the blockchain. In crypto jargon, this is what is known as a "Smart Contract." The code could then run on the blockchain and allowed anyone to transfer money into the decentralized investment group. The code also allowed investors to vote on the group's investment decisions. But almost immediately someone found a bug in the Smart Contract. And because the blockchain is immutable, no one could fix the code. Just days after the project launched, an unknown user took advantage of the bug to drain the entire investment fund of $50 million worth of cryptocurrency and transfer it into a private account.[39] [40]

---

[36] Castor, Amy. "Metakovan, the Mystery Beeple Art Buyer, and His NFT/Defi Scheme." Amy Castor, March 31, 2021. https://amycastor.com/2021/03/14/metakovan-the-mystery-beeple-art-buyer-and-his-nft-defi-scheme/.

[37] Dash, Anil. "NFTs Weren't Supposed to End like This." The Atlantic. Atlantic Media Company, April 2, 2021. https://www.theatlantic.com/ideas/archive/2021/04/nfts-werent-supposed-end-like/618488/.

[38] https://www.investopedia.com/tech/what-ether-it-same-ethereum/#toc-how-do-i-buy-ethereum-crypto

[39] "Ethereum Classic and Its Whole History." GetBlock.io. Accessed May 23, 2022. https://getblock.io/blog/ethereum-classic-and-its-whole-history/.

[40] Saddique, Adam. "Simply Explained: Ethereum Classic (ETC)." Cryptonary. Accessed May 23, 2022. https://www.cryptonary.com/cryptoschool/simply-explained-ethereum-classic-etc/.

Unsurprisingly, the wealthy investors were not happy at losing their investment. An average investor would be unable to do anything to recover the money. The "theft" was entirely legal: the rules of the organization were written explicitly in code, and the code had been followed exactly. And because the blockchain is immutable, the transaction could not be undone. But as the crypto community was about to learn, wealth will always find a way.[41]

In order to recover the transferred funds, the wealthy investors had to convince the entire Ethereum network to collectively revert to an earlier version of the blockchain, from before the money had been transferred. This was not supposed to be possible; in concept, it would be impossible to convince the entire network of users to revert to an earlier blockchain. This was the mechanism that was supposed to ensure immutability and protect the blockchain from political pressure and manipulation. But the mining operations for Ethereum had become so centralized that just a few individuals and organizations controlled most of it.[42]

The investors were able to use their wealth and connections to convince the centralized mining operations, about 80% of total mining operations, to erase the transfer and go back to a version of the blockchain. Just as in the traditional economy, wealthy individuals wield an outsized amount of power and can use it to manipulate crypto to their own ends.[43]

To Scam or Be Scammed?

Rather than dismantle the corrupt power structures of traditional finance, decentralized cryptocurrencies have simply created a new sphere where bad actors can throw around their weight. In many cases, these bad actors are the very same bad actors that control traditional financial markets: According to Forbes, "big money has taken over crypto."[44] According to research by Morgan Stanley, "institutional investors now account for more than two-thirds of trading volume in crypto."[45] Ultra wealthy individuals like Peter Thiel, the co-founder of PayPal, and the intelligence contractor Plantier, are also heavily investing in these technologies[46] Even Jordan Belford — the notorious stockbroker and felon who was convicted on multiple counts of money laundering and securities fraud in 1999 — has jumped on the crypto bandwagon.[47]

---

[41] "Ethereum Classic and Its Whole History." GetBlock.io.
[42] "Ethereum Classic and Its Whole History." GetBlock.io.
[43] Saddique. Cryptonary.
[44] Runkevicius, Dan. "'They Won't Be Immune' - the Fed's Stark Warning Sends the Price of Bitcoin, Ethereum, BNB, XRP, Solana, Cardano, and Dogecoin into Free Fall." Forbes. Forbes Magazine, April 25, 2022. https://www.forbes.com/sites/danrunkevicius/2022/04/22/they-wont-be-immune---the-feds-stark-warning-sends-the-price-of-bitcoin-ethereum-bnb-xrp-solana-cardano-and-dogecoin-into-free-fall/.
[45] Runkevicius, Forbes Magazine, 2022.
[46] Rizzo, Pete. "$100k Peter Thiel Fellowship Awarded to Ethereum's Vitalik Buterin." CoinDesk Latest Headlines RSS. CoinDesk, June 5, 2014. https://www.coindesk.com/markets/2014/06/05/100k-peter-thiel-fellowship-awarded-to-ethereums-vitalik-buterin/.
[47] Yaffe-bellany, David. "The Wolf of Crypto." The New York Times, April 15, 2022. https://www.nytimes.com/2022/04/15/technology/jordan-belfort-wolf-cryptocurrency.html.

Cryptocurrencies and decentralized technologies were supposed to take power away from the wealthy. They were supposed to decentralize global finance and democratize economic power. But this is not what they have done. Instead, the "free," unregulated market that crypto created has become a playground for grifters and scammers, where the most egregious forms of fraud run rampant.

The traditional financial system with its many flaws does have some regulations designed to protect those who are less well off. Cryptocurrencies, in the attempt to decentralize and democratize the economy, do away with all these regulations, good and bad. The result is a free market that the wealthy are "free" to manipulate at their leisure.

So, should you invest? Well, that depends on whether you think you'll be a grifter or a mark. You'll either lose your money or you'll take it from someone less lucky than you. You'll be a sucker or a thief. Personally, I wouldn't want to be either.

Additional Sources

A project documenting the mostly failed attempt to build a new type of internet known as Web3. This is usually associated with ideas of digital ownership, digital identity verification, and the metaverse.

White, Molly. "Web3 Is Going Just Great." Accessed May 23, 2022. https://web3isgoinggreat.com/.

More about Web3:

"The Third Web." Nodes in a social network, March 11, 2022. https://tante.cc/2021/12/17/the-third-web/.

More about the reality of Blockchain technology:

White, Molly. "Blockchain-Based Systems Are Not What They Say They Are." Molly White, January 9, 2022. https://blog.mollywhite.net/blockchains-are-not-what-they-say/.

More documentation of fraudulent business practices:

Golumbia, David. “Cryptocurrency Is Garbage. so Is Blockchain.” Medium. Medium, February 10, 2022. https://davidgolumbia.medium.com/cryptocurrency-is-garbage-so-is-blockchain-3e80078e77fe.

A bit more about decentralized finance, also known as DeFi, another blockchain application:

Gerard, David. “Libra Shrugged - Chapter 6: Banking the Unbanked.” Attack of the 50 Foot Blockchain, February 12, 2021. https://davidgerard.co.uk/blockchain/2021/02/12/libra-shrugged-chapter-6-banking-the-unbanked/.