Decrypting Crypto: Bitcoin and NFTs

Midnight Facts for Insomniacs

Podcast Transcript

(Note: transcript consists of episode outline)

So just to get this out of the way, we're not endorsing Bitcoin at all. Neither of us owns a Bitcoin. Or I should say, fraction of a bitcoin. Because right now, one bitcoin is worth about $35,000, and a few months ago it was worth twice that. I don't know about you, but I don't personally have the cost of an entire Tesla to

drop on a virtual asset with a dollar value that on a day to day basis looks like a heart monitor. Exchanging your money for cryptocurrency is straight up gambling. The one thing I will say is that you shouldn't invest any money that you actually NEED in cryptocurrency. Use fun money, if you're lucky enough to have that. If you're fancy. It's true that if you had purchased bitcoin years ago, you could very well be rich right now, it's also true if you purchased bitcoin last week, you would already have lost half of your investment. I'm imagining people who bought bitcoin this week like those old cartoon characters, walking around wearing just a barrel with suspenders. I've always loved that image, I like the idea that some guy runs out of money playing blackjack and is like, "I don't have any more money...do you accept pants?" So my point is that

this is not the typical crypto podcast with a couple of bitcoin evangelists trying to get you to invest. And we're also not anti Bitcoin. We're Bitcoin agnostic. We don't care what you do with your money. The lesser known MFFI motto: you do you. Knowledge is power, rationality is overrated. Hey, I've invested in terrible relationships, so who am I to talk? If time is money I've wasted a fortune on nice boobs.

To understand cryptocurrency, it helps to understand how money actually works

Money is a unique human creation, in that it requires consensus and agreement. Money only has value because we've all decided that it does. We've agreed that these particular pieces of paper can be exchanged for everything from an

iPhone to an animal, to a house. That's amazing to think about, that you can exchange pieces of dirty paper for a house or a creature. People will mow your lawn or clean your house or have sex with you or kill someone for pieces of paper. People will treat you differently based on how many pieces of paper you have. "You want me to be nice to you? Well, what's your paper situation? How many pieces of ground up and dried-up tree-pulp are you carrying?" Now, money didn't have to be paper, it could've been anything. Among some of the accepted forms of currency in history: salt—from which we get the word salary—bricks of compressed tea in Asia, and Parmesan cheese. In the region of Italy called Emilia-Romagna, wheels of genuine Parmesan cheese to this day can be used as collateral for bank loans. It

sounds silly except that look, when you think about it, cheese is intrinsically more valuable than paper. See what I'm saying? If I'm stuck in the wilderness, I'll give you 1 million dollars for a chunk of cheese. My kingdom for a mozzarella stick. Or some string cheese...mmm. But it's funny because many of these cryptocurrencies that we're going to talk about have often been mocked for being "made up," as if the value of green pieces of paper isn't made up. Most modern currency is made up. And it's kind of amazing that different pieces of paper with different markings have massively different values. A green piece of paper with a single vertical line on it, that's not worth much. That's just one dollar. Add two circles after that line, it's worth 100 times as much. Why? because zeroes add value. Even though a zero

actually signifies something that is worth nothing, but if you put two nothings after a straight line, it's worth 100 times as much as one straight line. It's all perfectly rational.

So as we established, there have been multiple types of currency through the ages, and multiple *categories* of currency. Commodity money is money that intrinsically has value based on the fact that it's made of a commodity. Solid gold coins are an obvious example, of course, but also as we've mentioned: tea and salt and cheese, and if you think about it, even today there are commodity currencies within the larger economy. In prison, cigarettes have traditionally been a commodity currency. You can exchange them for favors or other useful items. Like, your life. That's useful. So commodity currencies were the first forms of

money, and were eventually replaced by *representative* currency. Which can be anything, it can be paper or cardboard etc, but it always *represents* a commodity. And it can usually be exchanged in a bank for a certain quantity of that commodity. It sounds more confusing than it is. The common example is the gold standard. For many years in America, paper currency actually represented a certain weight of gold. So every paper dollar represented a dollar's worth of gold sitting in a bank somewhere, but no one wants to carry around heavy ass gold, so it makes more sense to carry around paper that represents that gold. Except of course now every rapper and showboating jackass in the world is obsessed with bling, voluntarily carrying pounds of gold, so we've come full

circle. It's like, we come up with a better system that makes our lives easier and then our lives become so easy that easiness loses its value and now it's cool to make your life difficult. This is actually supply and demand and it's the foundation of this episode, as we'll see. So back when we were on the gold standard in this country, you could actually take a dollar bill into a bank and exchange it for the equivalent amount of gold. A fraction of a flake. You can't do that anymore. But I encourage you to try. Just bring a dollar into a bank and demand a dollars worth of gold, and report back. The gold standard actually came after the silver standard; silver was the original gold. America adopted the silver standard in 1795, and officially switched to gold in 1900. But when the depression hit, Americans lost faith in paper

money and began frantically exchanging their greenbacks for gold, and hoarding gold, and as a result the gold standard was officially abandoned in 1933. “On April 20, FDR ordered Americans to turn in their gold in exchange for dollars to prohibit the hoarding of gold and the redemption of gold by other countries. This created the gold reserves at Fort Knox. The United States soon held the world's largest supply of gold.” It’s good to be the government. “I hereby decree that you all need to bring me your gold, and in return I shall give you some green paper with writing on it, and you can trade those green pieces of paper amongst yourselves, and I’m just going to be over here taking care of all your gold and keeping it safe. You’re welcome.”

Now, the gold standard does have the advantage of tying currency to something

tangible, which limits the amount of money a country can print—because you can't print more money than the amount of gold you possess--which in turn helps to control inflation. Inflation is when there's more currency floating around in the economy than the total value of goods and services to be purchased, it's just a supply and demand issue, when we all have a bunch of money in our pockets and we're all competing to buy the same goods, the value of those goods goes up and the purchasing power of your dollar goes down. So if the number of dollars in circulation is limited by the amount of gold, or mozzarella cheese or whatever, there's less inflation. But the gold standard also has the Smaug effect, the dragon effect, countries become creepy hoarders of gold and

if massive reserves of gold are discovered somewhere in the world, it affects the entire world economy. What if tomorrow a meteor shower hit the earth loaded with gold, it would rock the entire world economy. What if chemists finally cracked the alchemy code and found a way to manufacture gold? We did it with diamonds, it could happen. So we need a form of currency that's not attached to some particular substance. The word substance always sounds kind of gross. I don't know why I used it. It's technically accurate, but it sounds like saliva-based currency or something.

So now we have a fiat currency, which only has value because we say so. Fiat currency does not represent any commodity, instead it represents compact European two-door sedans. No. It just has value based on consensus. But fiat

currency comes with dangers as well, because it means a country can print as much money as it chooses to print. You're not limited by the amount of gold in Fort Knox, or the amount of cheese in cheeseville. And now we're back to the dangers of inflation.

So every type of currency has advantages and disadvantages, and crypto is no different.

If you're someone who has scoffed at crypto, I think it's important to point out that Digital currency is not weird or new at all. Currency in video games is digital currency. If you earn in-game money playing a game and then buy a sword or a magical loincloth or whatever, that's a digital transaction. And of course credit card transactions are digital. Bank transfers and debit card transactions and

bank accounts are all just numbers in the ether. Most of the money in the world is digital and exists only as bits of data. When you buy a Big Mac via credit card, the number representing your bank account balance ticks slightly down and the number in McDonald's banks account ticks slightly up, and zero paper is involved. And the number representing your cholesterol also slightly increases, and the number of days until your death decreases. So the point is that digital currency isn't some radical new idea. There are only two real differences between digital banking/credit, and cryptocurrency. One is that crypto is not sanctioned or backed by any official government, which means it's mostly unregulated, and the other is the blockchain. And we'll get to that shortly.

So in order to explain bitcoin, let's recap. For money to work, there has to be a limited amount of it. The law of supply and demand tells us that if there's an infinite supply of something, it has no monetary value. I can't sell you stupidity because there's plenty of stupidity for everyone, so no one would be willing to buy it unless they already had even more stupidity than pretty much everyone else. I can't sell you air, unless you've already bought some of that extra stupidity. Although I guarantee there is someone who will try to sell you air. If you want to waste your money on a commodity with zero value, you can do that, it's a free country. And it's a free country full of scammers, so even if you don't *want* to waste your money, there are plenty of people who will try to make that happen. But typically we

all agree that anything with infinite supply has zero value. Same with currency; if you try to give me a dollar bill to buy a beer, but I have a printing press in my basement and can print as many dollar bills as I want, my beer is worth way more to me than your dollar. So you have to find something that I want as much as you want a beer. And now we're back to a bartering economy, swapping commodities like goddam savages, and you would think a guy with a bunch of beer would be in a better mood and maybe be more generous and share the wealth but no, he's keeping it all to himself and so we don't have any choice but to take the beer by force, and now the country has descended into beer-stealing chaos all because your currency was no longer scarce and thus had no value.

So if your currency is physically made of something with low value, like paper, or even lower value like digital numbers in the ether, there has to be enforced scarcity. With paper fiat currency, we influence its value by limiting the amount that's printed and by making it difficult to forge. But how would that work with digital currency, which is ultimately just numbers in a computer that can be manipulated at will? You need a way to create scarcity, and make it difficult to increase the supply. So one strategy is to essentially make it a virtual commodity. You could model it after gold...you could force computers to digitally dig up your currency, aka "mine" it, ensuring that a limited amount is released over time, and that there's actual work that goes into producing or virtually

unearthing it. And that's what Bitcoin does. It mimics a representative currency. One Bitcoin represents a bunch of digital gold that was dug up using sophisticated tech.

So this idea of digital mining was just an abstract concept for years, and no one could figure out how to make it work. But that doesn't mean there weren't attempts to make a viable digital dollar. For instance,

E-GOLD, which was an early 1990s form of digital currency favored by drug dealers and money launderers. Because the supposed anonymity of digital currency is the initial appeal, right? You exchange real money for digital currency, and then you go online and use digital currency to buy drugs or a

wife or whatever, and then the drug dealer or wife dealer (nice name for a pimp—I'm not a pimp, I'm a lady dealer) either exchanges your digital currency back into fiat currency, or uses the digital currency to make his own illicit purchases. That's how Egold worked. It was a digital currency created in 1996 and tied to actual bullion, it was a representative currency with online dollars instead of paper dollars, so you bought real gold that sat in a vault and was represented online by egold. And for the first time you could easily initiate online third party transactions...it was like PayPal before PayPal, but it was vulnerable to all kinds of scams and hacking and phishing and all of the problems associated with windows ninety whatever. Can you imagine trying to handle digital transactions via windows 95, pre

mainstream internet? Sending money via modem?? AOL chat. @youve got gold. And viruses. Russian scammers now have your gold. The infrastructure wasn't ready.

So Bitcoin finally shows up in what's called a white paper on October 31 2008, on Halloween. It first appears on a Cypherpunk mailing list. Basically nerds. If you're confused about what a "white paper" is, well allow me to explain: it's a form of grey literature. So you're welcome. Moving on. No, look, grey literature is a genre of documentation released directly by companies and organizations, rather than by going through traditional publishing channels. If Apple releases a report detailing the steps they're taking to reduce their carbon footprint, that's grey literature. A white paper is a

specific form of grey literature, it's a technical document that is created by a non-governmental organization, and it is intended to explain or propose a complex subject to the public. Basically it's like, "here's how this complicated thing works, and maybe even our opinion of the thing, and some suggestions as to how to move forward considering everything we've said about the thing." That basically describes this podcast. We're the white paper of podcasts. That would have been a better name. Or at least, an equally confusing name. The Bitcoin white paper was signed by one Satoshi Nakamoto, the person or persons who created Bitcoin and mined a fortune of it before disappearing. While there has been speculation as to the true identity of the author or authors of the

white paper, he/she/they has never been conclusively unmasked. Not for lack of trying. If your name is satoshi nakamoto, for the last decade it sucks to be you, as was the case for Dorian Satoshi Nakamoto, a Japanese American Man in California who was hounded by reporters and even chased in his car, and to this day still fields frequent requests for interviews and fends off people constantly digging into his past. And look, If someone is denying being a billionaire, I'm just gonna take their word for it. Otherwise you're just rubbing in their lack of success. "I see you're driving a Kia Rio and living with your parents, but I'm pretty sure you're a billionaire. Nice try, undercover rich guy."
"Dammit, how many times do I have to tell you, I am not a rich genius. What do I have to do to prove to you that I

am an absolute loser?"
The word Bitcoin obviously is a mashing of bit and coin, "bit" being a contraction of the two words "binary digit" —the simplest and most basic form of computer data —and coin being coin. Which may be a word that actually needs explaining in a few years. I can't remember the last time I spent or even held an actual coin. I use Apple Pay, I avoid cash like the plague it is, or should I say the plague it can spread. My campaign against cash continues. But I don't remember the last time I touched an actual honest to god Metal coin. With like a bird stamped on it or whatever, that seems so historical. If you pull out some coins at the supermarket people are definitely going to look at you like, "OK Boomer." When I see a quarter on the ground I feel like an archaeologist. I'm like, wow,

a little piece of history. Oh the ancient wonders this silver eagle has seen.
So a couple months after the release of the white paper, On January 3rd, the anonymous person or persons behind Satoshi Nakamoto released the open-source code for Bitcoin and the protocol officially launched, implementing the content of the white paper and also the "genesis block," the first step on the path to the first ever Bitcoin mining project. Genesis block sounds like something from transformers. "The all spark has been removed from the genesis block." It took a week for the creator of Bitcoin to mine the first coins. Nakamoto would eventually mine over a million bitcoins before disappearing into the ether. That's the most Bitcoin owned by any one individual. At today's market valuation,

that's a 38 billion dollar fortune. Of course, that valuation will be different tomorrow. Nakamota might be wearing a barrel and suspenders by the end of the week. And for what it's worth, nakamoto (in quotes) has yet to remove or spend any of that Bitcoin stash. Very weird. There's been speculation that the founder of Bitcoin lost the password or digital key to the fortune, which is another common issue with cryptocurrency, but we may never know. It might also be possible that the creator is concerned that moving or spending the fortune would result in his or her unmasking. I'm fascinated by this mystery. What computer nerd with the chops to create something like Bitcoin is willing to just ignore thirty billion dollars. Did Bill gates create bitcoin? Some other tech billionaire? Or someone so benevolent and zen that

money just isn't important to him or her, even though he or she dedicated massive amounts of time and effort into studying and creating currency? It's mind boggling.

So the first so-called real-world transaction with Bitcoin was on May 22nd 2010, and involved a guy named Laszlo Hanyecz paying another guy ten thousand Bitcoin for 2 papa John's pizzas. At the time that was about 20 bucks and today would be approximately $380,000,000. I hope he got extra cheese.

So let's quickly explain the basics of the tech behind Bitcoin and blockchain.
At its core, Blockchain is not an intimidating or complicated concept. It's just a ledger, or database. It's basically a long ass receipt listing Bitcoin

transactions. Each new transaction is called a block, and it's added to the previous block in chronological order, forming a digital chain of transactions. The content of each block is dependent on the content of previous blocks...think of it as like legos or a Jenga puzzle in which the incoming blocks have to match up and fit with the previous blocks. If you tried to remove or alter a previous block, the whole thing would come crashing down. so you can't remove a block or rearrange them, and each of these million connected computers, or nodes, has a copy of the transaction list. It's decentralized and peer to peer, and this means that effectively, the blockchain can't be altered or hacked. You could break into a computer and mess with the ledger on that individual computer, but every other

computer would immediately compare the edits to the blockchain on a million other computers and reject that hack. It's majority rules, so in order to rewrite the Blockchain you would have to simultaneously control over 50% of the computers using the technology, or at least the mining/processing power, in order to create a verification crisis in which the computers suddenly don't know which blockchain is correct—the new version or the original. This kind of hack, known as a 51% attack, would generally only be possible with smaller cryptocurrencies—so called shitcoins—that are on very few computers...with a blockchain network the size of bitcoin's, it would be unfathomable. you can't simultaneously hack every computer that is running the Bitcoin software. Millions of them aren't even connected to the Internet at the same

time, and as soon as those devices reconnected they'd immediately detect the problem. So while *blockchain* isn't necessarily unhackable, the *Bitcoin* blockchain—and any other blockchain that reaches its size and scale—is for all intents and purposes secure. Now this doesn't apply to individual Bitcoin exchanges, which are services used to store and share Bitcoin. Those can be absolutely hacked or can even misplace Bitcoin through blatant incompetence as we'll soon see. Even the best technology is no match for human incompetence. I love that my iPhone is called a smartphone and I use it exclusively for stupid shit. This incredibly advanced piece of hardware and 99% of the time I'm using it use it to cheat at scrabble. That's not true. For anyone who is playing me in words with

friends, I wanna clarify that I only cheat when I'm playing against the computer. That's my story and I'm sticking to it.

So Bitcoins are "mined" via a proof of work concept. This sounds complicated but all it comes down to is that you have to work for Bitcoin. Or at least your computer has to work for Bitcoin. What you're doing when you're mining for Bitcoin is that you're giving computers extremely complex equations to solve, to make them work and show proof that they've worked. Proof of work. It's a way of artificially creating scarcity of Bitcoin. You can't just declare **I have created a Bitcoin**; I hereby announce that I am a millionaire. Trust me, I've tried it. No, you have to make your computer complete a time-consuming and also energy consuming task, chugging through

equations, in order to “mine” a Bitcoin. Or I should say be rewarded with a Bitcoin because honestly the idea of mining Bitcoin is an insult to real miners everywhere. Mining is filthy, backbreaking work. You can mine Bitcoin while sleeping. A Bitcoin miner is a miner in the same way that I’m a stock broker just because I have a 401k. Stocks are being traded in my name, I’m reasonably confident of that, and these complicated transactions are in theory making me money, and I’m responsible for exactly none of it. I’m a stock trader who specializes in giving my money to actual stock traders, and so far it’s working out swimmingly.

So this can get a little more complicated, but we’ll keep it simple by saying that the very difficult equations that miners are solving are equations that are verifying and storing transactions to the Blockchain. So the proof

of work is actually how the blockchain is built.
Anyone can technically mine bitcoin, but it takes a lot of processing power and a lot of time. And at this point you'd have to invest in some extreme technology. Because there are massive wealthy organizations that have huge server farms, football field size airplane hangers full of processors chugging away. And you're competing with those, so good luck. It's easier to be a bitcoin spender than a Bitcoin miner. I'm not equipped to set up a server farm, but I could spend the hell out of some Bitcoin. At least, as long as it's still being created. we discussed scarcity before...there is a maximum amount of Bitcoin available, which was determined by Satoshi Nakamoto, 21 million. Plus, the amount of the coin that can be mined every day and every year is predetermined,

and that number is being reduced over time as determined by Satoshi's bitcoin code. Which means that it is going to be less and less lucrative to be a bitcoin miner every passing year, even as more and more people jump on board to split that pot of virtual gold. Worldwide, there are fewer than 1000 bitcoins being mined every day, so if you're an amateur miner, you're probably earning fractions of a cent daily. In fact, 80% of the 21,000,000 maximum bitcoin have already been mined; however, it's going to take a long ass time to mine the last twenty percent due to that aforementioned steep decrease in available Bitcoin that Satoshi built into the code. Roughly every four years, the total number of bitcoin that can be mined in a given length of time drops by half. At the current pace, the supply of Bitcoin is set to

run out around 2140 when it hits 21 million. When that happens, bitcoin mining will cease. No one will be financially benefiting from bitcoin mining, but those equations still have to be crunched, because they are how the block chain is sustained. So how will we convince people to continue using all that energy and processing power without rewarding them with bitcoin? Well, there will still be transaction fees. Did you think this anarchist underground currency wouldn't involve bureaucracy and petty fees? Nickel and bitcoin diming? Right now, each transaction includes a fee similar to a credit card transaction, and those fees are divvied up among the miners. The fees vary depending on how quickly you want your transaction processed. It's complicated, but basically every transaction sits in a

memory pool until a miner grabs that transaction and starts crunching the numbers. But those miners are naturally going to grab the transactions with higher transaction fees first. Every transaction is basically like an auction, if you offer a higher transaction fee it's more likely that a Bitcoin miner will choose to process your transaction.
(Auctioneer voice: "do I hear one 8000th of a Bitcoin, do I hear one 7500th of a Bitcoin, going once going twice sold to the computer of that guy who's eating Cheetos and has nothing to with this because it's all automated and bitcoin isn't really mining at all." When all the bitcoin runs out in 2140, those transaction fees will be the only benefit to data crunching, and those fees are only about 6% of what miners are making today via mining Bitcoin . So how is this all going to shake out?

Well there are a few different future possibilities. Maybe all of the casual, independent miners will immediately go out of business, and only the large firms will still be able to make money. Or maybe the code will be revised. But either way, it's clear that Bitcoin will continue to become more accepted and mainstream, which sort of runs counter to the whole rebellious spirit of crypto. There's this idea that cryptocurrency is subversive, it's freedom, it's decentralized so it's not controlled by any single government, it's not controlled by THE MAN, and provides anonymous transactions. After all, as mentioned, cryptocurrency has historically been used by criminals and drug dealers to hide their illicit deals. Most famously via the Silk Road, which deserves its own episode. I read a book about the rise and fall of the

Silk Road, an online black market where you could buy drugs, weapons, sex, etc. But the future of crypto could be much more pedestrian and controlled. “Bitcoin is often perceived as an anonymous payment network. But in reality, Bitcoin is probably the most transparent payment network in the world…All Bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network.” Think about it: if I give you $300 right now for sexual favors, we exchange cash in this studio, there’s no record of the transaction, no one knows it happened except me and you. But if I send you the equivalent of $300 in bitcoin, there’s a record of the transaction in the block chain. Forever. For everyone to see. Maybe they don’t know who we are, right now, or what the transaction was for, but the fact is that there

is a permanent record of that transaction which makes it far less anonymous than cash. “once addresses are used, they become tainted by the history of all transactions they are involved with. Anyone can see the balance and all transactions of any address. Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous. As the blockchain is permanent, it's important to note that something not traceable currently may become trivial to trace in the future.” Bitcoin is referred to as “pseudononymous.” It’s been compared to a Twitter account. I have a Twitter account under a fake name, and no one on Twitter knows who I am. But there’s a record of every tweet, which is associated with that account. And if anyone could find a way to link me

to that account, they would then have a record of everything I ever tweeted.

Bitcoin is also no better than cash when it comes to storing your money. It's basically like regressing to the days of storing cash under your mattress. Or carrying it in your wallet. In fact, the name for a Bitcoin storage is a digital wallet.

Bitcoin wallets work just like an email program that you use for managing your emails. "In this case, the email program you use is your Bitcoin wallet, your emails are your Bitcoins, and your email address is your Bitcoin address."

There are different types of wallets: mobile wallet on your phone, web wallet—software on the web—desktop wallet—software on your computer—and hardware wallet, software on

a USB dongle. “Dongle” One of my favorite words, because I’m five. You’d better have a really large dongle to store all of that bitcoin. Fetch me the largest of dongles for my bitcoin. But if you’re storing your bitcoin in third-party software, that data is vulnerable. And it’s way more vulnerable than pretty much any other form of currency. I bank with Chase. If the Chase bank down the street gets robbed, and the thieves make off with all that money, I haven’t lost a dime. The bank lost money, not me. Can you imagine a bank getting robbed and then having to call all of the customers and be like, hey, funny story. That’s literally what bitcoin exchanges have done. “Remembers all that money you gave us to hold on to? Yeah, about that.” But that could never happen with fiat currency, because even if Chase went out of

business tomorrow, the federal government has insured my deposits. But bitcoin isn't backed by the FDIC. If those bitcoins fall into the wrong hands, they're gone for good. And this has happened numerous times. Most famously with mount Gox. Founded in 2010, by 2014 the mount Gox Japanese bitcoin exchange was handling 70% of worldwide bitcoin transactions. It was huge, it was the worlds leading and largest bitcoin exchange. And in 2014 it was hacked. When all was said and done, over 650,000 bitcoin were siphoned away. And then there was Canada's QuadrigaCX. CEO Gerald Cotten, an absolute grifter and con man, ran the entire business via a single laptop. When he died in India under mysterious circumstances at age 30, the password to the laptop, supposedly containing

cryptocurrency worth over 200 million dollars, expired with him. Except it would later turn out that those bitcoin wallet were empty, having been drained by Gerald cotton, and there's a ton of speculation online as to whether the sky is actually still alive, because the other thing that can happen with bitcoin business exchanges is that they just straight up steal money from their customers. This is such a common occurrence that it even has a name: exit scam. Which is also the title of a podcast I highly recommend explains the whole Gerald cotton fiasco.
These stories are not rare. The crypto landscape is littered with the remains of hacked and plundered Bitcoin exchanges.

So let's briefly talk about NFTs.

NFT stands for Non Fungible Token. Fungibility refers to the quality of fungishness, or fungosity, which is an earthy, umami flavor. Similar to shitaki-ism or portabellishness.
No. Fungibility is interchangeability. An item is fungible when you can trade it for other units of that same item and all of those items are of equal value and basically carbon copies. So a dollar bill is fungible. An ounce of gold is fungible. You exchange an ounce of gold for another ounce of gold and your financial situation hasn't changed. Bitcoins are fungible. If I send you one Bitcoin and you send me a Bitcoin at the same time, it's a wash, they're of equal value. So an NFT uses the blockchain, like Bitcoin, but unlike Bitcoin is non-fungible. An NFT is unique.

At its core An NFT is

basically just a digital certificate of ownership that gets recorded as a block in a block chain. Usually via the cryptocurrency called ethereum. It's a receipt for a purchase. But in this case the purchase is not of a physical item. An NFT is a declaration of ownership of a digital file.
Like, any digital file. A picture of grumpy cat. An episode of a podcast. An NFT is meaningless, because an online digital file is infinitely copyable. We could sell our first episode as an NFT, and nothing changes, all of the insomniacs could still download and listen to that episode, the only difference is that one insomniac could say "I officially own episode one...the proof is on the blockchain. See?" So an NFT basically provides proof that you...are a sucker. It's like a giant billboard on the internet displaying one of

those “I’m with stupid” arrows pointing at the idiot who voluntarily paid for what everyone else gets for free. When you buy an NFT you’re buying bragging rights.
But look, it’s an interesting idea, because what it really comes down to is a way of supporting artists. It’s patronage. It’s like, “I love this piece of digital art so much that I’m going to reward the creator for making it while simultaneously announcing my love for it to the world on the blockchain. And the blockchain is forever.”

So what’s the future of Bitcoin and the blockchain? There are some great aspects of cryptocurrency. It enables peer to peer monetary transactions for people who don’t have access to banks, for instance people in countries in which the currency is

volatile and wildly fluctuating. Fluctuating even more than Bitcoin. If you have family in Venezuela, where the value of the currency has fallen precipitously amidst rocketing inflation, it can be very difficult to reliably send money back home due to diplomatic issues between the nations. But if your Venezuelan family member can find WiFi for a few minutes, he/she can receive Bitcoin from you without any government or banks getting involved. But there is a major downside to crypto. We have to address the electronic elephant in the room: all of the energy that is used when mining bitcoin. The server farms are huge, they're hot, they take up a ton of electricity. But to be fair, so do the server farms for every other computing company. In my opinion the environmental impact of crypto is a bit of a red

herring, for instance in China many crypto farms aren't using coal energy, but instead will actually move around to follow the rainy season, so that they can take advantage of massive influxes of Hydro power in different areas of the country. Plus, bitcoin will most likely eventually move from the "proof of work" system to "proof of stake," and we're not going to get into the weeds on this but suffice to say that all of that computing power necessary for proof of work, for crypto mining, can be mitigated with different methodology. So while the environmental impact of crypto is currently undeniably dramatic, that's not necessarily going to be the case for much longer, and regardless, the block chain is here to stay, so we need to figure out workarounds for the negative aspects of crypto

mining without demonizing a new and inevitable technology. Again, I'm not a fan of crypto by any stretch, I don't own any, but I'm also not shortsighted, this technology isn't going away.

We didn't talk about fake-genius Elon musk and his boneheaded tweets that cause massive shifts in crypto. Elon btw was a rich kid who bought Tesla, he didn't create it. He's a solid hype man and skilled at getting media attention, but hasn't engineered a rocket or vehicle in his life. But we have limited time and we have to end somewhere. This one wasn't the most fun but you can't say you don't understand crypto.

https://www.google.com/amp/s/www.vanityfair.com/news/2019/11/the-strange-tale-of-quadriga-gerald-cotten/amp

https://www.mentalfloss.com/article/94593/delicious-asset-inside-italys-cheese-bank

https://en.m.wikipedia.org/wiki/Compressed_tea#Use_as_currency

https://apple.news/AQA5_VNH1TC6a-cHL-kvftw

https://www.google.com/amp/s/www.esquire.com/lifestyle/money/gmp36290032/history-of-cryptocurrency/

https://www.thebalance.com/what-is-the-history-of-the-gold-standard-3306136

https://
www.investopedia.com/
articles/investing/092413/
how-currency-works.asp

https://bitcoin.org/en/
protect-your-privacy

https://blog.hubspot.com/
marketing/bitcoin-address

https://www.google.com/
amp/s/en.bitcoinwiki.org/
wiki/Amp/E-gold