Cryptocurrency

March 9, 2025

There are two questions that weigh heavily on an investor's mind: Should I invest in cryptocurrency? And, what is cryptocurrency? The one sentence answer is, "Warren Buffett says do not invest in cryptocurrencies, because you are buying the Sword of Azeroth."

I state Buffett's answer below. After that, I explain the technical reason behind Buffett's answer. After reading the paper, you will know what cryptocurrency is.

Should I invest in cryptocurrency? No

Warren Buffett answers :

"There are two kinds of items that people buy and think they're investing. One really is investing and the other isn't. If you buy something--a farm, an apartment house, or an interest in a business, and look to the asset itself to determine whether it does something: what the farm produces, what the business earns and so on--you don't really care whether the stock market is open. You can do it on a private basis. In fact, you do it on a private basis if you buy a farm or an apartment house, generally. And it's a perfectly satisfactory investment. You look at the investment itself to deliver the return to you. Now if you buy some bitcoin or some cryptocurrency, you don't really have anything to produce anything, you're just hoping the next guy pays more."

BRIAN CECCARELLI, PE
4605 WOODMILL RUN; APEX NC 27539
T: (919) 815-0126 U: https://talussoftware.com ceccareb@talussoftware.com

What is Cryptocurrency?

I describe cryptocurrency in a sequence of definitions and concepts. Read them in order. First I define four words. The definitions stand by themselves. Then I describe the concepts. I describe each concept with an analogy between US dollars and bitcoins. After you understand the definitions and concepts, I present warnings.

You will not find math in this paper because the math does not help answer the questions.

Definitions

Term	Meaning
currency	A means of exchanging commodities and services. Money in the form of paper or coins, issued by a government and accepted at face value, is known as *currency*. There are about 180 currencies in the world. Examples of currencies are the United States Dollar, the European Union Euro, the Indian Rupee, and the Japanese Yen.
cryptocurrency	A cryptocurrency is also a means of exchanging commodities and services. Cryptocurrency is money that takes the form of ones and zeros in a token, like 01011101010100010101010111, stored electronically on a computer on the internet. A computer program, behaving identically to a video game,

	rewards cryptocurrency to the first player who solves a mathematical puzzle. As of March 2024, there are 13,217 cryptocurrencies in the world. Not all cryptocurrencies are active or valuable. Not including the many "dead" cryptos, there are about 8,985 active cryptocurrencies. Examples of cryptocurrencies are Bitcoin, Ethereum, Solana (Trump's Memecoin is a part of Solana), DOGEcoin and LiteCoin.
bartering	In *bartering*, goods and services are exchanged directly for other goods and services
bitcoin	The word *bitcoin* causes confusion. Depending on context, "bitcoin" has four different definitions: 1. The name of the cryptocurrency 2. A denomination of money in the cryptocurrency 3. The name of the internet-based network which is the source and record of transactions in the cryptocurrency 4. The name of the stock symbol for bitcoin: BTC

Concepts

It is easiest to understand the concepts of cryptocurrency when they take the form of analogies. Below are analogies between dollars and bitcoins. Read the concepts in order.

#	Concept	United States (is the location used)	Bitcoin Network (is the location used)
1	Name of Currency	Dollar The dollar is the name of a currency. The dollar is also the name of a denomination of money in the currency. Unlike Bitcoin, a "dollar" is not the name of an internet network. Unlike Bitcoin, "dollar" is not the name of a stock. You cannot buy dollars on the stock market. You can buy dollars in a foreign bank or foreign exchange market.	Bitcoin A Bitcoin (upper case "B") is the name of a currency, and "bitcoin" (lower case "b") is a name of the denomination of money in the cryptocurrency. Exchanging dollars for bitcoins can only be done on the stock market. Bitcoin exists only in the Bitcoin computer network. What is the Bitcoin Network? The Bitcoin Network functions like a video game. When you play the video game and win, the game master awards you points. These points are called *bitcoins*. These points

			are useful only inside the game. *It is just a game*. Obviously many people assign value to bitcoins outside the game, but the truth remains. Only in the game, non-reality, do bitcoins have value. This YouTube clip from the *Big Bang Theory* illustrates this point. In the video, the Sword of Azeroth exemplifies a bitcoin. We know from the clip that it takes days playing the game before you get the chance to obtain the sword. In the clip, Sheldon Cooper wins the sword. Then Sheldon immediately turns the "asset" around by putting it on E-Bay. The fact that Sheldon can sell a virtual sword on E-Bay for real money is crazy in itself. But crazier still is that someone actually buys it. Wolowitz buys it with real money. This implies that the virtual sword has value in the real world. But does it really? The sword is indeed coveted by game players, but no matter how

			many people venerate the sword, no matter how much time and energy people spend to obtain a sword, no matter how much real money people are willing to buy the sword, the sword is still not real.
2	**Fungible** A fungible asset is one that can be swapped for a similar item, and can be divided.	Yes 1 dollar = 100 cents When I swap my dollar bill for your dollar bill, each of us has the same amount of asset as before the swap. When I swap my 100 pennies for your dollar bill, each of us has the same amount of asset as we had before the swap.	Yes 1 bitcoin = 100,000,000 satoshis The denomination *satoshi* comes from the name *Satoshi* Nakamura. Satoshi Nakamura was the author of the 2008 paper *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamura is a pseudonym. Nobody knows the identity of Satoshi Nakamura and Satoshi Nakamura does not want anyone to know.
3	**Fiat** Fiat money is government-issued currency that is not backed	Yes The last time the US Dollar was backed by gold was in 1933. The US remained on a quasi-gold standard	Yes Like the US Dollar, the Bitcoin Network's Bitcoin is not backed by a commodity.

	by a commodity such as gold. What gives currency value?	until President Nixon officially converted the US dollar into a fiat currency. A US Dollar is backed by 2 things: the government's ability to generate revenues (via debt or taxes), and its authority to compel economic participants to transact in dollars. A government can legislate its value. For example, Section 31 U.S.C. 5103.	Unlike a dollar, a bitcoin is not backed by a government's ability to generate revenues or *government's authority* to compel participants to transact in bitcoins. Unlike a dollar, a bitcoin's value cannot be legislated. As stated by Warren Buffett, the only value bitcoins have is what people are willing to pay for them.
4	How is the Currency Created?	The Federal Reserve has the authority to print dollars. Printing gives the Federal Reserve greater control of the economy.	The best way to describe how bitcoins are created is to use the video game analogy. We will call the video game "Gods of Crypto". Bitcoins are the points awarded when you win a game in *Gods of Crypto*. *Gods of Crypto* is a multiplayer game. Each player competes with others to solve a bunch of math puzzles. The first one who solves the puzzles, wins bitcoins.

			Now, as opposed to a game, the solution to one of these math puzzles has value in the real world of accounting. The solution to a puzzle, though a mere number, has the ability to link two business transactions together in such a way that no person in the future can alter either transaction. In other words, the number prevents future hackers from cooking the books. Because security has value to real-world businesses, businesses submit their unsecured transactions (in units of bitcoins) to the game master of *Gods of Crypto*. Players receive the business' transactions from the game master in a *block*. There are about 1000 transactions to a block. Each player then goes on a *quest* to find the numbers that make all the transactions in the block secure. Each number is called a *hash.* The hash is the "proof of work" that the player successfully linked one transaction to another.

			This quest is called *mining*. Once the player finds all the numbers for his block of transactions, he submits his now-secured block to the game master. If the player is first to submit the block, the game master rewards the player with bitcoins. A bitcoin is the equivalent of the Sword of Azeroth. The winning player is happy. The rest of the players lose. (Because it is difficult for a single player to find all the numbers in a single block, players form a alliance, just like the alliance our Big Bang friends formed to get the Sword of Azeroth.) The game master then records the winning player's block of transactions. The game master appends the player's block to blocks previously recorded by all other players from all games from

			all time. The result is a big chain of blocks called the *blockchain*. There is only one blockchain in Bitcoin. It is currently about 620 GB. Most video games are cheap to play. But *Gods of Crypto* is extremely expensive. Finding a hash takes a lot of computer CPU power. The amount of CPU cycles eat a lot of electricity. On average, mining 1 bitcoin consumes around 6,400,000 kWH. That is about 18.6 years of electricity consumed by the average American household. The cost of using 6,400,000 kWH depends on your utility's power rate. When the smoke clears, and though you did some practical work securing transactions, you still only have the Sword of Azeroth. Though expensive in the real world to obtain the sword, the sword exists only in Cyberspace.

5	Where does the Currency Exist?	In your pocket You can deposit currency into your bank account, where it becomes a number on a computer. But then you can swap the number back to currency whenever you wish.	On the internet You don't carry bitcoins on your person, on your computer or on your USB drive. Instead, you carry the *addresses* of the bitcoins on your computer or on your USB drive. These addresses are similar to bank account numbers. The bitcoins are not in your pocket, but rather exist remotely on the computer network. The only way to access your bitcoins is on the internet. If the internet goes down, you are moneyless. If your personal access to the internet goes down, you are moneyless. If the electricity shuts off, you are moneyless. The addresses are stored in a "digital wallet". A digital wallet is an app. If your app crashes, you are moneyless. If your computer storage device containing your wallet becomes corrupt, you are moneyless. If

			you lose your USB drive or accidently erase your storage device, you are moneyless. Digital wallets can also be hacked.
5	Bank	The purpose of a bank is to store your money in a safe place, to safeguard your money from theft, from counterfeiting, from fraud, and to make it easier for you to exchange assets from a distance—for example a wire transfer, an ACH transaction or a check. You trust the bank with your money and the bank guarantees that your money is safe by FDIC insuring it to a certain amount. The bank also gives you records of the transactions in the form of bank statements. You use these statements to keep yourself and the bank honest.	There is no bank. The purpose of cryptocurrency is to remove the bank from managing transactions. The financial world is based on transactions. Withdrawals. Deposits. Selling a house. Buying a car. So on and so forth. You can save a lot of US dollars if you remove the middle man. The promise of cryptocurrency is that you avoid transaction fees. The promise is a mirage. As already shown, mining is expensive. There is always a price to compute every hash. The safety of your bitcoins is guaranteed on the Bitcoin Network because nobody but the owner of a bitcoin can access the bitcoin. You transfer your bitcoins to other people by the

			same transaction mechanism as businesses. The Bitcoin Network offers safe storage of bitcoin money, and safeguards your money like a bank. The Bitcoin Network prevents counterfeiting and the "double-spend problem" better than a bank. Unlike a bank, the Bitcoin Network does *not* insure your money. And as stated before, unlike a bank, there are several cases where you can lose your money forever.
6	**Inflationary or Deflationary**	Inflationary As time goes on, the price of eggs increases. The price of eggs in 1960 was 47 cents per dozen. It is now $4.95 per dozen. The economic benefit of an inflationary currency is that people are inspired to consume. People want to spent their money now	Deflationary A deflationary market inspires hoarding. No one spends their money now because it will be worth more in the future. Bitcoin is the only cryptocurrency that is strictly deflationary. There is only a fixed amount of bitcoins that can be mined. It is estimated that by 2140, there will be no more bitcoins left in the

		while it is still worth something.	mine. After 2140, instead of creating new bitcoin when a player solves a math puzzle, the player gets paid only by transaction fees. Businesses submitting transactions will pay the *Gods of Crypto* players satoshis to find the numbers which link their transactions.

Warnings

1	Nobody takes credit for Bitcoin. Anonymity implies unwillingness to take responsibility, and all the things that implies.
2	The monikers “Trump coin” and “DOGEcoin” violate the trust manifesto of cryptocurrency. In order for cryptocurrency to work fairly, cryptocurrency networks must be owned by the public and operated without bias. A person or a government agency, by the very fact that the owning entity is not the public, is an oxymoron. It means that the cryptocurrency can be controlled and gamed by an individual or group. Even now, on the Bitcoin public network, 70% of bitcoins are owned by 0.01% of owners of bitcoins. Just as in the real world, these .01% of owners exert unfair influence over the stock. Just as in real world, these influencers are called whales and have the power to affect prices and circulation.

3	Cryptocurrencies are unregulated. Some cryptocurrencies use a Proof of Stake (PoS) mechanism which can further defraud others from fair participation.
4	A computer system can always be gamed . . . just like a Nevada slot machine.
5	The fear of missing out (FOMO) is the strategy cryptocurrency advocates use to entice buyers to invest in cryptocurrency. The "F" in FOMO, this time in particular, is the fear of not knowing what cryptocurrency is. Some investors advertise , "We are investing in blockchain technology." What are they really buying? It is not what they are *buying* but rather what they are *paying* for. They are paying to secure transactions on the Bitcoin Network. There is tremendous cost in kilowatt hours to solve these math puzzles. The cost requires that BTC stock trades higher than the price of securing transactions. At the moment, the Bitcoin Network subsidizes miners of bitcoins. The Bitcoin Network creates new bitcoins in order to prevent businesses from having to pay transaction fees. (All transactions are in bitcoins.) As long as the Bitcoin Network has bitcoins "still in the ground", and the price of BTC stock surpasses the cost of mining, miners have the incentive to mine and businesses do not have to pay transaction fees. However, once either precondition is not met, businesses must charge transaction fees--the very thing cryptocurrency claims to avoid.
6	Quantum-computers can devalue cryptocurrencies instantly. Because quantum computers have the potential to solve math problems millions of times faster than silicon computers, the acquiring of a quantum computer can turn a person into a whale over night. The person can flood the circulation with new crypto coin, devalue the cryptocurrency, and/or prevent others from acquiring cryptocurrency. Microsoft just introduced the first quantum computer chip Majorana 1.

Summary

Warren Buffett says do not invest in cryptocurrencies, because you are buying the Sword of Azeroth.

To pay the energy costs for securing transactions, one must sell cryptocurrency, the exchange thereof being a secured transaction. One can regard cryptocurrency as a circular fallacy.

To sustain a dollar value in cryptocurrency, advocates must solicit others and claim their swords are worth something. These people are called "stock pumpers".

Biography

I am a professional engineer licensed in North Carolina. The license comes from passing the professional engineer's software engineering exam. My degree is in physics, and a physics education comes in tandem with a math education. For years I have watched the hype of Bitcoin and wanted to know if the hype had merit. So a couple of years ago, I bought a book and taught myself how to program Bitcoin from scratch. It has a steep learning curve. I worked with prime fields, ecliptic curve cryptography, encoding and decoding public and private keys, computing hashes, and successfully submitting transactions on the Bitcoin TestNet network.

The math knowledge and the tedium with the data processing which manages Bitcoin reminds me of entering the *Publisher's Clearing House Sweepstakes*.