

What Exactly Is Crypto? *And Is It for You?*

Introduction -- Not your usual currency

Cryptocurrency. It's a name that seems to conceal as much as it explains. The first part, crypto, comes from cryptography, the study of securing communications. And the second part, currency, is a matter of dispute. Some observers, including the Internal Revenue Service, categorize cryptocurrency as property. Others define it as one of the following: a commodity, an asset, an investment tool, a payment system, a digital currency. And still others see it as an online casino at best, and a Ponzi scheme at worst.

If it is a currency, it is not like any other. Most cryptocurrencies are not issued by a government or central bank. Instead, they exist as digital records maintained by computer networks. Crypto comes in various forms, and these forms have been proliferating in the past few years. As with widely recognized legal tender, its units are called coins or tokens, though they can be neither seen nor held.

Cryptocurrency transactions are banned in China and closely watched in Europe, while Bitcoin has been adopted as legal tender in El Salvador and the Central African Republic. A growing number of retailers accept it, but some of the largest cyberspace advertisers, including Google and Facebook, banned crypto advertising for a time. And despite a tortured history of extraordinary booms followed by crushing busts, it continues to grow in popularity. As of this writing (January 2023), an estimated 300 million people own or trade crypto worldwide. Approximately \$50 billion worth of tokens change hands every day, and crypto has a global market capitalization of \$1.08 trillion, an impressive figure, but only 36% of its record peak in 2021.

So, what exactly is crypto? And even more important, is it something you should own or trade? In the following article, we provide a brief background on the crypto phenomenon and take a stab at whether it is here to stay. We then offer guidelines on investing, and end with some thoughts on the future of money.

Beginnings – The libertarian's revenge

Bitcoin, the first cryptocurrency as we know it, was born during the financial crisis of 2007-2009. Put off by the control that governments and banks wielded over economies, Satoshi Nakamoto (a pseudonym for a person or a group) developed Bitcoin as a peer-to-peer payment system. Through cryptography and a pioneering technology called "blockchain," Nakamoto sought to bypass the worldwide banking system by using a database spread across a decentralized network of computers.

Such a database, known as a "distributed ledger," was not new. Synchronized records had previously been stored across multiple computers. Nakamoto's breakthrough was to combine that concept with cryptography and a decentralized system for validating transactions, creating a digital currency that could operate without a bank or another central authority.

New Bitcoin transactions are digitally signed, broadcast to the network, and checked by participating computers before being collected in a block. Each block can contain thousands of

transactions, although the number varies depending primarily on the amount of data each transaction requires. More complex transactions consume more of a block's total data capacity, leaving room for fewer transactions.

A completed block is linked to the previous block using a unique digital fingerprint, known as a hash. Because each block refers to the one before it, the blocks form a continuous chain. This linkage creates a permanent record and helps secure the system. Altering an earlier block would change its fingerprint and break the links to every block that followed.

Bitcoin uses a process called "mining" to verify transactions, add new blocks to the blockchain, and issue new coins. Specialized computers called miners compete to find a valid solution to a difficult computational puzzle. The first miner to succeed broadcasts its proposed block to the network. If the block is verified and accepted, the miner receives newly created Bitcoins, along with transaction fees.

Why go through all this rigmarole? The competition makes the blockchain extremely difficult to corrupt. The solution is tied mathematically to the contents of the proposed block, so changing even one transaction invalidates it. A cheater would have to redo the computational work for that block and every block that followed, while also outpacing the rest of the network.

Mining therefore provides a decentralized way for participants to agree on the official transaction record without relying on a bank or another central authority. Although miners with more computing power have a greater chance of succeeding, no one knows in advance which miner will add the next block.

All Bitcoin transactions are publicly viewable on the blockchain, a significant step forward in transparency and traceability compared with the current banking system. Participants use digital addresses rather than names, making the transactions pseudonymous rather than completely anonymous. Addresses can sometimes be linked to real identities, and a growing number of countries require traders to identify themselves on major exchanges.

Profusion of cryptos

The Bitcoin network was launched in 2009, but crypto didn't catch on immediately. It wasn't until 2010 that someone actually used it to buy something – two Papa John's pizzas in Florida, which cost 10,000 Bitcoins. (The tokens were very cheap in the beginning.) But eventually crypto achieved traction within the investment community, to the point where it has grown into a flourishing industry.

At the end of last year, there were nearly 22,000 distinct cryptocurrencies and some 500 exchanges where they could be bought or traded. There were also crypto ETFs, ATMs, databases and a crypto counterpart to an initial public offering (IPO), known as an ICO (Initial Coin Offering). ICOs have tended to operate more like crowdfunding than traditional IPOs and generally reward investors with coins. A coin's initial price is often only a fraction of a penny, although price alone says little about value because the number of coins issued varies widely.

The crypto phenomenon has also given rise to affiliated businesses such as coin mining, crypto consulting, and crypto investment lending.

Even with the torrent of new crypto versions, Bitcoin continues to reign over the industry, representing approximately 42% of total crypto market capitalization. A number of others, however, have created significant brands of their own. Ethereum, in particular, has developed a strong following, as much for its innovations as for its relative strength. One major innovation was its adoption of a less cumbersome method of assembling, verifying and connecting new blocks.

Unlike Bitcoin mining, there is no problem-solving contest. Instead, companies or individuals deposit 32 ether (Ethereum's cryptocurrency) as collateral and wait for their validator software to be randomly selected as a block stitcher. Once a new block is proposed, other validator programs check its transactions and confirm that it follows the network's rules. Validators who cheat can lose some or all of their deposit, which was worth roughly \$50,000 in late January 2023. On the plus side, properly functioning validators can earn small amounts of newly issued ether for helping confirm blocks, while those selected to stitch blocks together can earn additional rewards and transaction fees.

Ethereum's validation method has a number of advantages over mining. For one, it requires much less energy. Mining is so energy-intensive in its use of computer power – computers frantically run endless loops to be the first to solve a problem – that it has contributed significantly to carbon emissions. Another advantage is that Ethereum is much quicker in creating blocks and confirming transactions. Bitcoin produces a new block approximately every ten minutes.

That may not seem like a long waiting period, but if a gas (petrol) station required the first on-chain Bitcoin confirmation, you'd have time not only to clean your own windshield (windscreen in the UK), but those of the customers waiting in line behind you as well. And ten minutes is just the average. Sometimes it can take an hour. By contrast, Ethereum provides an opportunity to create a new block every 12 seconds, so transactions generally receive their first confirmation much more quickly.

In its brief life, crypto has morphed into several new forms known as "altcoins." Probably the standout among them is the stablecoin, developed in the mid-2010s as a response to crypto's volatility. A stablecoin can be pegged to a fiat currency, a commodity (gold, for instance), or even other cryptocurrencies. As its name implies, a stablecoin tends to hold its value better than other crypto. However, under extreme duress, stablecoins can lose their peg. For instance, in 2022, one stablecoin (UST) dropped in value from \$1 to 26 cents and then to nearly zero when its algorithmic mechanism lost its dollar peg, precipitating the collapse of the Terra ecosystem and wiping out roughly \$40 billion in market value.

Another form of crypto is the privacy coin, which obscures the identities of transaction parties even more than other crypto. While favored by many crypto enthusiasts, privacy coins, as well as crypto in general, have come under attack as a financial enabler for money laundering, drug trafficking, and terrorism.

While such illicit uses do occur, they represent only a fraction of crypto transactions. In January, Chainalysis, a software company specializing in the industry, estimated that transactions involving known illicit addresses accounted for 0.12% of total crypto transaction volume in 2021. The company cautioned that this was a lower-bound estimate that excluded unidentified addresses and

much criminal activity originating outside the crypto market, such as human trafficking and tax evasion.

Tantalizing returns

Why are there so many cryptocurrencies? For starters, a promising new technology tends to ignite a storm of competition. Even a casual glance at tech magazines in the years following the introduction of the personal computer reveals a cornucopia of brands, many of which crashed soon afterward, both mechanically and financially.

And second, the astonishing rise in value achieved by the successful cryptocurrencies is a huge motivator. The business magazine *Forbes* keeps an updated list of the [top ten cryptocurrencies](#) by market capitalization, and it's worth taking a look at the comparative valuations.

According to *Forbes*, in late January, Bitcoin was worth approximately \$458 billion. Between May 2016, when a single Bitcoin was worth about \$500, and January 2023, when it was valued at \$23,764, Bitcoin grew in price by approximately 4,653%. And that was after major downturns in 2022.

Ether (Ethereum's coin) was solidly at number two, worth \$1,331 per coin in mid-January, a rise of 11,996% from its value of about \$11 in April 2016.

Some of the newer cryptos have experienced even more incredible growth. Dogecoin, which began as a joke in 2013, was worth \$0.0002 at birth. By January of this year, its value had soared to \$0.08, an increase of 39,900%. Its market cap of \$10.1 billion earned it a ranking as number 9 on the *Forbes* list.

These remarkable gains haven't gone unnoticed by hackers. They have engaged in an ongoing battle with the industry for years, sometimes spelling the doom of major players. In 2014, for example, the then-dominant Bitcoin exchange, Mt. Gox, filed for bankruptcy after approximately \$460 million of the currency was stolen. At the time, Mt. Gox handled approximately 70% of Bitcoin transactions.

One positive outcome of chronic hacking is that it has pushed the industry to strengthen its security through a number of measures. These include so-called "hardware wallets," which are discussed below.

Despite these safety measures, the threat of hacking continues. Through October of last year, according to a CBS News report, hackers made off with a record \$3 billion. And in November, with the collapse of FTX, the second largest crypto exchange at the time, hundreds of millions of dollars in tokens were removed in unauthorized transfers.

Many of these hacks exploited a couple of salient weak points: the transfer bridges between blockchains and the poor habits of some crypto owners who don't safeguard the codes that unlock accounts, known as "keys." The larger blockchains themselves tend to be inherently secure because taking control of them would require enormous computing power and expense.

Boom and bust cycles

If crypto gains have been breathtaking, so have the busts. Around the time of Mt. Gox's collapse in 2014, Bitcoin fell nearly 50%, from \$1,238 to \$688. Three years later, in 2017, Bitcoin found new life and surged to \$19,345, only to fall to \$6,636 in 2019. It then soared even higher in November 2021 to \$68,991 before plummeting again to around \$18,000 in December 2022. Despite all these price collapses, Bitcoin has been able to achieve not only higher highs but also higher lows, which is one of the more positive signs in technical analysis (the study of asset price charts).

Another supposedly positive feature, one touted from crypto's early days, was its potential as a hedge against inflation. Unlike fiat currencies, some cryptocurrencies stipulated that they would produce only a limited number of tokens. Bitcoin, for its part, set that limit at 21 million coins, a "hard cap" written into its source code and enforceable by the network. Additionally, Bitcoin's block reward is halved every 210,000 blocks, which has historically worked out to approximately once every four years. Given these pre-set limits, the assumption was that while central banks printed their way out of economic difficulties, crypto would simply float on the ensuing rise in prices.

But it hasn't turned out that way. With the most recent bout of inflation, the worst in 40 years, crypto valuations fell along with the equity markets. Today, it is mired in a "crypto winter" in which trading activity is way down and skepticism is on the rise. In addition to the ongoing criticism noted earlier, commentators have recently called crypto "magical thinking" and "the Wild West" of investing.

Still, it would probably be a mistake to count crypto out. As Matt Weller, Global Head of Research at StoneX Retail, noted, "Past crypto winters have historically lasted for 1-2 years and laid the groundwork for the next bull cycle."

Moreover, we may have seen this movie before in the dot-com bubble. Between 1995 and 2000, the market for new internet companies overheated, attracting overly optimistic business plans and pile-on investments. When the bubble burst, the sector lost 78% of its market cap between 2000 and 2002. But as we all know by the current preponderance of dot-com firms, that was by no means the end of the sector. After reconstituting itself at a more sustainable pace, the internet economy became a leading market mover. (Think Amazon, Netflix, etc.)

While there is no guarantee that crypto will follow the same path, at the very least, certain aspects of the crypto market appear to have staying power. One is the development of DeFi (decentralized finance) platforms, which match borrowers, lenders and traders directly through the use of smart contracts and blockchains. The total value locked in DeFi rose sharply between 2020 and late 2021, briefly exceeding \$200 billion before falling sharply in 2022.

Another positive sign of recovery is the spread of the technologies underpinning crypto. Blockchains are finding applications in a growing number of industries, from automaking to telecommunications. And while crypto has been banned in China, the country has been testing its central-bank-issued digital yuan on a large scale. Additionally, central-bank digital-currency pilot programs have sprung up in India, Singapore, South Africa and elsewhere.

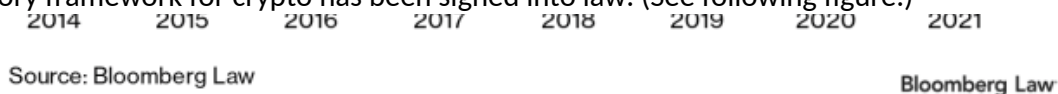
Frontier market, frontier regulation

As with many new technologies, regulation hasn't kept up with crypto's breakneck pace. Part of the problem is that the market is global and thus comes under a wide variety of jurisdictions. Another hurdle is that crypto was designed to allow direct transactions without traditional financial intermediaries, even though exchanges and other service providers now play major roles. And finally, there is the issue we began this article with: What is crypto? If it is a security, then it comes under the authority of the Securities and Exchange Commission (SEC) in the US. But many crypto backers claim it is a commodity. If treated solely as a commodity traded on spot markets, it would not face the comprehensive regulation applied to securities exchanges, such as the New York Stock Exchange.

Movements have been afoot in recent years to bring the market under some form of regulation. A major international banking organization, the Basel Committee, has recommended stringent capital requirements for banks holding certain crypto assets. And Europe is expected to finalize its Markets in Crypto-Assets (MiCA) Regulation this year. The regulation would unify various financial rules and help protect crypto customers.

In the US, several states have passed laws governing digital currency, which vary widely in nature. Bloomberg, a financial news and media company, maintains a [state-by-state list](#), which it updates periodically.

On the federal level, bills continue to be introduced at an ever-increasing pace, with more than 20 submitted in both houses of Congress in 2021. But as of this writing, no comprehensive federal regulatory framework for crypto has been signed into law. (See following figure.)



Still, some action has been taken. The SEC, for its part, has concluded that some digital tokens qualify as securities and that offerings of such securities must be registered unless an exemption applies. And the SEC has been so tough on crypto IPOs in recent months, according to the *Wall Street Journal*, that some firms have either extended their time frame for going public or simply given up, at least for now.

Two former directors of the SEC and the Commodity Futures Trading Commission (CFTC) recommended recently that both of these organizations establish basic standards, such as lending maximums and segregation of customer assets. On the subject of stablecoins, they argued that all issuers should possess adequate reserves "in cash and high-quality liquid assets".

Looking forward, it's probably a good bet that there will be some form of regulatory framework commensurate with crypto's global nature. And it may well be that crypto proponents have a hand in building it as a way of gaining greater public acceptance.

To Bitcoin or not to Bitcoin

So, based on this briefing, is crypto for you? If you think crypto is the tide of the future, you may decide it merits a place in your portfolio. If, however, you are afflicted with FOMO (fear of missing

out), then odds are your decision-making process would be more emotional than rational, which is never a good approach to investing.

For those who are interested in crypto, there are a number of ways to invest:

- Coins
- ICOs (Initial Coin Offerings)
- Equity shares of companies with crypto exposure (Coinbase, MicroStrategy, etc.)
- ETFs (exchange-traded funds) tied to Bitcoin futures or crypto-related companies
- Cryptocurrency futures
- CFDs (contracts for difference, where legally available)

Some crypto lenders also offer interest in return for deposited coins, with stablecoins sometimes earning far more than bank deposits. The failures of several major crypto lenders in 2022, however, demonstrated that these deposits can carry substantial risk and generally lack government insurance. You can also arbitrage your coins by purchasing them on one exchange and then selling them on another at a better price. As a general rule, don't invest more than you can afford to lose.

"The entire crypto market represents less than 1% of the global investable asset universe," StoneX's Matt Weller noted. "So, anything above that allocation may be seen as overweight."

Additionally, you should have hard and fast rules about trading or investing. What is your exit strategy for profit-taking? For downturns? Are you on solid ground funding your trades? Do you have an investment plan (for example, investing a set amount in dollars or pounds per month)? And how will you access your crypto coins? Private keys, which provide digital access to coins, are managed through "wallets," which come in various forms: hot wallets, cold wallets, hardware wallets, mobile wallets, paper wallets, etc.

Hot wallets are connected to the internet and convenient for frequent transactions; a wallet held on an exchange is one common example. Cold wallets, by contrast, keep private keys offline and are generally more secure. Hardware wallets are specialized physical devices, often resembling USB drives, designed to store private keys offline. They tend to offer very strong protection, but they too can be lost, damaged, mishandled or compromised through poor recovery-phrase security.

You will also want to know what affects the market. StoneX's retail trading subsidiary, City Index, has provided a handy list of the following market movers.

- Software upgrades
- Public hype
- Wallet improvements
- Platform applications
- Government regulation
- Support from big industry players

For easy reference to this list and an easy-to-follow guide on purchasing crypto, you can bookmark the [relevant City Index window](#).

Conclusion – 21st century money

Crypto's successes have seldom made the headlines, while its failures have landed with a resounding thud. Many of these failures have been due to old-fashioned human bungling or malfeasance rather than the technology itself. Nonetheless, the question remains whether crypto can live up to its promise as an enduring currency and payment system, one that is accessible and transparent, as well as secure and relatively stable.

A larger question, and one that may hold the answer, is what money will look like in the coming years. We are so used to the US dollar dominating the globe that it is hard to imagine its 102-year reign coming to an end. And yet, that is what Ruchir Sharma, an investor and fund manager, has asserted in a recent Financial Times article. He is not the first to do so. To paraphrase Mark Twain, there have been many occasions when news of the dollar's death as the benchmark currency has been exaggerated. But this time it may be different.

Sharma pointed out that the dollar's dominance has lasted "eight years longer than average for its five predecessors, going back to the 15th century, including most recently the British pound." Hastening the dollar's demise, he argued, are metrics that show it is currently overvalued by about 25%, as well as the expectation that US interest rates and economic growth will lag those of other leading nations. None of this bodes well for the greenback's purchasing power.

If the dollar has had its day, what may follow it is anyone's guess. But it is helpful to understand that money has a shifting and colorful history, from bags of barley to slabs of silver to a plastic card with the words "Diners Club" on it, presumably identifying its owner as a diner. In its current form, whether as a paper note or a row of digits in your bank account, money has no inherent value. It is a "collective fiction," to quote Israeli historian Yuval Noah Harari. This collective fiction has enabled tremendous economic growth, but only because people around the world accept money at its denominated value.

That being the case, there is no reason to believe that the concept of money can't change and broaden once again. This might be especially true in a crisis, say if the US defaults on its debt, causing faith in the leading fiat currency to falter. At that point, rather than relying on another fiat currency, there could be a growing consensus that crypto's time has come, either in its current form or another iteration. Whether that happens is open to conjecture. But as crypto grows in popularity, and as leading economies continue to spend beyond their means, the fork in the road may come sooner than we anticipate.