# Cryptocurrency

Figure 1: A logo for Bitcoin, the first decentralized cryptocurrency

A cryptocurrency (colloquially crypto) is a digital currency designed to work through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. However, a type of cryptocurrency called a stablecoin may rely upon government action or legislation to require that a stable value be upheld and maintained.

Individual coin ownership records are stored in a digital ledger or blockchain, which is a computerized database that uses a consensus mechanism to secure transaction records, control the creation of additional coins, and verify the transfer of coin ownership. The two most common consensus mechanisms are proof of work and proof of stake. Despite the name, which has come to describe many of the fungible blockchain tokens that have been created, cryptocurrencies are not considered to be currencies in the traditional sense, and varying legal treatments have been applied to them in various jurisdictions, including classification as commodities, securities, and currencies. Cryptocurrencies are generally viewed as a distinct asset class in practice.

The first cryptocurrency was bitcoin, which was first released as open-source software in 2009. As of June 2023, there were more than 25,000 other cryptocurrencies in the marketplace, of which more than 40 had a market capitalization exceeding $1 billion. As of April 2025, the cryptocurrency market capitalization was already estimated at $2.76 trillion.

## History

In 1983, American cryptographer David Chaum conceived of a type of cryptographic electronic money called ecash. Later, in 1995, he implemented it through Digicash, an early form of cryptographic electronic payments. Digicash required user software in order to withdraw notes from a bank and designate specific encrypted keys before they could be sent to a recipient. This allowed the digital currency to be untraceable by a third party.

In 1996, the National Security Agency published a paper entitled How to Make a Mint: The Cryptography of Anonymous Electronic Cash, describing a cryptocurrency system. The paper was first published in an MIT mailing list (October 1996) and later (April 1997) in The American Law Review.

In 1998, Wei Dai described “b-money,”an anonymous, distributed electronic cash system. Shortly thereafter, Nick Szabo described bit gold. Like bitcoin and other cryptocurrencies that would follow it, bit gold (not to be confused with the later gold-based exchange BitGold) was described as an electronic currency system that required users to complete a proof of work function with solutions being cryptographically put together and published.

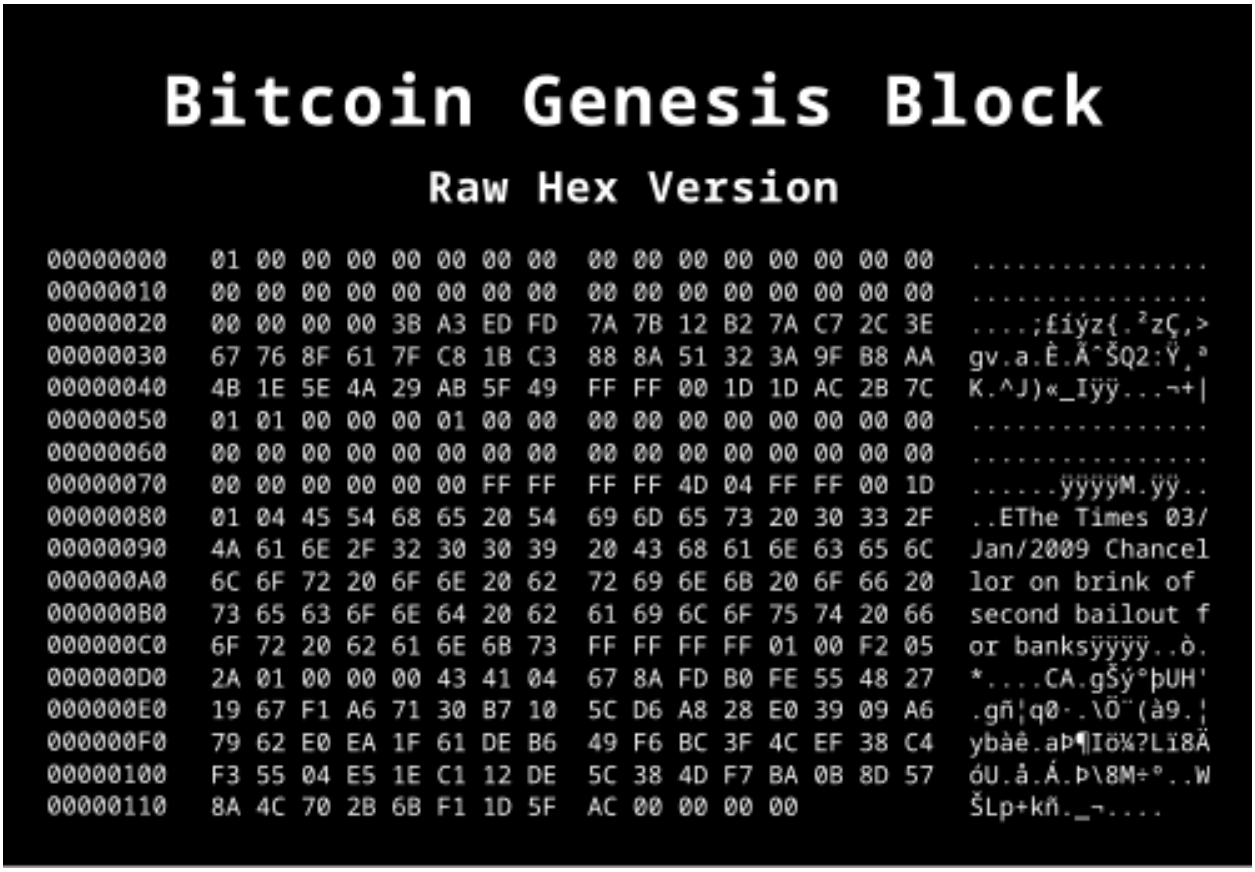


Figure 2: The genesis block of Bitcoin's blockchain, with a note containing The Times newspaper headline. This note has been interpreted as a comment on the instability caused by fractional-reserve banking.: 18

In January 2009, bitcoin was created by pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, in its proof-of-work scheme. In April 2011, Namecoin was created as an attempt at forming a decentralized DNS. In October 2011, Litecoin was released, which used scrypt as its hash function instead of SHA-256. Peercoin, created in August 2012, used a hybrid of proof-of-work and proof-of-stake.

Cryptocurrency has undergone several periods of growth and retraction, including several bubbles and market crashes, such as in 2011, 2013–2014/15, 2017–2018, and 2021–2023.

In August 2014, the UK announced its Treasury had commissioned a study of cryptocurrencies and what role, if any, they could play in the UK economy. The study was also to report on whether regulation should be considered. Its final report was published in 2018, and it issued a consultation on cryptoassets and stablecoins in January 2021.

In June 2021, El Salvador became the first country to accept bitcoin as legal tender, after the Legislative Assembly had voted 62–22 to pass a bill submitted by President Nayib Bukele classifying the cryptocurrency as such.

In August 2021, Cuba followed with Resolution 215 to recognize and regulate cryptocurrencies such as bitcoin.

In September 2021, the government of China, the single largest market for cryptocurrency, declared all cryptocurrency transactions illegal. This completed a crackdown on cryptocurrency that had previously banned the operation of intermediaries and miners within China.

In September 2022, the world's second largest cryptocurrency at that time, Ethereum, transitioned its consensus mechanism from proof-of-work (PoW) to proof-of-stake (PoS) in an upgrade process known as "the Merge". According to the Ethereum Founder, the upgrade would cut both Ethereum's energy use and carbon-dioxide emissions by 99.9%.

On 11 November 2022, FTX Trading Ltd., a cryptocurrency exchange, which also operated a crypto hedge fund, and had been valued at $18 billion, filed for bankruptcy. The financial impact of the collapse extended beyond the immediate FTX customer base, as reported, while, at a Reuters conference, financial industry executives said that "regulators must step in to protect crypto investors."Technology analyst Avivah Litan commented on the cryptocurrency ecosystem that "everything...needs to improve dramatically in terms of user experience, controls, safety, customer service."

## Formal definition

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:

1. The system does not require a central authority; its state is maintained through distributed consensus.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

In March 2018, the word cryptocurrency was added to the Merriam-Webster Dictionary.

### Altcoins

After the early innovation of bitcoin in 2008 and the early network effect gained by bitcoin, tokens, cryptocurrencies, and other digital assets that were not bitcoin became collectively known during the 2010s

as alternative cryptocurrencies, or "altcoins". Sometimes the term "alt coins"was used, or disparagingly, "shitcoins". Paul Vigna of The Wall Street Journal described altcoins in 2020 as "alternative versions of Bitcoin"given its role as the model protocol for cryptocurrency designers. A Polytechnic University of Catalonia thesis in 2021 used a broader description, including not only alternative versions of bitcoin but every cryptocurrency other than bitcoin. As of early 2020, there were more than 5,000 cryptocurrencies.

Figure 3: The logo of Ethereum, the second largest cryptocurrency

Altcoins often have underlying differences when compared to bitcoin. For example, Litecoin aims to process a block every 2.5 minutes, rather than bitcoin's 10 minutes which allows Litecoin to confirm transactions faster than bitcoin. Another example is Ethereum, which has smart contract functionality that allows decentralized applications to be run on its blockchain. Ethereum was the most used blockchain in 2020, according to Bloomberg News. In 2016, it had the largest "following"of any altcoin, according to the New York Times.

Significant market price rallies across multiple altcoin markets are often referred to as an "altseason".

Stablecoins are cryptocurrencies designed to maintain a stable level of purchasing power. Notably, these designs are not foolproof, as a number of stablecoins have crashed or lost their peg. For example, on 11

May 2022, Terra's stablecoin UST fell from $1 to 26 cents. The subsequent failure of Terraform Labs resulted in the loss of nearly $40B invested in the Terra and Luna coins. In September 2022, South Korean prosecutors requested the issuance of an Interpol Red Notice against the company's founder, Do Kwon. In Hong Kong, the expected regulatory framework for stablecoins in 2023/24 is being shaped and includes a few considerations.

Memecoins are a category of cryptocurrencies that originated from Internet memes or jokes. The most notable example is Dogecoin, a memecoin featuring the Shiba Inu dog from the Doge meme. Memecoins are known for extreme volatility; for example, the record-high value for a Dogecoin was 73 cents, but that had plunged to 13 cents by mid-2024. Scams are prolific among memecoins.

## Physical crypto

Physical cryptocurrency coins have been made as promotional items and some have become collectibles. Some of these have a private key embedded in them to access crypto worth a few dollars. There have also been attempts to issue bitcoin "bank notes".

The term "physical bitcoin"is used in the finance industry when investment funds that hold crypto purchased from crypto exchanges put their crypto holdings in a specialised bank called a "custodian".

These physical representations of cryptocurrency do not hold any value by themselves; these are only utilized for collectable purposes. For example, the first incarnation of the bitcoin Casascius, coins made of silver, brass or aluminum sometimes with gold plating, or Titan Bitcoin, which in silver or gold versions are sought after by numismatists.

## Architecture

Cryptocurrency is produced by an entire cryptocurrency system collectively, at a rate that is defined when the system is created and that is publicly stated. In centralized banking and economic systems such as the US Federal Reserve System, corporate boards or governments control the supply of currency.[citation needed] In the case of cryptocurrency, companies or governments cannot produce new units and have not so far provided backing for other firms, banks, or corporate entities that hold asset value measured in it. The underlying technical system upon which cryptocurrencies are based was created by Satoshi Nakamoto.

Within a proof-of-work system such as bitcoin, the safety, integrity, and balance of ledgers are maintained by a community of mutually distrustful parties referred to as miners. Miners use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme. In a proof-of-stake blockchain, transactions are validated by holders of the associated cryptocurrency, sometimes grouped together in stake pools.

Most cryptocurrencies are designed to gradually decrease the production of that currency, placing a cap on the total amount of that currency that will ever be in circulation. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.

### Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp, and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.

### Nodes

A node is a computer that connects to a cryptocurrency network. The node supports the cryptocurrency' s network through either relaying transactions, validation, or hosting a copy of the blockchain. In terms of relaying transactions, each network computer (node) has a copy of the blockchain of the cryptocurrency it supports. When a transaction is made, the node creating the transaction broadcasts details of the transaction using encryption to other nodes throughout the node network so that the transaction (and every other transaction) is known.

Node owners are either volunteers, those hosted by the organization or body responsible for developing the cryptocurrency blockchain network technology, or those who are enticed to host a node to receive rewards from hosting the node network.

Cryptocurrencies use various timestamping schemes to "prove"the validity of transactions added to the blockchain ledger without the need for a trusted third party.

The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and scrypt.

Some other hashing algorithms that are used for proof-of-work include CryptoNote, Blake, SHA-3, and X11.

Another method is called the proof-of-stake scheme. Proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there is currently no standard form of it. Some cryptocurrencies use a combined proof-of-work and proof-of-stake scheme.

### Mining

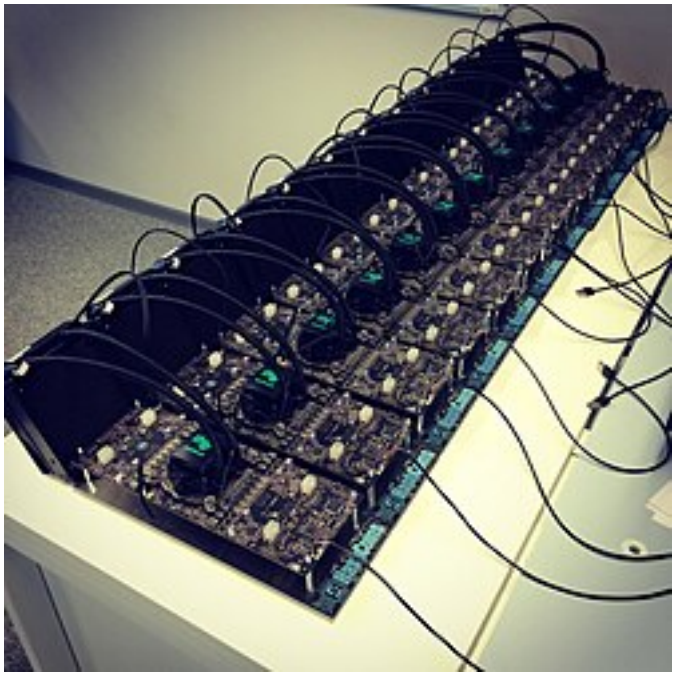

Figure 4: A hashcoin mine

On a blockchain, mining is the validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized hardware such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and scrypt. This arms race for cheaper-yet-efficient machines has existed since bitcoin was introduced in 2009. Mining is measured by hash rate, typically in TH/s. A 2023 IMF working paper found that crypto mining could generate 450 million tons of CO2 emissions by 2027, accounting for 0.7 percent of global emissions, or 1.2 percent of the world total

With more people entering the world of virtual currency, generating hashes for validation has become more complex over time, forcing miners to invest increasingly large sums of money to improve computing performance. Consequently, the reward for finding a hash has diminished and often does not justify the investment in equipment and cooling facilities (to mitigate the heat the equipment produces) and the electricity required to run them.

Popular regions for mining include those with inexpensive electricity, a cold climate, and jurisdictions with clear and conducive regulations. By July 2019, bitcoin's electricity consumption was estimated to be approximately 7 gigawatts, around 0.2% of the global total, or equivalent to the energy consumed nationally by Switzerland.

Some miners pool resources, sharing their processing power over a network to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share"is awarded to members of the mining pool who present a valid partial proof-of-work.

As of February 2018[update], the Chinese government has halted trading of virtual currency, banned initial coin offerings, and shut down mining. Many Chinese miners have since relocated to Canada and Texas. One company is operating data centers for mining operations at Canadian oil and gas field sites due to low gas prices. In June 2018, Hydro Quebec proposed to the provincial government to allocate 500 megawatts of power to crypto companies for mining. According to a February 2018 report from Fortune, Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity.

In March 2018, the city of Plattsburgh, New York put an 18-month moratorium on all cryptocurrency mining in an effort to preserve natural resources and the "character and direction"of the city. In 2021, Kazakhstan became the second-biggest crypto-currency mining country, producing 18.1% of the global exahash rate. The country built a compound containing 50,000 computers near Ekibastuz.

An increase in cryptocurrency mining increased the demand for graphics cards (GPU) in 2017. The computing power of GPUs makes them well-suited to generating hashes. Popular favorites of cryptocurrency miners, such as Nvidia's GTX 1060 and GTX 1070 graphics cards, as well as AMD's RX 570 and RX 580 GPUs, doubled or tripled in price –or were out of stock.

A GTX 1070 Ti, which was released at a price of $450, sold for as much as $1,100. Another popular card, the GTX 1060 (6 GB model), was released at an MSRP of $250 and sold for almost $500. RX 570 and RX 580 cards from AMD were out of stock for almost a year. Miners regularly buy up the entire stock of new GPUs as soon as they are available.

Nvidia has asked retailers to do what they can when it comes to selling GPUs to gamers instead of miners. Boris Böhles, PR manager for Nvidia in the German region, said: "Gamers come first for Nvidia."

Numerous companies developed dedicated crypto-mining accelerator chips, capable of price-performance far higher than that of CPU or GPU mining. At one point, Intel marketed its own brand of crypto accelerator chip, named Blockscale.

### Wallets

A cryptocurrency wallet is a means of storing the public and private "keys"(address) or seed, which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.


Figure 5: An example paper printable Bitcoin wallet consisting of one Bitcoin address for receiving, and the corresponding private key for spending

There exist multiple methods of storing keys or seed in a wallet. These methods range from using paper wallets (which are public, private, or seed keys written on paper), to using hardware wallets (which are hardware to store your wallet information), to a digital wallet (which is a computer with software hosting your wallet information), to hosting your wallet using an exchange where cryptocurrency is traded, or by storing your wallet information on a digital medium such as plaintext.

### Anonymity

Bitcoin is pseudonymous, rather than anonymous; the cryptocurrency in a wallet is not tied to a person but rather to one or more specific keys (or "addresses"). Thereby, bitcoin owners are not immediately identifiable, but all transactions are publicly available in the blockchain. Still, cryptocurrency exchanges are often required by law to collect the personal information of their users.

Some cryptocurrencies, such as Monero, Zerocoin, Zerocash, and CryptoNote, implement additional measures to increase privacy, such as by using zero-knowledge proofs.

A recent 2020 study presented different attacks on privacy in cryptocurrencies. The attacks demonstrated how the anonymity techniques are not sufficient safeguards. In order to improve privacy, researchers suggested several different ideas, including new cryptographic schemes and mechanisms for hiding the IP address of the source.

## Economics

Cryptocurrencies are used primarily outside banking and governmental institutions and are exchanged over the Internet.

### Block rewards

Proof-of-work cryptocurrencies, such as bitcoin, offer block rewards incentives for miners. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the blockchain, but a study suggests that this may not be the case under certain circumstances.

The rewards paid to miners increase the supply of the cryptocurrency. By making sure that verifying transactions is a costly business, the integrity of the network can be preserved as long as benevolent nodes control a majority of computing power. The verification algorithm requires a lot of processing power, and thus electricity, in order to make verification costly enough to accurately validate the public blockchain. Miners have to factor in the costs associated with expensive equipment necessary to stand a chance of solving a hash problem, and consider the significant amount of electrical power in search of the solution. Generally, the block rewards outweigh electricity and equipment costs, but this may not always be the case.

The current value, not the long-term value, of the cryptocurrency supports the reward scheme to incentivize miners to engage in costly mining activities. In 2018, bitcoin's design caused a 1.4% welfare loss compared to an efficient cash system, while a cash system with 2% money growth has a minor 0.003% welfare cost. The main source for this inefficiency is the large mining cost, which is estimated to be US$360 million per year. This translates into users being willing to accept a cash system with an inflation rate of 230% before being better off using bitcoin as a means of payment. However, the efficiency of the bitcoin system can be significantly improved by optimizing the rate of coin creation and minimizing transaction fees. Another potential improvement is to eliminate inefficient mining activities by changing the consensus protocol altogether.

### Transaction fees

Transaction fees (sometimes also referred to as miner fees or gas fees) for cryptocurrency depend mainly on the supply of network capacity at the time, versus the demand from the currency holder for a faster transaction. The ability for the holder to be allowed to set the fee manually often depends on the wallet software used, and central exchanges for cryptocurrency (CEX) usually do not allow the customer to set a custom transaction fee for the transaction.[citation needed] Their wallet software, such as Coinbase Wallet, however, might support adjusting the fee.

Select cryptocurrency exchanges have offered to let the user choose between different presets of transaction fee values during the currency conversion. One of those exchanges, namely LiteBit, previously headquartered in the Netherlands, was forced to cease all operations in August 2023, "due to market changes and regulatory pressure".

The "recommended fee"suggested by the network will often depend on the time of day (due to depending on network load).

For Ethereum, transaction fees differ by computational complexity, bandwidth use, and storage needs, while bitcoin transaction fees differ by transaction size and whether the transaction uses SegWit. In February 2023, the median transaction fee for Ether corresponded to $2.2845, while for bitcoin it corresponded to $0.659.

Some cryptocurrencies have no transaction fees, the most well-known example being Nano (XNO), and instead rely on client-side proof-of-work as the transaction prioritization and anti-spam mechanism.

### Exchanges

Cryptocurrency exchanges allow customers to trade cryptocurrencies for other assets, such as conventional fiat money, or to trade between different digital currencies.

Crypto marketplaces do not guarantee that an investor is completing a purchase or trade at the optimal price. As a result, as of 2020, it was possible to arbitrage to find the difference in price across several markets.

### Atomic swaps

Atomic swaps are a mechanism where one cryptocurrency can be exchanged directly for another cryptocurrency without the need for a trusted third party, such as an exchange.

### ATMs

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States in February 2014. The kiosk installed in Austin, Texas, is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license, or a passport to confirm users'identities.

### Initial coin offerings

An initial coin offering (ICO) is a controversial means of raising funds for a new cryptocurrency venture. An ICO may be used by startups with the intention of avoiding regulation. However, securities regulators in many jurisdictions, including in the U.S. and Canada, have indicated that if a coin or token is an "investment contract"(e.g., under the Howey test, i.e., an investment of money with a reasonable expectation of profit based significantly on the entrepreneurial or managerial efforts of others), it is a security and is subject to securities regulation. In an ICO campaign, a percentage of the cryptocurrency (usually in the form of "tokens") is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, often bitcoin or Ether.

According to PricewaterhouseCoopers, four of the 10 biggest proposed initial coin offerings have used Switzerland as a base, where they are frequently registered as non-profit foundations. The Swiss regulatory agency FINMA stated that it would take a "balanced approach"to ICO projects and would allow "legitimate innovators to navigate the regulatory landscape and so launch their projects in a way consistent with national laws protecting investors and the integrity of the financial system."In response to numerous requests by industry


Figure 6: A Bitcoin ATM

representatives, a legislative ICO working group began to issue legal guidelines in 2018, which are intended to remove uncertainty from cryptocurrency offerings and to establish sustainable business practices.

### Price trends

The market capitalization of a cryptocurrency is calculated by multiplying the price by the number of coins in circulation. The total cryptocurrency market cap has historically been dominated by bitcoin accounting for at least 50% of the market cap value where altcoins have increased and decreased in market cap value in relation to bitcoin. Bitcoin's value is largely determined by speculation among other technological limiting factors known as blockchain rewards coded into the architecture technology of bitcoin itself.

The cryptocurrency market cap follows a trend known as the "halving", which is when the block rewards received from bitcoin are halved due to technological mandated limited factors instilled into bitcoin which in turn limits the supply of bitcoin. As the date reaches near of a halving (twice thus far historically) the cryptocurrency market cap increases, followed by a downtrend.

By June 2021, cryptocurrency had begun to be offered by some wealth managers in the US for 401(k)s.

### Volatility

Cryptocurrency prices are much more volatile than established financial assets such as stocks. For example, over one week in May 2022, bitcoin lost 20% of its value and Ethereum lost 26%, while Solana and Cardano lost 41% and 35% respectively. The falls were attributed to warnings about inflation. By comparison, in the same week, the Nasdaq tech stock index fell 7.6 per cent and the FTSE 100 was 3.6 per cent down.

In the longer term, of the 10 leading cryptocurrencies identified by the total value of coins in circulation in January 2018, only four (bitcoin, Ethereum, Cardano and Ripple (XRP)) were still in that position in early 2022. The total value of all cryptocurrencies was $2 trillion at the end of 2021, but had halved nine months later. The Wall Street Journal has commented that the crypto sector has become "intertwined"with the rest of the capital markets and "sensitive to the same forces that drive tech stocks and other risk assets,"such as inflation forecasts.

### Databases

There are also centralized databases, outside of blockchains, that store crypto market data. Compared to the blockchain, databases perform fast as there is no verification process. Four of the most popular cryptocurrency market databases are CoinMarketCap, CoinGecko, BraveNewCoin, and Cryptocompare.

## Social and political aspects

According to Alan Feuer of The New York Times, libertarians and anarcho-capitalists were attracted to the philosophical idea behind bitcoin. Early bitcoin supporter Roger Ver said: "At first, almost everyone who got involved did so for philosophical reasons. We saw bitcoin as a great idea, as a way to separate money from the state."Economist Paul Krugman argues that cryptocurrencies like bitcoin are "something of a cult" based in "paranoid fantasies"of government power.

David Golumbia says that the ideas influencing bitcoin advocates emerge from right-wing extremist movements such as the Liberty Lobby and the John Birch Society and their anti-Central Bank rhetoric, or, more recently, Ron Paul and Tea Party-style libertarianism. Steve Bannon, who owns a "good stake"in bitcoin, sees cryptocurrency as a form of disruptive populism, taking control back from central authorities.

Bitcoin's founder, Satoshi Nakamoto, supported the idea that cryptocurrencies go well with libertarianism. "It's very attractive to the libertarian viewpoint if we can explain it properly,"Nakamoto said in 2008.

According to the European Central Bank, the decentralization of money offered by bitcoin has its theoretical roots in the Austrian school of economics, especially with Friedrich von Hayek in his book Denationalisation of Money: The Argument Refined, in which Hayek advocates a complete free market in the production, distribution and management of money to end the monopoly of central banks.

## Regulation

The rise in the popularity of cryptocurrencies and their adoption by financial institutions has led some governments to assess whether regulation is needed to protect users. The Financial Action Task Force (FATF) has defined cryptocurrency-related services as "virtual asset service providers"(VASPs) and recommended that they be regulated with the same money laundering (AML) and know your customer (KYC) requirements as financial institutions.

In May 2020, the Joint Working Group on interVASP Messaging Standards published "IVMS 101", a universal common language for communication of required originator and beneficiary information between VASPs. The FATF and financial regulators were informed as the data model was developed.

In June 2020, FATF updated its guidance to include the "Travel Rule"for cryptocurrencies, a measure which mandates that VASPs obtain, hold, and exchange information about the originators and beneficiaries of virtual asset transfers. Subsequent standardized protocol specifications recommended using JSON for relaying data between VASPs and identity services. As of December 2020, the IVMS 101 data model has yet to be finalized and ratified by the three global standard setting bodies that created it.

The European Commission published a digital finance strategy in September 2020. This included a draft regulation on Markets in Crypto-Assets (MiCA), which aimed to provide a comprehensive regulatory framework for digital assets in the EU.

In June 2021, the Basel Committee on Banking Supervision proposed that banks that held cryptocurrency assets must set aside capital to cover all potential losses. For instance, if a bank were to hold bitcoin worth $2 billion, it would be required to set aside enough capital to cover the entire $2 billion. This is a more extreme standard than banks are usually held to when it comes to other assets. However, this is a proposal and not a regulation.

The IMF is seeking a coordinated, consistent and comprehensive approach to supervising cryptocurrencies. Tobias Adrian, the IMF's financial counsellor and head of its monetary and capital markets department said in a January 2022 interview that "Agreeing global regulations is never quick. But if we start now, we can achieve the goal of maintaining financial stability while also enjoying the benefits which the underlying technological innovations bring,"

In May 2024, 15 years after the advent of the first blockchain, bitcoin, the US Congress advanced a bill to the full House of Representatives to provide regulatory clarity for digital assets. The Financial Innovation and Technology for the 21st Century Act, which defines responsibilities between various US agencies, notably between the Commodity Futures Trading Commission (CFTC) for decentralized blockchains and the Securities and Exchange Commission (SEC) for blockchains that are functional but not decentralized. Stablecoins are excluded from both CFTC and SEC regulation in this bill, "except for fraud and certain activities by registered firms."

### China

In September 2017, China banned ICOs to cause abnormal return from cryptocurrency decreasing during announcement window. The liquidity changes by banning ICOs in China was temporarily negative while the liquidity effect became positive after news.

On 18 May 2021, China banned financial institutions and payment companies from being able to provide cryptocurrency transaction related services. This led to a sharp fall in the price of the biggest proof of work cryptocurrencies. For instance, bitcoin fell 31%, Ethereum fell 44%, Binance Coin fell 32% and Dogecoin fell 30%. Proof of work mining was the next focus, with regulators in popular mining regions citing the use of electricity generated from highly polluting sources such as coal to create bitcoin and Ethereum.

In September 2021, the Chinese government declared all cryptocurrency transactions of any kind illegal, completing its crackdown on cryptocurrency.

### Cook Islands

In April 2024, TVNZ's 1News reported that the Cook Islands government was proposing legislation that would allow "recovery agents"to use various means including hacking to investigate or find cryptocurrency that may have been used for illegal means or is the "proceeds of crime."The Tainted Cryptocurrency Recovery Bill was drafted by two lawyers hired by US-based debt collection company Drumcliffe. The proposed legislation was criticised by Cook Islands Crown Law's deputy solicitor general David Greig, who described it as "flawed"and said that some provisions were "clearly unconstitutional". The Cook Islands Financial Services Development Authority described Drumcliffe's involvement as a conflict of interest.

Similar criticism was echoed by Auckland University of Technology cryptocurrency specialist and senior lecturer Jeff Nijsse and University of Otago political scientist Professor Robert Patman, who described it as government overreach and described it as inconsistent with international law. Since the Cook Islands is an associated state that is part of the Realm of New Zealand, Patman said that the law would have "implications for New Zealand's governance arrangements."A spokesperson for New Zealand Foreign Minister Winston Peters confirmed that New Zealand officials were discussing the legislation with their Cook Islands counterparts. Cook Islands Prime Minister Mark Brown defended the legislation as part of the territory's fight against international cybercrime.

### El Salvador

On 9 June 2021, El Salvador announced that it will adopt bitcoin as legal tender, becoming the first country to do so.

### EU

The EU defines crypto assets as "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology."The EU regulation Markets in Crypto-Assets (MiCA) covering asset-referenced tokens (ARTs) and electronic money tokens (EMTs) (also known as stablecoins) came into force on 30 June 2024. As of 17 January 2025, the European Securities and Markets Authority (ESMA) issued guidance to crypto-asset service providers (CASPs) allowing them to maintain crypto-asset services for non-compliant ARTs and EMTs until the end of March 2025.

The rest of MiCA came into force as of 30 December 2024, covering crypto-assets other than ART and EMT and CASPs. MiCA excludes crypto-assets if they qualify as financial instruments according to ESMA guidelines published on 17 December 2024 as well as crypto-assets that are unique and not fungible with other crypto-assets.

### India

At present, India neither prohibits nor allows investment in the cryptocurrency market. In 2020, the Supreme Court of India had lifted the ban on cryptocurrency, which was imposed by the Reserve Bank of India. Since then, an investment in cryptocurrency is considered legitimate, though there is still ambiguity about the issues regarding the extent and payment of tax on the income accrued thereupon and also its regulatory regime. But it is being contemplated that the Indian Parliament will soon pass a specific law to either ban or regulate the cryptocurrency market in India.

Expressing his public policy opinion on the Indian cryptocurrency market to a well-known online publication, a leading public policy lawyer and Vice President of SAARCLAW (South Asian Association for Regional Co-operation in Law) Hemant Batra has said that the "cryptocurrency market has now become very big with involvement of billions of dollars in the market hence, it is now unattainable and irreconcilable for the government to completely ban all sorts of cryptocurrency and its trading and investment". He mooted regulating the cryptocurrency market rather than completely banning it. He favoured following IMF and FATF guidelines in this regard.

**Singapore**

**South Africa**

South Africa, which has seen a large number of scams related to cryptocurrency, is said to be putting a regulatory timeline in place that will produce a regulatory framework. The largest scam occurred in April 2021, where the two founders of an African-based cryptocurrency exchange called Africrypt, Raees Cajee and Ameer Cajee, disappeared with $3.8 billion worth of bitcoin. Additionally, Mirror Trading International disappeared with $170 million worth of cryptocurrency in January 2021.

**South Korea**

In March 2021, South Korea implemented new legislation to strengthen their oversight of digital assets. This legislation requires all digital asset managers, providers and exchanges to be registered with the Korea Financial Intelligence Unit in order to operate in South Korea. Registering with this unit requires that all exchanges are certified by the Information Security Management System and that they ensure all customers have real name bank accounts. It also requires that the CEO and board members of the exchanges have not been convicted of any crimes and that the exchange holds sufficient levels of deposit insurance to cover losses arising from hacks.

**Switzerland**

Switzerland was one of the first countries to implement the FATF's Travel Rule. FINMA, the Swiss regulator, issued its own guidance to VASPs in 2019. The guidance followed the FATF's Recommendation 16, with stricter requirements. According to FINMA's requirements, VASPs need to verify the identity of the beneficiary of the transfer.

**Turkey**

In April 2021, the Central Bank of the Republic of Turkey banned the use of cryptocurrencies and cryptoassets for making purchases on the grounds that the use of cryptocurrencies for such payments poses significant transaction risks.

**United Arab Emirates**

**United Kingdom**

In the United Kingdom, as of 10 January 2021, all cryptocurrency firms, such as exchanges, advisors and professionals that have either a presence, market product or provide services within the UK market must register with the Financial Conduct Authority. On 27 June 2021, the financial watchdog demanded that Binance cease all regulated activities in the UK.

In November 2024, the incoming Labour government confirmed that it will proceed with the regulation of cryptoassets and new UK requirements are expected to come into force in 2026.

**United States**

In 2021, 17 states in the US passed laws and resolutions concerning cryptocurrency regulation. This led the Securities and Exchange Commission to start considering what steps to take. On 8 July 2021, Senator Elizabeth Warren, part of the Senate Banking Committee, wrote to the chairman of the SEC and demanded answers on cryptocurrency regulation due to the increase in cryptocurrency exchange use and the danger this posed to consumers. On 5 August 2021, the chairman, Gary Gensler, responded to Warren's letter and called for legislation focused on "crypto trading, lending and DeFi platforms,"because of how vulnerable investors could be when they traded on crypto trading platforms without a broker. He also argued that many tokens in the crypto market may be unregistered securities without required disclosures or market oversight. Additionally, Gensler did not hold back in his criticism of stablecoins. These tokens, which are

pegged to the value of fiat currencies, may allow individuals to bypass important public policy goals related to traditional banking and financial systems, such as anti-money laundering, tax compliance, and sanctions.

On 19 October 2021, the first bitcoin-linked exchange-traded fund (ETF) from ProShares started trading on the NYSE under the ticker "BITO."ProShares CEO Michael L. Sapir said the ETF would expose bitcoin to a wider range of investors without the hassle of setting up accounts with cryptocurrency providers. Ian Balina, the CEO of Token Metrics, stated that SEC approval of the ETF was a significant endorsement for the crypto industry because many regulators globally were not in favor of crypto, and retail investors were hesitant to accept crypto. This event would eventually open more opportunities for new capital and new people in this space.

The Department of the Treasury, on 20 May 2021, announced that it would require any transfer worth $10,000 or more to be reported to the Internal Revenue Service since cryptocurrency already posed a problem where illegal activity like tax evasion was facilitated broadly. This release from the IRS was a part of efforts to promote better compliance and consider more severe penalties for tax evaders.

On 17 February 2022, the Department of Justice named Eun Young Choi as the first director of a National Cryptocurrency Enforcement Team to help identify and deal with misuse of cryptocurrencies and other digital assets.

The Biden administration faced a dilemma as it tried to develop regulations for the cryptocurrency industry. On one hand, officials were hesitant to restrict a growing industry. On the other hand, they were committed to preventing illegal cryptocurrency transactions. To reconcile these conflicting goals, on 9 March 2022, Biden issued an executive order. Followed this, on 16 September 2022, the Comprehensive Framework for Responsible Development of Digital Assets document was released to support development of cryptocurrencies and restrict their illegal use. The executive order included all digital assets, but cryptocurrencies posed both the greatest security risks and potential economic benefits. Though this might not address all of the challenges in crypto industry, it was a significant milestone in the US cryptocurrency regulation history.

In February 2023, the SEC ruled that cryptocurrency exchange Kraken's estimated $42 billion in staked assets globally operated as an illegal securities seller. The company agreed to a $30 million settlement with the SEC and to cease selling its staking service in the US. The case would impact other major crypto exchanges operating staking programs.

On 23 March 2023, the SEC issued an alert to investors stating that firms offering crypto asset securities might not be complying with US laws. The SEC argued that unregistered offerings of crypto asset securities might not include important information.

On 23 January 2025, President Donald Trump signed Executive Order 14178, Strengthening American Leadership in Digital Financial Technology revoking Executive Order 14067 of 9 March 2022, Ensuring Responsible Development of Digital Assets and the Department of the Treasury's Framework for International Engagement on Digital Assets of 7 July 2022. In addition the order prohibits the establishment, issuance or promotion of Central bank digital currency and establishes a group tasked with proposing a federal regulatory framework for digital assets within 180 days.

## Legality

The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. At least one study has shown that broad generalizations about the use of bitcoin in illicit finance are significantly overstated and that blockchain analysis is an effective crime fighting and intelligence gathering tool. While some countries have explicitly allowed their use and trade, others have banned or restricted it.

According to the Library of Congress in 2021, an "absolute ban"on trading or using cryptocurrencies applies in 9 countries: Algeria, Bangladesh, Bolivia, China, Egypt, Iraq, Morocco, Nepal, and the United Arab Emirates. An "implicit ban"applies in another 39 countries or regions, which include: Bahrain, Benin, Burkina Faso, Burundi, Cameroon, Chad, Cote d'Ivoire, the Dominican Republic, Ecuador, Gabon, Georgia, Guyana, Indonesia, Iran, Jordan, Kazakhstan, Kuwait, Lebanon, Lesotho, Macau, Maldives, Mali, Moldova,

Namibia, Niger, Nigeria, Oman, Pakistan, Palau, Republic of Congo, Saudi Arabia, Senegal, Tajikistan, Tanzania, Togo, Turkey, Turkmenistan, Qatar and Vietnam.

In the United States and Canada, state and provincial securities regulators, coordinated through the North American Securities Administrators Association, are investigating "Bitcoin scams"and ICOs in 40 jurisdictions.

Various government agencies, departments, and courts have classified bitcoin differently. China Central Bank banned the handling of bitcoins by financial institutions in China in early 2014.

In Russia, though owning cryptocurrency is legal, its residents are only allowed to purchase goods from other residents using the Russian ruble while nonresidents are allowed to use foreign currency. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.

In August 2018, the Bank of Thailand announced its plans to create its own cryptocurrency, the Central Bank Digital Currency (CBDC).

### Advertising bans

Cryptocurrency advertisements have been banned on the following platforms:

- Baidu
- Bing—Ended June 2022
- Facebook—Ended December 2021
- Google—Ended August 2021
- Line
- LinkedIn
- MailChimp
- Snapchat
- Tencent
- Twitter
- Weibo
- Yandex

### U.S. tax status

In March 2014, the United States Internal Revenue Service (IRS) ruled that bitcoin will be treated as property for tax purposes. Therefore, virtual currencies are considered commodities subject to capital gains tax.

### Legal concerns relating to an unregulated global economy

As the popularity and demand for online currencies has increased since the inception of bitcoin in 2009, so have concerns that such an unregulated person to person global economy that cryptocurrencies offer may become a threat to society. Concerns abound that altcoins may become tools for anonymous web criminals.

Cryptocurrency networks display a lack of regulation that has been criticized as enabling criminals who seek to evade taxes and launder money. Money laundering issues are also present in regular bank transfers, however with bank-to-bank wire transfers for instance, the account holder must at least provide a proven identity.

Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, and therefore can make tax evasion simpler for individuals. Since charting taxable income is based upon what a recipient reports to the revenue service, it becomes extremely difficult to account for transactions made using existing cryptocurrencies, a mode of exchange that is complex and difficult to track.

Systems of anonymity that most cryptocurrencies offer can also serve as a simpler means to launder money. Rather than laundering money through an intricate net of financial actors and offshore bank accounts, laundering money through altcoins can be achieved through anonymous transactions.

Cryptocurrency makes legal enforcement against extremist groups more complicated, which consequently strengthens them. White supremacist Richard Spencer went as far as to declare bitcoin the "currency of the alt-right".

**Loss, theft, and fraud**

In February 2014, the world's largest bitcoin exchange, Mt. Gox, declared bankruptcy. Likely due to theft, the company claimed that it had lost nearly 750,000 bitcoins belonging to their clients. This added up to approximately 7% of all bitcoins in existence, worth a total of $473 million. Mt. Gox blamed hackers, who had exploited the transaction malleability problems in the network. The price of a bitcoin fell from a high of about $1,160 in December to under $400 in February.

On 21 November 2017, Tether announced that it had been hacked, losing $31 million in USDT from its core treasury wallet.

On 7 December 2017, Slovenian cryptocurrency exchange Nicehash reported that hackers had stolen over $70 million using a hijacked company computer.

On 19 December 2017, Yapian, the owner of South Korean exchange Youbit, filed for bankruptcy after suffering two hacks that year. Customers were still granted access to 75% of their assets.

In May 2018, Bitcoin Gold had its transactions hijacked and abused by unknown hackers. Exchanges lost an estimated $18m and bitcoin Gold was delisted from Bittrex after it refused to pay its share of the damages.

On 13 September 2018, Homero Josh Garza was sentenced to 21 months of imprisonment, followed by three years of supervised release. Garza had founded the cryptocurrency startups GAW Miners and ZenMiner in 2014, acknowledged in a plea agreement that the companies were part of a pyramid scheme, and pleaded guilty to wire fraud in 2015. The SEC separately brought a civil enforcement action in the US against Garza, who was eventually ordered to pay a judgment of $9.1 million plus $700,000 in interest. The SEC's complaint stated that Garza, through his companies, had fraudulently sold "investment contracts representing shares in the profits they claimed would be generated"from mining.

In January 2018, Japanese exchange Coincheck reported that hackers had stolen cryptocurrency worth $530 million.

In June 2018, South Korean exchange Coinrail was hacked, losing over $37 million in crypto. The hack worsened a cryptocurrency selloff by an additional $42 billion.

On 9 July 2018, the exchange Bancor, whose code and fundraising had been subjects of controversy, had $23.5 million in crypto stolen.

A 2020 EU report found that users had lost crypto-assets worth hundreds of millions of US dollars in security breaches at exchanges and storage providers. Between 2011 and 2019, reported breaches ranged from four to twelve a year. In 2019, more than a billion dollars'worth of cryptoassets was reported stolen. Stolen assets "typically find their way to illegal markets and are used to fund further criminal activity".

According to a 2020 report produced by the United States Attorney General's Cyber-Digital Task Force, three categories make up the majority of illicit cryptocurrency uses: "(1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself."The report concluded that "for cryptocurrency to realize its truly transformative potential, it is imperative that these risks be addressed"and that "the government has legal and regulatory tools available at its disposal to confront the threats posed by cryptocurrency's illicit uses".

According to the UK 2020 national risk assessment—a comprehensive assessment of money laundering and terrorist financing risk in the UK—the risk of using cryptoassets such as bitcoin for money laundering and terrorism financing is assessed as "medium"(from "low"in the previous 2017 report). Legal scholars suggested that the money laundering opportunities may be more perceived than real. Blockchain analysis company Chainalysis concluded that illicit activities like cybercrime, money laundering and terrorism financing made up only 0.15% of all crypto transactions conducted in 2021, representing a total of $14 billion.

In December 2021, Monkey Kingdom, a NFT project based in Hong Kong, lost US$1.3 million worth of cryptocurrencies via a phishing link used by the hacker.

On November 2, 2023, Sam Bankman-Fried was pronounced guilty on seven counts of fraud related to FTX. Federal criminal court sentencing experts speculated on the potential amount of prison time likely to be meted out. On March 28, 2024, the court sentenced Bankman-Fried to 25 years in prison.

### Money laundering

According to blockchain data company Chainalysis, criminals laundered US$8,600,000,000 worth of cryptocurrency in 2021, up by 30% from the previous year. The data suggests that rather than managing numerous illicit havens, cybercriminals make use of a small group of purpose built centralized exchanges for sending and receiving illicit cryptocurrency. In 2021, those exchanges received 47% of funds sent by crime linked addresses. Almost $2.2bn worth of cryptocurrencies was embezzled from DeFi protocols in 2021, which represents 72% of all cryptocurrency theft in 2021.

According to Bloomberg and the New York Times, Federation Tower, a two skyscraper complex in the heart of Moscow City, is home to many cryptocurrency businesses under suspicion of facilitating extensive money laundering, including accepting illicit cryptocurrency funds obtained through scams, darknet markets, and ransomware. Notable businesses include Garantex, Eggchange, Cashbank, Buy-Bitcoin, Tetchange, Bitzlato, and Suex, which was sanctioned by the U.S. in 2021. Bitzlato founder and owner Anatoly Legkodymov was arrested following money-laundering charges by the United States Department of Justice.

Dark money has also been flowing into Russia through a dark web marketplace called Hydra, which is powered by cryptocurrency, and enjoyed more than $1 billion in sales in 2020, according to Chainalysis. The platform demands that sellers liquidate cryptocurrency only through certain regional exchanges, which has made it difficult for investigators to trace the money.

Almost 74% of ransomware revenue in 2021 —over $400 million worth of cryptocurrency —went to software strains likely affiliated with Russia, where oversight is notoriously limited. However, Russians are also leaders in the benign adoption of cryptocurrencies, as the ruble is unreliable, and President Putin favours the idea of "overcoming the excessive domination of the limited number of reserve currencies."

In 2022, RenBridge - an unregulated alternative to exchanges for transferring value between blockchains - was found to be responsible for the laundering of at least $540 million since 2020. It is especially popular with people attempting to launder money from theft. This includes a cyberattack on Japanese crypto exchange Liquid that has been linked to North Korea.

### Darknet markets

Properties of cryptocurrencies gave them popularity in applications such as a safe haven in banking crises and means of payment, which also led to the cryptocurrency use in controversial settings in the form of online black markets, such as Silk Road. The original Silk Road was shut down in October 2013 and there have been two more versions in use since then. In the year following the initial shutdown of Silk Road, the number of prominent dark markets increased from four to twelve, while the amount of drug listings increased from 18,000 to 32,000.

Darknet markets present challenges in regard to legality. Cryptocurrency used in dark markets are not clearly or legally classified in almost all parts of the world. In the US, bitcoins are regarded as "virtual assets".[citation needed] This type of ambiguous classification puts pressure on law enforcement agencies around the world to adapt to the shifting drug trade of dark markets.[unreliable source?]

### Wash trades

Various studies have found that crypto-trading is rife with wash trading. Wash trading is a process, illegal in some jurisdictions, involving buyers and sellers being the same person or group, and may be used to manipulate the price of a cryptocurrency or inflate volume artificially. Exchanges with higher volumes can demand higher premiums from token issuers. A study from 2019 concluded that up to 80% of trades on unregulated

cryptocurrency exchanges could be wash trades. A 2019 report by Bitwise Asset Management claimed that 95% of all bitcoin trading volume reported on major website CoinMarketCap had been artificially generated, and of 81 exchanges studied, only 10 provided legitimate volume figures.

#### As a tool to evade sanctions

In 2022, cryptocurrencies attracted attention when Western nations imposed severe economic sanctions on Russia in the aftermath of its invasion of Ukraine in February. However, American sources warned in March that some crypto-transactions could potentially be used to evade economic sanctions against Russia and Belarus.

In April 2022, the computer programmer Virgil Griffith received a five-year prison sentence in the US for attending a Pyongyang cryptocurrency conference, where he gave a presentation on blockchains which might be used for sanctions evasion.

## Impacts and analysis

The Bank for International Settlements summarized several criticisms of cryptocurrencies in Chapter V of their 2018 annual report. The criticisms include the lack of stability in their price, the high energy consumption, high and variable transactions costs, the poor security and fraud at cryptocurrency exchanges, vulnerability to debasement (from forking), and the influence of miners.

#### Speculation, fraud, and adoption

Cryptocurrencies have been compared to Ponzi schemes, pyramid schemes and economic bubbles, such as housing market bubbles. Howard Marks of Oaktree Capital Management stated in 2017 that digital currencies were "nothing but an unfounded fad (or perhaps even a pyramid scheme), based on a willingness to ascribe value to something that has little or none beyond what people will pay for it", and compared them to the tulip mania (1637), South Sea Bubble (1720), and dot-com bubble (1999), which all experienced profound price booms and busts.

Regulators in several countries have warned against cryptocurrency and some have taken measures to dissuade users. However, research in 2021 by the UK's financial regulator suggests such warnings either went unheard, or were ignored. Fewer than one in 10 potential cryptocurrency buyers were aware of consumer warnings on the FCA website, and 12% of crypto users were not aware that their holdings were not protected by statutory compensation. Of 1,000 respondents between the ages of eighteen and forty, almost 70% wrongly assumed cryptocurrencies were regulated, 75% of younger crypto investors claimed to be driven by competition with friends and family, 58% said that social media enticed them to make high risk investments. The FCA recommends making use of its warning list, which flags unauthorized financial firms.

Many banks do not offer virtual currency services themselves and can refuse to do business with virtual currency companies. In 2014, Gareth Murphy, a senior banking officer, suggested that the widespread adoption of cryptocurrencies may lead to too much money being obfuscated, blinding economists who would use such information to better steer the economy. While traditional financial products have strong consumer protections in place, there is no intermediary with the power to limit consumer losses if bitcoins are lost or stolen. One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

The French regulator Autorité des marchés financiers (AMF) lists 16 websites of companies that solicit investment in cryptocurrency without being authorized to do so in France.

An October 2021 paper by the National Bureau of Economic Research found that bitcoin suffers from systemic risk as the top 10,000 addresses control about one-third of all bitcoin in circulation. It is even worse for miners, with 0.01% controlling 50% of the capacity. According to researcher Flipside Crypto, less than 2% of anonymous accounts control 95% of all available bitcoin supply. This is considered risky as a great deal of the market is in the hands of a few entities.

A paper by John Griffin, a finance professor at the University of Texas, and Amin Shams, a graduate student found that in 2017 the price of bitcoin had been substantially inflated using another cryptocurrency, Tether.

Roger Lowenstein, author of "Bank of America: The Epic Struggle to Create the Federal Reserve,"says in a New York Times story that FTX will face over $8 billion in claims.

### Non-fungible tokens

Non-fungible tokens (NFTs) are digital assets that represent art, collectibles, gaming, etc. Like crypto, their data is stored on the blockchain. NFTs are bought and traded using cryptocurrency. The Ethereum blockchain was the first place where NFTs were implemented, but now many other blockchains have created their own versions of NFTs.

### Banks

According to Vanessa Grellet, renowned panelist in blockchain conferences, there was an increasing interest from traditional stock exchanges in crypto-assets at the end of the 2010s, while crypto-exchanges such as Coinbase were gradually entering the traditional financial markets. This convergence marked a significant trend where conventional financial actors were adopting blockchain technology to enhance operational efficiency, while the crypto world introduced innovations like Security Token Offering (STO), enabling new ways of fundraising. Tokenization, turning assets such as real estate, investment funds, and private equity into blockchain-based tokens, had the potential to make traditionally illiquid assets more accessible to investors. Despite the regulatory risks associated with such developments, major financial institutions, including JP-Morgan Chase, were actively working on blockchain initiatives, exemplified by the creation of Quorum, a private blockchain platform.

As the first big Wall Street bank to embrace cryptocurrencies, Morgan Stanley announced on 17 March 2021 that they will be offering access to bitcoin funds for their wealthy clients through three funds which enable bitcoin ownership for investors with an aggressive risk tolerance. BNY Mellon on 11 February 2021 announced that it would begin offering cryptocurrency services to its clients.

On 20 April 2021, Venmo added support to its platform to enable customers to buy, hold and sell cryptocurrencies.

In October 2021, financial services company Mastercard announced it is working with digital asset manager Bakkt on a platform that would allow any bank or merchant on the Mastercard network to offer cryptocurrency services.

### Environmental effects

Mining for proof-of-work cryptocurrencies requires enormous amounts of electricity and consequently comes with a large carbon footprint due to causing greenhouse gas emissions. Proof-of-work blockchains such as bitcoin, Ethereum, Litecoin, and Monero were estimated to have added between 3 million and 15 million tons of carbon dioxide (CO2) to the atmosphere in the period from 1 January 2016 to 30 June 2017. By November 2018, bitcoin was estimated to have an annual energy consumption of 45.8TWh, generating 22.0 to 22.9 million tons of CO2, rivalling nations like Jordan and Sri Lanka. By the end of 2021, bitcoin was estimated to produce 65.4 million tons of CO2, as much as Greece, and consume between 91 and 177 terawatt-hours annually.

Critics have also identified a large electronic waste problem in disposing of mining rigs. Mining hardware is improving at a fast rate, quickly resulting in older generations of hardware.

Bitcoin is the least energy-efficient cryptocurrency, using 707.6 kilowatt-hours of electricity per transaction.

Before June 2021, China was the primary location for bitcoin mining. However, due to concerns over power usage and other factors, China forced out bitcoin operations, at least temporarily. As a result, the United States promptly emerged as the top global leader in the industry. An example of a gross amount of electronic waste associated with bitcoin mining operations in the US is a facility that located in Dalton, Georgia which

is consuming nearly the same amount of electricity as the combined power usage of 97,000 households in its vicinity. Another example is that Riot Platforms operates a bitcoin mining facility in Rockdale, Texas, which consumes approximately as much electricity as the nearby 300,000 households. This makes it the most energy-intensive bitcoin mining operation in the United States.

The world's second-largest cryptocurrency, Ethereum, uses 62.56 kilowatt-hours of electricity per transaction. XRP is the world's most energy efficient cryptocurrency, using 0.0079 kilowatt-hours of electricity per transaction.

Although the biggest PoW blockchains consume energy on the scale of medium-sized countries, the annual power demand from proof-of-stake (PoS) blockchains is on a scale equivalent to a housing estate. The Times identified six "environmentally friendly"cryptocurrencies: Chia, IOTA, Cardano, Nano, Solarcoin and Bitgreen. Academics and researchers have used various methods for estimating the energy use and energy efficiency of blockchains. A study of the six largest proof-of-stake networks in May 2021 concluded:

- Cardano has the lowest electricity use per node;
- Polkadot has the lowest electricity use overall; and
- Solana has the lowest electricity use per transaction.

In terms of annual consumption (kWh/yr), the figures were: Polkadot (70,237), Tezos (113,249), Avalanche (489,311), Algorand (512,671), Cardano (598,755) and Solana (1,967,930). This equates to Polkadot consuming 7 times the electricity of an average U.S. home, Cardano 57 homes and Solana 200 times as much. The research concluded that PoS networks consumed 0.001% the electricity of the bitcoin network. University College London researchers reached a similar conclusion.

Variable renewable energy power stations could invest in bitcoin mining to reduce curtailment, hedge electricity price risk, stabilize the grid, increase the profitability of renewable energy power stations and therefore accelerate transition to sustainable energy.

### Technological limitations

There are also purely technical elements to consider. For example, technological advancement in cryptocurrencies such as bitcoin result in high up-front costs to miners in the form of specialized hardware and software. Cryptocurrency transactions are normally irreversible after a number of blocks confirm the transaction. Additionally, cryptocurrency private keys can be permanently lost from local storage due to malware, data loss or the destruction of the physical media. This precludes the cryptocurrency from being spent, resulting in its effective removal from the markets.

### Academic studies

In September 2015, the establishment of the peer-reviewed academic journal Ledger (ISSN 2379-5980) was announced. It covers studies of cryptocurrencies and related technologies, and is published by the University of Pittsburgh.

The journal encourages authors to digitally sign a file hash of submitted papers, which will then be timestamped into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address in the first page of their papers.

### Aid agencies

A number of aid agencies have started accepting donations in cryptocurrencies, including UNICEF. Christopher Fabian, principal adviser at UNICEF Innovation, said the children's fund would uphold donor protocols, meaning that people making donations online would have to pass checks before they were allowed to deposit funds.

However, in 2021, there was a backlash against donations in bitcoin because of the environmental emissions it caused. Some agencies stopped accepting bitcoin and others turned to "greener"cryptocurrencies. The

U.S. arm of Greenpeace stopped accepting bitcoin donations after seven years. It said: "As the amount of energy needed to run bitcoin became clearer, this policy became no longer tenable."

In 2022, the Ukrainian government raised over US$10,000,000 worth of aid through cryptocurrency following the 2022 Russian invasion of Ukraine.

**Criticism**

Bitcoin has been characterized as a speculative bubble by eight winners of the Nobel Memorial Prize in Economic Sciences: Paul Krugman, Robert J. Shiller, Joseph Stiglitz, Richard Thaler, James Heckman, Thomas Sargent, Angus Deaton, and Oliver Hart; and by central bank officials including Alan Greenspan, Agustín Carstens, Vítor Constâncio, and Nout Wellink.

Investors Warren Buffett and George Soros have respectively characterized it as a "mirage"and a "bubble"; while business executives Jack Ma and JP Morgan Chase CEO Jamie Dimon have called it a "bubble"and a "fraud", respectively, although Jamie Dimon later said he regretted dubbing bitcoin a fraud. BlackRock CEO Laurence D. Fink called bitcoin an "index of money laundering".

In June 2022, business magnate Bill Gates said that cryptocurrencies are "100% based on greater fool theory" .

Legal scholars criticize the lack of regulation, which hinders conflict resolution when crypto assets are at the center of a legal dispute, for example a divorce or an inheritance. In Switzerland, jurists generally deny that cryptocurrencies are objects that fall under property law, as cryptocurrencies do not belong to any class of legally defined objects (Typenzwang, the legal numerus clausus). Therefore, it is debated whether anybody could even be sued for embezzlement of cryptocurrency if they had access to someone's wallet. However, in the law of obligations and contract law, any kind of object would be legally valid, but the object would have to be tied to an identified counterparty. However, as the more popular cryptocurrencies can be freely and quickly exchanged into legal tender, they are financial assets and have to be taxed and accounted for as such.

Losses associated with crytocurrency investments have been linked to suicides. In 2018, an increase in crypto-related suicides was noticed after the cryptocurrency market crashed in August.[citation needed] The situation was particularly critical in Korea as crypto traders were on "suicide watch".[citation needed] The May 2022 collapse of the Luna currency operated by Terra also led to reports of suicidal investors in crypto-related subreddits.