IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

What to Know About Cryptocurrency

Rahul Sharma
Senior Manager
UCO Bank

Share this page

- Facebook
- Twitter
- Linked-In

Cryptocurrency is digital money. That means there's no physical coin or bill — it's all online. You can transfer cryptocurrency to someone online without a go-between, like a bank. Bitcoin and Ether are well-known cryptocurrencies, but new cryptocurrencies continue to be created.

People might use cryptocurrencies for quick payments and to avoid transaction fees. Some might get cryptocurrencies as an investment, hoping the value goes up. You can buy cryptocurrency with a credit card or, in some cases, get it through a process called "mining." Cryptocurrency is stored in a digital wallet, either online, on your computer, or on other hardware.

Before you buy cryptocurrency, know that it does not have the same protections as when you are using U.S. dollars. Also know that scammers are asking people to pay with cryptocurrency because they know that such payments are typically not reversible.

- Cryptocurrencies vs. U.S. Dollars
- Investing in Cryptocurrency
- Paying with Cryptocurrency
- Cryptocurrency Scams
- Cryptojacking
- Report Scams

Cryptocurrencies vs. U.S. Dollars

The fact that cryptocurrencies are digital is not the only important difference between cryptocurrencies and traditional currencies like U.S. dollars.

Cryptocurrencies aren't backed by a government.

Cryptocurrencies are **not** insured by the government like U.S. bank deposits are. This means that cryptocurrency stored online does not have the same protections as money in a bank account. If you store your cryptocurrency in a digital wallet provided by a company, and the company goes out of business or is hacked, the government may not be able to step and help get your money back as it would with money stored in banks or credit unions.

A cryptocurrency's value changes constantly.

A cryptocurrency's value can change by the hour. An investment that may be worth thousands of U.S. dollars today might be worth only hundreds tomorrow. If the value goes down, there's no guarantee that it will go up again.

Investing in Cryptocurrency

As with any investment, before you invest in cryptocurrency, know the risks and how to spot a scam. Here are some things to watch out for as you consider your options.

No one can guarantee you'll make money.

Anyone who promises you a guaranteed return or profit is likely a scammer. Just because an investment is well known or has celebrity endorsements does not mean it is good or safe. That holds true for cryptocurrency, just as it does for more traditional investments. Don't invest money you can't afford to lose.

Not all cryptocurrencies — or companies promoting cryptocurrency — are the same.

Look into the claims that companies promoting cryptocurrency are making. Search online for the name of the company, the cryptocurrency name, plus words like "review," "scam," or "complaint."
Read more about Investing Online.

Paying with Cryptocurrency

If you are thinking about using cryptocurrency to make a payment, know the important differences between paying with cryptocurrency and paying by traditional methods.

You don't have the same legal protections when you pay with cryptocurrency.

Credit cards and debit cards have legal protections if something goes wrong. For example, if you need to dispute a purchase, your credit card company has a process to help you get your money back. Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you only can get your money back if the seller sends it back.

Before you buy something with cryptocurrency, know a seller's reputation, where the seller is located, and how to contact someone if there is a problem.

Refunds might not be in cryptocurrency.

If refunds are offered, find out whether they will be in cryptocurrency, U.S. dollars, or something else. And how much will your refund be? The value of a cryptocurrency changes constantly. Before you buy something with cryptocurrency, learn how the seller calculates refunds.

Some information will likely be public.

Although cryptocurrency transactions are anonymous, the transactions may be posted to a public ledger, like Bitcoin's blockchain. A blockchain is a public list of records that shows when someone transacts with cryptocurrency. Depending on the cryptocurrency, the information added to the blockchain can include information like the transaction amount. The information also can include the sender's and recipient's wallet addresses — a long string of numbers and letters linked to a digital wallet that stores cryptocurrency. Both the transaction amount and wallet addresses could be used to identify who the actual people using it are.

Cryptocurrency Scams

As more people get interested in cryptocurrency, scammers are finding more ways to use it. For example, scammers might offer investment and business "opportunities," promising to double your investment or give you financial freedom. Watch out for anyone who:

- guarantees that you'll make money
- promises big payouts that will double your money in a short time
- promises free money in dollars or cryptocurrency
- makes claims about their company that are not clear

Cryptojacking

Cryptojacking is when scammers use your computer or smartphone's processing power to "mine" cryptocurrency for their own benefit, and without your permission. Scammers can put malicious code onto your device simply by your visiting a website. Then they can help themselves to your device's processor without you knowing.

If you notice that your device is slower than usual, burns through battery power quickly, or crashes, your device might have been cryptojacked. Here is what to do about it:

- Close sites or apps that slow your device or drain your battery.
- Use antivirus software, set software and apps to update automatically, and never install software or apps you do not trust.
- Do not click links without knowing where they lead, and be careful about visiting unfamiliar websites.
- Consider a browser extension or ad blockers that can help defend against cryptojacking. But do your research first. Read reviews and check trusted sources before installing any online tools. Some websites may keep you from using their site if you have blocking software installed.

Report Scams

Report fraud and other suspicious activity involving cryptocurrency, or other digital assets to:

- the FTC at ftc.gov/complaint
- the Commodity Futures Trading Commission (CFTC) at 866-366-2382 or at CFTC.gov/TipOrComplaint
- the U.S. Securities and Exchange Commission (SEC) at sec.gov/tcr

Tagged with: cryptocurrency, invest
October 2018

Cryptocurrency Regulations **In India**

Cryptocurrencies: Not legal tender
Cryptocurrency exchanges: Effectively illegal – regulations being considered

Cryptocurrencies are not legal tender in India, and while exchanges are legal, the government has made it very difficult for them to operate. Although there is currently a lack of clarity over the tax status of cryptocurrencies, the chairman of the Central Board of Direct Taxation has said that anyone making profits from Bitcoin will have to pay taxes on them. Other Income Tax Department sources have suggested that cryptocurrency profits should be taxed as capital gains.

Exchanges

Cryptocurrency exchange regulations in India have grown increasingly harsh. While technically legal, in April 2018 the Reserve Bank of India (RBI) banned banks and any regulated financial institutions from "dealing with or settling virtual currencies". The sweeping regulation prohibited trade of cryptocurrencies on domestic exchanges – and gave existing exchanges until 6 July 2018 to wind down.

Future Regulation

India's government seems to be looking at the possibility of less prohibitive cryptocurrency regulations. In 2017, the Special Secretary of Economic Affairs formed a committee to suggest ways of dealing with the potential AML/CFT and consumer protection issues related to cryptocurrencies. In 2018, reports suggested that a government committee was drafting new legislation which introduced greater cryptocurrency protections for "the common man".

0

- Company

Save my name, and email in this browser for the next time I comment.

Submit Comment

- ***Stacey Roberts***

May 12, 2020 at 12:21 pm

"in April 2018 the Reserve Bank of India (RBI) banned banks and any egulated financial institutions from "dealing with or settling virtual currencies". But now the ban has been lifted by Indian Supreme court in March 5,2020.

10+

Reply

A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership.[1][2] It typically does not exist in physical form (like paper money) and is typically not issued by a central authority. Cryptocurrencies typically use decentralized control as opposed to centralized digital currency and central banking systems.[3] When a cryptocurrency is minted or created prior to issuance or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.[4]

Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency.[5] Since the release of bitcoin, over 6,000 *altcoins* (alternative variants of bitcoin, or other cryptocurrencies) have been created.

Contents

History

See also: History of bitcoin

In 1983, the American cryptographer David Chaum conceived an anonymous cryptographic electronic money called ecash.[6][7] Later, in 1995, he implemented it through Digicash,[8] an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or any 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, first publishing it in an MIT mailing list[9] and later in 1997, in *The American Law Review* (Vol. 46, Issue 4).[10]

In 1998, Wei Dai published a description of "b-money", characterized as an anonymous, distributed electronic cash system.[11] Shortly thereafter, Nick Szabo described bit gold.[12] 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 which required users to complete a proof of work function with solutions being cryptographically put together and published.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by presumably pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme.[13][14] In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256. Another notable cryptocurrency, Peercoin was the first to use a proof-of-work/proof-of-stake hybrid.[15]

On 6 August 2014, the UK announced its Treasury had been commissioned a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered.[16]

Formal definition

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:[17]

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*.[18]

Altcoins

Tokens, cryptocurrencies, and other types of digital assets that are not Bitcoin are collectively known as alternative cryptocurrencies,[19][20][21] typically abbreviated to “altcoins”[22] or “alt coins”.[23] The term is commonly used to describe Ethereum,[24][25][26] Ripple,[27] Litecoin and forks of Litecoin like Dogecoin,[28][29][30] forks of bitcoin like Bitcoin SV,[31] and other coins and tokens created after Bitcoin. Sometimes these coins and tokens are referenced by a more scatological term: "shitcoins".[32]

Paul Vigna of *The Wall Street Journal* also described altcoins as “alternative versions of bitcoin”[33] given its role as the model protocol for altcoin inventors. In October 2018, *The Wall Street Journal* created its own altcoin, called WSJCoin.[34]

Ethereum has the largest “following” of any altcoins that have tried to improve on Bitcoin.[35]

Significant rallies across altcoin markets are often referred to as an “altseason”.[36][37]

Crypto token

A blockchain account can provide functions other than making payments, for example in decentralized applications or smart contracts. In this case, the units or coins are sometimes referred to as crypto tokens (or cryptotokens).The conflicts between token and cryptocurrency remains unsettled. Cryptocurrencies generated by their own blockchain like Bitcoin and Litecoin whereas tokens are usually issued within a smart contract which managed by Ethereum(blockchain network).[38]

Architecture

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In the case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.[39]

As of May 2018, over 1,800 cryptocurrency specifications existed.[40] Within a cryptocurrency system, the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: who use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme.[13]

Most cryptocurrencies are designed to gradually decrease production of that currency, placing a cap on the total amount of that currency that will ever be in circulation.[41] Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.[1] This difficulty is derived from leveraging cryptographic technologies.

Blockchain

Main article: 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.[39][42] Each block typically contains a hash pointer as a link to a previous block,[42] a timestamp and transaction data.[43] By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[44] 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.[45] The public nature of the blockchain ledger protects the integrity of whatever is being transacted since no one entity owns the database. The added work required to solve the encryption in a proof-of-stake system ensures that the public ledger is not modified at random, thus solving the double-spending problem without the need of a trusted authority or central server to administer the database, assuming no 51% attack (that has worked against several cryptocurrencies).[*citation needed*]

Timestamping

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.[15]

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

The 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's currently no standard form of it. Some cryptocurrencies use a combined proof-of-work and proof-of-stake scheme.[15]

Mining

Hashcoin mine

In cryptocurrency networks, *mining* is a 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 machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and Scrypt.[citation needed] This arms race for cheaper-yet-efficient machines has existed since the day the first cryptocurrency, bitcoin, was introduced in 2009.[citation needed] With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the heat they produce, and the electricity required to run them.[46] As of July 2019, bitcoin's electricity consumption is estimated to about 7 gigawatts, 0.2% of the global total, or equivalent to that of Switzerland.[47]

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, the Chinese Government halted trading of virtual currency, banned initial coin offerings and shut down mining. Some Chinese miners have since relocated to Canada.[48] One company is operating data centers for mining operations at Canadian oil and gas field sites, due to low gas prices.[49] In June 2018, Hydro Quebec proposed to the provincial government to allocate 500 MW to crypto companies for mining.[50] According to a February 2018 report from *Fortune*,[51] Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity.

In March 2018, the city of Plattsburgh in upstate 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.[52]

GPU price rise

An increase in cryptocurrency mining increased the demand for graphics cards (GPU) in 2017.[53] (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.[54] A GTX 1070 Ti which was released at a price of $450 sold for as much as $1100. Another popular card GTX 1060's 6 GB model was released at an MSRP of $250, 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 GPU's as soon as they are available.[55]

Nvidia has asked retailers to do what they can when it comes to selling GPUs to gamers instead of miners. "Gamers come first for Nvidia," said Boris Böhles, PR manager for Nvidia in the German region.[56]

Wallets

An example paper printable bitcoin wallet consisting of one bitcoin address for receiving and the corresponding private key for spending

Main article: Cryptocurrency wallet

A cryptocurrency wallet stores the public and private "keys" or "addresses" 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.

Anonymity

Bitcoin is pseudonymous rather than anonymous in that the cryptocurrency within a wallet is not tied to people, but rather to one or more specific keys (or "addresses").[57] Thereby, bitcoin owners are not 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.[citation needed]

Additions such as Zerocoin, Zerocash and CryptoNote have been suggested, which would allow for additional anonymity and fungibility.[58][59]

Fungibility

Main articles: Fungibility and Non-fungible token

Most cryptocurrency tokens are fungible and interchangeable. However, unique non-fungible tokens also exist. Such tokens can serve as assets in games like CryptoKitties.

Economics

Cryptocurrencies are used primarily outside existing 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.[60]

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 public blockchain. Not only do miners have to factor in the costs associated with expensive equipment necessary to stand a chance of solving a hash problem, they further must 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.[61]

The current value, not the long-term value, of the cryptocurrency supports the reward scheme to incentivize miners to engage in costly mining activities. Some sources claim that the current bitcoin design is very inefficient, generating a welfare loss of 1.4% relative to an efficient cash system. The main source for this inefficiency is the large mining cost, which is estimated to be 360 Million USD 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.[62]

Transaction fees

Transaction 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.[citation needed] The currency holder can choose a specific transaction fee, while network entities process transactions in order of highest offered fee to lowest.[citation needed] Cryptocurrency exchanges can simplify the process for currency holders by offering priority alternatives and thereby determine which fee will likely cause the transaction to be processed in the requested time.[citation needed]

For ether, 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 September 2018, the median transaction fee for ether corresponded to $0.017,[63] while for bitcoin it corresponded to $0.55.[64]

Some cryptocurrencies have no transaction fees, and instead rely on client-side proof-of-work as the transaction prioritization and anti-spam mechanism.[65][66][67]

Exchanges

Main article: Cryptocurrency exchange

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

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

Bitcoin ATM

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States on 20 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.[68]

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.[69][70][71]

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 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.[72]

Legality

Main article: Legality of bitcoin by country or territory

The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade,[73] others have banned or restricted it. According to the Library of Congress, an "absolute ban" on trading or using cryptocurrencies applies in eight countries: Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, and the United Arab Emirates. An "implicit ban" applies in another 15 countries, which include Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan.[74] 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.[75]

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 cryptocurrencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble.[76] Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.[77]

Cryptocurrencies are a potential tool to evade economic sanctions for example against Russia, Iran, or Venezuela. Russia also secretly supported Venezuela with the creation of the petro (El Petro), a national cryptocurrency initiated by the Maduro government to obtain valuable oil revenues by circumventing US sanctions.[*citation needed*]

In August 2018, the Bank of Thailand announced its plans to create its own cryptocurrency, the Central Bank Digital Currency (CBDC).[78]

Advertising bans

Cryptocurrency advertisements were temporarily banned on Facebook,[79] Google, Twitter,[80] Bing,[81] Snapchat, LinkedIn and MailChimp.[82] Chinese internet platforms Baidu, Tencent, and Weibo have also prohibited bitcoin advertisements. The Japanese platform Line and the Russian platform Yandex have similar prohibitions.[83]

U.S. tax status

On 25 March 2014, the United States Internal Revenue Service (IRS) ruled that bitcoin will be treated as property for tax purposes. This means bitcoin will be subject to capital gains tax.[84] In a paper published by researchers from Oxford and Warwick, it was shown that bitcoin has some characteristics more like the precious metals market than traditional currencies, hence in agreement with the IRS decision even if based on different reasons.[85]

In July 2019, the IRS started sending letters to cryptocurrency owners warning them to amend their returns and pay taxes.[86]

The legal concern of an unregulated global economy

As the popularity of and demand for online currencies has increased since the inception of bitcoin in 2009,[87] 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.[88]

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.[88]

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.[88]

Loss, theft, and fraud

Main article: Cryptocurrency and security

In February 2014 the world's largest bitcoin exchange, Mt. Gox, declared bankruptcy. The company stated that it had lost nearly $473 million of their customers' bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. The price of a bitcoin fell from a high of about $1,160 in December to under $400 in February.[89]

Two members of the Silk Road Task Force—a multi-agency federal task force that carried out the U.S. investigation of Silk Road—seized bitcoins for their own use in the course of the investigation.[90] DEA agent Carl Mark Force IV, who attempted to extort Silk Road founder Ross Ulbricht ("Dread Pirate Roberts"), pleaded guilty to money laundering, obstruction of justice, and extortion under color of official right, and was sentenced to 6.5 years in federal prison.[90] U.S. Secret Service agent Shaun Bridges pleaded guilty to crimes relating to his diversion of $800,000 worth of bitcoins to his personal account during the investigation, and also separately pleaded guilty to money laundering in connection with another cryptocurrency theft; he was sentenced to nearly eight years in federal prison.[91]

Homero Josh Garza, who 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 U.S. Securities and Exchange Commission separately brought a civil enforcement action 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.[92]

On 21 November 2017, the Tether cryptocurrency announced they were hacked, losing $31 million in USDT from their primary wallet.[93] The company has 'tagged' the stolen currency, hoping to 'lock' them in the hacker's wallet (making them unspendable). Tether indicates that it is building a new core for its primary wallet in response to the attack in order to prevent the stolen coins from being used.

In May 2018, Bitcoin Gold (and two other cryptocurrencies) were hit by a successful 51% hashing attack by an unknown actor, in which exchanges lost estimated $18m.[94] In June 2018, Korean exchange Coinrail was hacked, losing US$37 million worth of altcoin. Fear surrounding the hack was blamed for a $42-billion cryptocurrency market selloff.[95] On 9 July 2018 the exchange Bancor had $23.5 million in cryptocurrency stolen.[96]

The French regulator Autorité des marchés financiers (AMF) lists 15 websites of companies that solicit investment in cryptocurrency without being authorised to do so in France.[97]

Darknet markets

Main article: Darknet market

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.[88] 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.[88]

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 U.S., bitcoins are labelled 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.[98][*unreliable source?*]

Reception

Cryptocurrencies have been compared to Ponzi schemes, pyramid schemes[99] and economic bubbles,[100] such as housing market bubbles.[101] 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).[102] The New Yorker has explained the debate based on interviews with blockchain founders in an article about the "argument over whether Bitcoin, Ethereum, and the blockchain are transforming the world".[103]

While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward them, fearing their lack of central control and the effects they could have on financial security.[104] Regulators in several countries have warned against cryptocurrency and some have taken concrete regulatory measures to dissuade users.[105] Additionally, many banks do not offer services for cryptocurrencies and can refuse to offer services to virtual-currency companies.[106] Gareth Murphy, a senior central banking officer has stated "widespread use [of cryptocurrency] would also make it more difficult for statistical agencies to gather data on economic activity, which are used by governments to steer the economy". He cautioned that virtual currencies pose a new challenge to central banks' control over the important functions of monetary and exchange rate policy.[107] 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.[108] One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

Some companies such as Flexa, Gemini, and NCR Corporation have started integrating them in their POS systems and retailers that have such POS systems (like Starbucks, Wholefoods, Nordstroms, ...) hence offer the possibility of paying with them.[109][110]

Cryptocurrency mining consumes significant quantities of electricity and has a large associated carbon footprint.[111] In 2017, bitcoin mining was estimated to consume 948MW, equivalent to countries the scale of Angola or Panama, respectively ranked 102nd and 103rd in the world. Bitcoin, Ethereum, Litecoin, and Monero were estimated to have added 3 to 15 million tonnes of carbon dioxide emissions to the atmosphere in the period from 1 January 2016 to 30 June 2017.[112] By November 2018, Bitcoin was estimated to have an annual energy consumption of 45.8TWh, generating 22.0 to 22.9 million tonnes of carbon dioxide, rivalling nations like Jordan and Sri Lanka.[113]

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.[114] 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 prevents the cryptocurrency from being spent, resulting in its effective removal from the markets.[115]

The cryptocurrency community refers to pre-mining, hidden launches, ICO or extreme rewards for the altcoin founders as a deceptive practice.[116] It can also be used as an inherent part of a cryptocurrency's design.[117] Pre-mining means currency is generated by the currency's founders prior to being released to the public.[118]

Paul Krugman, winner of the Nobel Memorial Prize in Economic Sciences, has repeated numerous times that it is a bubble that will not last[119] and links it to Tulip mania.[120] American business magnate Warren Buffett thinks that cryptocurrency will come to a bad ending.[121] In October 2017, BlackRock CEO Laurence D. Fink called bitcoin an 'index of money laundering'.[122] "Bitcoin just shows you how much demand for money laundering there is in the world," he said.

Academic studies

Main article: Ledger (journal)

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.[123]

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.[124][125]

Aid agencies

A number of aid agencies have started accepting donations in cryptocurrencies, including the American Red Cross, UNICEF,[126] and the UN World Food Program.

Cryptocurrencies make tracking donations easier and have the potential to allow donors to see how their money is used (financial transparency).

Christopher Fabian, principal adviser at UNICEF Innovation said that UNICEF would uphold existing donor protocols, meaning that those making donations online would have to pass rigorous checks before they were allowed to deposit funds to UNICEF.[127][128]

Indians have a clear favourite when it comes to cryptocurrencies. The world's largest virtual currency by market capitalisation—bitcoin—is the most traded cryptocurrency in India.

Since March when the ban on cryptocurrencies was revoked, bitcoin accounted for 20% of the total traded volumes on WazirX, one of the popular cryptocurrency exchanges in India. Over the last six months, bitcoins worth $184 million were traded on WazirX's platform.

On CoinDCX, another popular crypto exchange, around 78% of the Indian users trade bitcoin since April this year.

"Bitcoin is the flag bearer of cryptocurrencies. Also, it's more liquid and the less volatile compared to other currencies. Hence, most people come to the exchange to buy bitcoins," says Nischal Shetty, CEO of WazirX.

Tether, which is seen as a stable coin as it is pegged against US dollar but this claim hasn't been verified through a public audit, was the second most popular virtual currency on WazirX.

Bitcoin is one of the base currencies for buying altcoins if a user doesn't want to use sovereign-backed money to trade. This too has pushed up the demand for Bitcoin.

Indians, who see cryptocurrencies as a long-term investment, usually buy bitcoin, whereas day-traders usually prefer other virtual currencies, which fluctuate heavily, Shetty of WazirX said.

What has further helped is the surge in the valuation of bitcoin after the outbreak of the pandemic in March as well as an endorsement from some Wall Street veterans.

As cryptocurrencies gain popularity in India, other virtual currencies will also start finding takers. For instance, ethereum, the second largest cryptocurrency by market capitalisation, is gaining popularity on CoinDCX, said its co-founder and CEO, Sumit Gupta. Since April, CoinDCX has also seen investor interest in ripple, tron, and stellar.