ANNAMACHARYA
INSTITUTE OF TECHNOLOGY AND SCIENCES
(AUTONOMOUS)

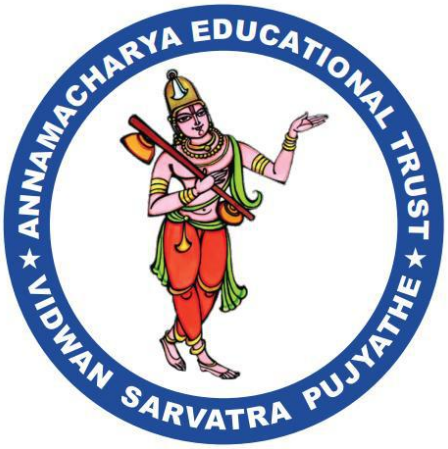
Approved by AICTE, New Delhi & Permanent Affiliation to JNTUA, Anantapur.

Three B. Tech Programmes (CSE , ECE & CE) are accredited by NBA, New Delhi,Accredited by NAAC with 'A' Grade , Bangalore.

A-grade awarded by AP Knowledge Mission. Recognized under sections 2(f) & 12(B) of UGC Act 1956.

Venkatapuram Village, Renigunta Mandal, Tirupati, Andhra Pradesh-517520.

Department of Computer Science and Engineering



Academic Year 2023-24

IV. B.Tech I Semster

Cypto Currencies

(20APE3608)

Prepared By

Mr. S Revanth Babu., M.Tech(Ph.D).
Assistant Professor
Department of CSE, AITS
kingrevu99@gmail.com

UNIT-1 Introduction to cryptocurrencies

History and evolution of cryptocurrencies

What Is Cryptocurrency? Every society since mankind began trading things of value had some type of currency. Notice I used the word currency, not money. The reason for this is because money is merely one form of currency; it is used to transfer VALUE from one party to the next. Now that we are in the digital age, cryptocurrency is simply currency in digital form. In the past, people used all sorts of things to transfer value from one person to the next. At one point, they were using livestock (cattle, goats, sheep, pigs, chickens, etc.). Later, when carrying around a few cows every time you needed to go shopping turned out to be cumbersome, they began trading shells (conch, Telegram Channel : @IRFaraExam puka, conch, etc.) or beads, after that it was bone, metal, and now paper (actually paper money is not really paper at all, it's a secret blend of bamboo and cotton fibers, woven together with silk threads). But I'm sure you've noticed over the past few years, that the need to carry around physical money is not as important or necessary as it once was. People now do much of their buying and selling either online or with credit or debit cards. Eventually, physical money may completely fade from use. What's now taking its place is cryptocurrency, the next step up in a digital form of currency that is traded and managed entirely online. The word cryptocurrency itself is a blend of two Greek words, "crypto," which means "to be hidden or to be kept private." In English, we use these as root words quite often. A crypt is a place where you can hide dead bodies, cryptic – to have a mysterious or hidden meaning, cryptography – the study of breaking codes to find their hidden meaning or the practice of solving them. This is the general idea behind cryptocurrency, the art of writing code (encrypt) or decoding (decrypt). The second word in the blend "currency" refers to the object used to transfer value from one party to the next. Today, that object is money, but in the modern world of cryptocurrency, it is digital code. It is basically the use of a complex code to encrypt data transfers to exchange value. This is done by creating complex mathematical formulas and unique protocols designed to make the codes virtually impossible to break, counterfeit, or duplicate. These protocols then not only protect the transaction between two parties but they also conceal the identity of all those involved. The beauty of cryptocurrency is that it is not under the control of any governmental agency, so there is no centralized institution or political entity responsible for determining its value. The value, therefore, is determined primarily by its users and is based on supply and demand. This causes the price to fluctuate more like that of stocks and bonds. It is used just like you would use a physical currency; you can make purchases, save it, trade it, or even invest it in the same manner. The difference is that you would never hold them in your hands; they only exist as lines of code maintained in a database, and just like with physical currency, you cannot change its value. If you have $20 bill in your hand, there is no way you can change that to $100 or any other value. It is what it is. However, you can always add to it, subtract from it, or save it anytime you like.

History of Cryptocurrency

Cryptocurrency, like all other innovations, was created to solve a particular problem. In the beginning, it was never meant to become the preferred currency Telegram Channel : @IRFaraExam of trade but was to be used as a side product to complement an already existing digital currency system. You probably had no idea that each time you used your debit card, credit card, or had an automatic deposit sent to your bank account, you were using digital currency. Each time you paid your bills online, you were using digital currency. While these tools certainly made life simpler, they presented a major problem, that of double spending. Double spending simply meant that the same money could be spent twice, simply because it could easily be copied. There was always a risk that the possessor could replicate the currency and send it

to another party and still hold on to the original. However, with the introduction of cryptocurrency, for the first time, people could use digital currency without going through a centralized server, without any specialized regulation, or a single authority overseeing everything. The system was based entirely on P2P (person to person) networks used as an assurance against double spending. While it may not have been the original intent of this new monetary instrument, another issue that cryptocurrency resolved was creating a system that eliminated the need for a third-party to be involved in transactions. This automatically provided a more secure system for making online payments. It also eliminated the cost of having to pay exorbitant fees for every transaction made. The new digital currency was designed to be completely independent of any type of central regulation or third-party involvement. Actually, the original intent for cryptocurrency was as a wealth enrichment tool. As there is a cap on the amount of cryptocurrency available on the market, the more people use it, the higher the demand. Therefore, over time, the value of the currency will gradually increase. With this system, all transactions take place between the two parties involved and no any other third parties. No transaction takes place unless there is an absolute consensus and no funds can be transferred unless it is legitimate.

Blockchain Technology

The best way to see how the blockchain works are to compare it with traditional databases. With these, when you put a new transaction on the ledger, you would have to work with a third party that you trusted, like a financial institution or a government, to help record the information and keep it all safe for you. It was the responsibility for these third parties to help build up trust between themselves and their customers. For example, a bank can build up this trust because it has the government behind it, ensuring the money so you will always be able to get your money back out no matter what kind of trouble the bank runs into. This trust is really important when we complete our transactions. Any time that we do a transfer of money, such as when we make payments for goods and services, we have to trust the bank or financial institution that we work with. They will take the exact right amount of our accounts and then give it to the right seller. The seller also has to trust this system as well, trusting that the money will end up in their account and not get lost or be the wrong amount. Over the years, we have learned how to trust credit card companies and banks to do these transactions accurately for us, no matter what seller or store we are working with. We also trust that the company will maintain a database that will maintain all of the transactions and that the company will make sure that they keep all of your personal information safe from hackers and other individuals. We know that when we get onto our accounts, we will be able to see the right amount of money there because the financial institution has shown they can be trustworthy. When it comes to using the blockchain technology, you will be able to get this trust and the same security without needing to rely on those third parties in the process. This is why blockchain is used on Bitcoin and other digital currencies. These currencies are still growing and haven't had the time to build up the trust that is needed, so blockchain helps to add in the trust. These currencies have no government backing, are brand new, and just haven't had the history to see how well they would do. This means that blockchain has some work ahead of it, but it is possible to rely on this technology to complete your transactions. As the database for blockchain is decentralized, it makes it easier for the user to gain trust inside of a system that doesn't have a government or bank behind it. Anyone who is on the blockchain network will be able to view and check on all their transactions, which will make it easier to create transparency and some trust in the network. This is why right now, the most common reason for people to use blockchain ledgers is with Bitcoin and some of the other cryptocurrencies. This technology allows users to complete transactions with each other in just a few minutes while still keeping their information safe. However, there are a few other methods and applications for how you can use the blockchain

technology. The blockchain can handle any kind of valuable information, so any industry that will handle property, shares, money and digital files will be able to benefit from this technology

How Does Blockchain Technology Work?

So, now that we have spent some time talking about blockchain and some of the benefits that come with this technology, it is time to understand how this type of technology is going to work. It is pretty simple for users to use this kind of technology, it only takes a few minutes to do the transactions and you are signed up automatically when you join in a digital currency. But the things that happen behind the scenes are a bit more complex, which helps to provide the trust and security that the system needs.

Decentralized ledger systems

A decentralized ledger is a record of all transactions on a network. This ledger is maintained and updated by many independent nodes, who collaborate based on a ruleset established by the protocol. Bitcoin uses a blockchain and a Proof-of-Work mechanism to organize the network and maintain its decentralized ledger.Traditional banks use centralized ledgers to track balances. Each bank branch periodically updates this central ledger, but this ledger is neither public nor auditable. The Bitcoin protocol changes this paradigm by allowing anyone to read and write directly to the ledger. Anyone is capable of publishing a

Bitcoin transaction. Miners will add that transaction to the blockchain, and anyone can query the blockchain to check their balances and transaction history.All nodes in the Bitcoin network keep and validate identical copies of the ledger so that there exists no central point of failure or fraud. Whereas executives at a traditional bank can conspire to arbitrarily change the ledger at their own bank, no one is capable of dishonestly altering the Bitcoin blockchain. This gives Bitcoin ultimate security and trustworthiness.

Advantages of Distributed Ledgers

While centralized ledgers are prone to cyber attacks, distributed ledgers are inherently harder to attack because all of the distributed copies need to be attacked simultaneously for an attack to be successful. Furthermore, these records are resistant to malicious changes by a single party. By being difficult to manipulate and attack, distributed ledgers allow for extensive transparency.1

Distributed ledgers also reduce operational inefficiencies, speed up the amount of time a transaction takes to complete, and are automated, and therefore function 24/7, all of which reduce overall costs for the entities that use them.

Distributed ledgers also provide for an easy flow of information, which makes an audit trail easy to follow for accountants when they conduct reviews of financial statements. This helps remove the possibility of fraud occurring on the financial books of a company. The reduction in the use of paper is also a benefit to the environment.

Use of Distributed Ledgers

Distributed ledger technology has great potential to revolutionize the way governments, institutions, and corporations work. It can help governments collect tax, issue passports, and record land registries, licenses, and the outlay of Social Security benefits, as well as voting procedures.

The technology is making waves in several industries, including:

- Finance
- Music and entertainment
- Diamond and precious assets
- Artwork
- Supply chains of various commodities

While the distributed ledger technology has multiple advantages, it’s in a budding stage and is still being explored in how to adopt it in the best possible way. One thing is clear, though: The future format of centuries-old ledgers is to be decentralized.

Cryptographic principles

Cryptographic principles are the fundamental concepts and techniques that are used in the field of cryptography to secure communication and protect data. These principles include confidentiality, integrity, authentication, non-repudiation, and key management.

There are several fundamental principles that are important in the field of cryptography, including −

- Confidentiality − Confidentiality refers to the ability to keep information private and secure. Cryptographic techniques, such as encryption, can be used to protect the confidentiality of information by making it unreadable to anyone who does not have the proper decryption key.
- Integrity − Integrity refers to the ability to ensure that information has not been altered or tampered with. Cryptographic techniques, such as hash functions, can be used to ensure the integrity of information by providing a way to detect any changes to the data.
- Authentication − Authentication refers to the process of verifying the identity of a user or device. Cryptographic techniques, such as digital signatures, can be used to authenticate the identity of a user or device in a secure manner.
- Non-repudiation − Non-repudiation refers to the ability to prevent someone from denying that they performed a particular action. Cryptographic techniques, such as digital signatures, can be used to provide non-repudiation by allowing the sender of a message to prove that they sent the message and the receiver to prove that they received the message.
- Key management − Key management refers to the process of generating, distributing, and managing cryptographic keys. Proper key management is essential for the security of a cryptographic system, as the security of the system depends on the secrecy of the key.

Overall, these principles are fundamental to the field of cryptography and are important for ensuring the security and integrity of information.

Security in cryptocurrencies

Is Cryptocurrency Secure?

Blockchain is the technology behind cryptocurrency. The backend process for cryptocurrency transactions is quite complex, and the transactions are recorded into the blocks and time-stamped. Due to its complexity, it is very hard for hackers to get through, making the cryptocurrency pretty secure.

Also, cryptocurrency can become more secure by taking some measures, which we will be discussing further in this article. For now, some basic things must be considered like, a two-stage authentication process while making cryptocurrency transactions. For example, at the time of processing transactions, you need to enter a username first and a verification code that is sent to your personal smartphone via text or email.

This type of security is just not enough; therefore, companies and investors make sure that they invest or even open their own cryptocurrency. They must be aware of the cryptocurrency security standards.

Cryptocurrency Security Standards

What are Cryptocurrency Security standards? It is a set of security requirements for the systems used for cryptocurrency. This includes cryptocurrency exchanges, mobile, and web applications. For increasing cryptocurrency security, it is better to have an information system having cryptocurrency Security standards. This helps to manage and standardize the techniques and perform methods to a particular system for security. Cryptocurrency Security Standards (CCSS) allow the end-users to make smart choices and decisions for purchasing and investing in the right services. Also, the Cryptocurrency Security Standards CCSS helps the customers and investors to make good decisions when allying with the companies.

Mostly, Cryptocurrency Security Standards (CCSS) have ten points that are fulfilled while setting up cryptocurrency security systems. It is a 10 step security put up in 3 levels. Thus the standard is followed by most cryptocurrency exchanges.

The following are the steps that most blockchain companies and organizations follow, and investors must invest in the services of companies following the Cryptocurrency Security Standards:

- Key/seed generation
- Wallet Creation

- Key Storage
- Key Usage
- Key Compromise policy
- Keyholder Grant/ Revoke Policy and Procedures
- Third-party audits
- Data Sanitization Policy
- Proof of Reserve
- Log Audits

How to Protect your Digital Investments?

It is crucial to protect your digital assets, and for that, you must imply cryptocurrency security as it gives the fundamental security aspects. As the cryptocurrency services do not offer a security level as banks, certain risks and precautions must be looked over and implemented while investing in cryptocurrency.

Cryptocurrency security offers safeguards for your crypto assets. It also allows you to trade and invest in cryptocurrency safely. However, there are some things that can be taken care of at a personal level. Few mistakes from your end can save you many dollars or coins. That means there are some risks that you can overcome with proper knowledge about cryptocurrency trading. You can check out cryptocurrency certifications and courses online on blockchain council.

Risks that occur are as follows-

1. Leaving cryptocurrency on a single exchange making it more prone to hackers.
2. Keeping Cryptocurrency locally can have consequences like data can be lost or stolen, as local storage is vulnerable, and someone can track down your transaction and steal it.
3. Another risk is when someone targets you specifically, then Email phishing attacks are prevalent. Also, some standard methods and techniques leading to personal attacks like SIM Swap assaults for clearing the 2-way authentication are used.
4. Cryptocurrency can be lost due to a natural disaster or by any accident. With these unexpected accidents, billions of dollars are the estimated digital currency that has been damaged. However, this cause is usually overlooked by many investors.
5. Another risk that can damage your digital assets is not distributing them to the beneficiaries, which means loss of generation wealth. This comes in the limelight if the person has a sudden death or any complication. We usually don't think about this. Still, when stepping your foot in the crypto world, it's essential to take account of all the possibilities.

How to Protect your Digital Investments?

Cryptocurrency is the major application of blockchain technology, and many professionals use this digital currency to buy goods and services. Therefore, it is essential to protect your digital assets and to keep your cryptocurrency secure. Also, before investing in cryptocurrency, there are some points which you must consider and follow.

- Thorough Run Research on Exchanges

Researching is the first step before investing your time and money into the crypto market. So, learn and understand cryptocurrency exchanges. There are numerous exchanges in the market where you can sell and purchase cryptocurrency. Exchanges are the platform that allows people to do cryptocurrency trading. Therefore, if you plan to start your crypto trading, do your homework, google it, or consult crypto advisors, you must also check reviews of each cryptocurrency exchange and contact experienced investors or cryptocurrency traders. After having proper knowledge, make the decision accordingly.

- Store your Cryptocurrency Safely

Another important point for investing your money into cryptocurrency is to store your cryptocurrency in a wallet but keeping it safe is a challenge. Now, every digital wallet has its own features, security standards, technology used, and advantages. Therefore, it is important to include all these factors and then choose the best-suited wallet as per your security needs.

- Using a Hybrid Strategy will be a wise investment

As most of the wallets are online and gaining popularity, they have become a good investment option. However, hackers look for these types of wallets. Therefore, when it comes to consumer's cryptocurrency, they use offline wallets for cryptocurrency storage and only a little amount is kept online. Users must keep separate their public and private key for their deposit box where cryptocurrency is stored.

- Use a strong password

Always keep the password solid and different. Never repeat a password that you have used for another account. As cryptocurrency is prone to cyber-attacks and hackers attack the accounts with low security. Always have two-way verification before logging in and also keep changing the password after few months.

- Use trustworthy wallets

You must do trading in cryptocurrency through authentic and reliable wallets, brokers, apps, and exchanges. Do not put your money blindly. Invest in exchanges and wallets which follow the cryptocurrency security standards. This includes 2 stage authentication, SSL/TLS encryption, and keeping air-gapped devices offline.

- Keep the key secret

When sending or receiving digital currency, a secret key is used. The ower owns that key which is required to enter before processing any transactions. Therefore, the user must keep that key secretive and do not disclose it to anyone. The private key is very important, and thus it is required to be stored somewhere safe.

Steps to prevent Your Cryptocurrency from Cyber Attacks

Cryptocurrency is a profitable investment when done in the right way. Also, having extensive knowledge plays a vital role in Cryptocurrency trading. Also, cryptocurrency security systems must be included, and some serious measures must be taken to avoid common cyber attacks.

- Try to avoid storing cryptocurrency on digital storage.
- Invest in buying a cryptocurrency hardware wallet.
- Do not use public wifi while making transactions.
- Use private and secured internet connection.
- Also, make sure to keep the security level high and do not install any unsecured apps.
- Use 2-stage authentication and verification for better secure transactions.
- Make sure to stay away from the bitcoin gambling sites.
- Hold cryptocurrency privately.
- Put a unique and robust password.
- Do not share your passwords, key, and wallet details with anyone.

Cyberattacks are very severe, and investors must follow these basic and easy steps at their level to avoid any loss. Also, with the increased demand for cryptocurrency, investing in high-end security systems will be a significant long-term investment.

Cryptocurrency Security Measures

Following the security measures strictly can save your cryptocurrency from any fraud, loss, accident, etc. However, making the right decision can lead you to high profit, whereas a single and minute mistake can bring you losses. When dealing with a critical technology prone to cyber-attacks and a target of hackers, cryptocurrencies must be handled with proper security.

Some of the ways by which you can secure your crypto investments are as follows:

- Cold Wallet is a better option as it is not connected to the internet.
- Using secured Internet Network
- Maintaining multiple wallets
- Ignore phishing Mails
- Keep changing your password
- Make sure to update your devices with the latest software

- Also, have antivirus software to protect your device from viruses and malfunctions.
- Keep your keys separate and with high security.

These few points can make your digital assets secure and away from cyber attacks. Also, make sure to invest in multiple cryptocurrencies and do not hold on to a single currency. There are many cryptocurrencies in which you can start investing. Moreover, it is recommended to invest in stable coins like Tether (USTD), DIA, Paxos Standard (PAX), US Coin (USDC), etc., at the beginning for a safer side.

Popular cryptocurrencies

One of the unique advantages of cryptocurrency is that they are created to fulfill a void in the economy. Unlike traditional dollars and coins, a cryptocurrency can be designed to achieve a certain purpose. Of course, not all cryptocurrencies are the same. Because they are so easy to create, some have been developed as a joke, others for scams, and still others for special events or occasions. However, there are plenty of solid digital currencies to choose from so depending on your needs; there is no doubt that you will find the perfect one for you. Below we will take a closer look at some of the most common currencies available and see why they are so important.

1. Bitcoin Most likely when you think of digital currency, Bitcoin is the name that comes to your mind. Just like the name Xerox is almost synonymous with copy, Bitcoin is often confused and believed to be the only cryptocurrency around. Some people actually refer to it as the "people's currency" because they expect it to be the one cryptocurrency that will uproot and replace all national currencies in the future. Bitcoin was created by a mysteriously anonymous figure, Satoshi Nakamoto, it was the very first digital currency of its kind. It holds the largest market cap to date, placing it well over any other currency on the list. For those interested in investing in cryptocurrencies, the best place to start is with Bitcoin. It is without a doubt the leader of the pack and has had the longest history of any other coins on the market. As a matter of fact, all other coins are referred to as altcoins (alternative coins) because they are viewed as alternatives to Bitcoin. People use them to buy or sell and even to pay for services both on and offline. It is even possible now to pick up Bitcoins through ATM being introduced in some different countries.

While it does require the use of codes to buy or sell Bitcoins, it is not necessary to understand all the technical details to get the benefits they offer.

1. Ethereum (Ether) Like Bitcoin, Ethereum is a public Blockchain digital currency with a few technical differences. Where Bitcoin is geared more towards keeping track of who owns the currency, Ethereum is designed more towards the function of the programming code. Ethereum is most known for its use of Smart Contracts, offering people the ability to code and enact very definite contract terms without the involvement of a third-party. At its basic level, it solves the problem of handling legal contracts online. When a smart contract is put into motion, it works like a self-operating computer program designed to take action automatically once agreed upon conditions are met. Whatever the system is programmed to do, it will follow those procedures exactly. There is no possibility to censor or interfere with the parameters set. Another unique feature of Ethereum is that there are very few limitations on Ethereum's ability to process code. A developer is free to come up with thousands of different applications, so its potential is virtually endless. This currency has been divided into two distinct forms: Ethereum (ETH) and Ethereum Classic (ETC). Created in 2015 by Vitalik Buterin, it has already reached a market cap of more than $1 billion.

1. Ripple Not only is Ripple a digital currency but it is also an open payment network where users can transfer currency from one party to the next. It is designed to work pretty much the same way that Bitcoin does on a decentralized network using the same format that the Internet does with the information. Its

purpose is to make a connection between different payment systems used by different parties. It eliminates the snags of different companies using different systems, so that transfer of funds is practically seamless regardless of the country it is going to.

Not only it will give users the ability to connect with users of other forms of digital currency, but it will also speed up the transfer process and provide more stability. With Ripple, there is no need to wait for confirmation, so every transaction goes through quickly.

1. Monero One of the biggest problems people deal within online technology is that of maintaining privacy, which is Monero's primary concern. While this may present a problem in most western governments, Monero is extremely important in nations where one's identity must be protected at all costs. For example, in the USA when people are concerned about their identity, it is about protecting their assets. They don't want someone to come in and steal the value they have accumulated. However, for someone who lives in places where playing on the economic playground could be perceived as anti-government, secrecy could mean your life. In addition to being private, it is secure, and anything traded through Monero is untraceable. It uses its own unique cryptography that ensures that every transaction made cannot be linked to the parties involved. This is accomplished through the use of multiple keys. Unlike other cryptocurrencies where the user may have one public view key and one private view key, with Monero your public key is provided to generate a one-time public address. The private key, however, is given to the receiver to scan the Blockchain to search for the funds they are to receive. But you will also have a public spend key, a private spend key, which has their own unique functions they are to perform. One of the reasons Monero is so popular is because you can maintain total control over all of your transactions. Therefore, you and only you are responsible for what happens to your money. It is also fungible meaning, and no one can know the history of the money you received.

1. Litecoin Litecoin is very similar to Bitcoin when it comes to code, but there are a few significant functional differences. While both currencies have the same purpose, Litecoin processes much faster than Bitcoin. Since Bitcoin transactions are not complete until they have received confirmation, users must "wait" for "miners" to verify every transaction. This process could take as little as 10 minutes, but it could also take much longer. Litecoin does the same thing in an even shorter time frame. Like Bitcoin, it is a peer-to-peer currency that provides immediate payments to anyplace in the world for a minuscule fee. The same powerful mathematical equations used to provide the network's security also gives each user the ability to manage their own finances. Litecoin uses what is called an Open Source Protocol, which lets developers know where to access the user's source code.

1. Golem The Golem Network has been compared to the Airbnb for computers allowing its users to rent out their computing power to other users online. It allows other machines located in different places around the globe to transact and work together on a particular project. Golem also takes advantage of the same smart contracts capabilities that Ethereum uses. However, like Ethereum allows the user to buy fuel, cars, and pay their owners, Golem does the same thing with computer power. Through Golem users help to create the world's largest supercomputer, an interplanetary network comprised of everything from personal laptops in people's homes to entire data centers; all completely decentralized, meaning no one is monitoring its works. This network would not be owned, managed, or operated by any individual, government, or corporation and it cannot be utilized to monopolize the economy or regulate people's abilities to control their own money, and it can never be shut down. When your computer joins the Golem system it could be used to perform scientific research, render graphics, create Artificial Intelligence, analyze data, or mine for a cryptocurrency.

1. Factom One of the things that Factom is known for is its ability to solve many business challenges because of how it maintains unalterable records. It creates a layer of data using the Bitcoin Blockchain as its foundation. Their distributed ledger technology can maintain millions of records on a Blockchain with just one hash. Businesses, as well as governments, can both use Factom as a means of documenting their data in a way that prevents it from being altered, deleted, or backdated in any way. This assures that all data stored remains intact and ensures user privacy at the same time. Because this information is stored on a decentralized network, the threat of hackers or organizations and their attempts to tamper or interfere with its processes is virtually impossible. Through Factom, users can store all kinds of data making it perfect for all sorts of applications. Medical records, supply chain management, legal applications, and more can make use of this type of cryptocurrency

Whatever problem these currencies address, it must be something you understand. Take the time to learn about the technology behind it, learn about its developers and the team who put it together. It can also be beneficial if you can visualize where that currency will go in the future and see yourself as part of its ultimate goal. Also, it is important to know which merchants you might expect to accept that currency and decide if you are likely to be dealing with that type of business. Once you've learned and understood all of these things, your first decision investing in cryptocurrency is made.

UNIT-2 Cryptocurrency Mining and Consensus Mechanisms

Cryptocurrency mining process

How Does Cryptocurrency Mining Work? To understand mining, one must begin with understanding the Blockchain and how it works. When you think of a Blockchain, it is best to try to visualize it as a public ledger that is constantly being updated every second. It is not under any central control, but as each transaction is completed, it is added to the ledger keeping a running total of everything that is happening with that particular cryptocurrency. The miner's job is to find those Bitcoins, validate each transaction and record every completed transaction as a new block on the Blockchain. To accomplish this, miners need to have the power to search these out. How to Mine Your Cryptocurrency Okay, now let's look at exactly how to find those blocks to add to the chain. There are several steps involved in the mining process. 1. Spending: When a user decides he wants to buy goods from another user he will use his wallet to send 1 Bitcoin to the seller. 1. Announcement: An announcement that 1 Bitcoin payment needs to go to the seller's wallet is broadcast to all the nodes or computers connected to the buyer's wallet. 1. Propagation: The nodes then look at the buyer's spend amount and compares it to any other transactions that may still be pending. If they find no conflicts, the nodes broadcast the transaction to the entire network. 1. Miners will take their copy of the Blockchain and monitor for any new transactions that may be coming. He then works to fit all new and verified transactions into the block. The miner who completes the work faster and provides his work test (the hash) actually receives the reward. Every solved block receives a substantial reward.

1. Confirmation: The miner solves the block and he announces it to the network. If the other nodes are in agreement, the new block is added to the Blockchain, and the miner starts again looking for a new problem to solve.

1. Notification: The seller is notified and can now send his product to the buyer secure in knowing that the funds have been transferred successfully. This process is pretty straightforward, but in some cases, it can become quite complicated. Especially in situations where large sums of money are being transferred where more than one confirmation may be necessary to ensure the validity of the transaction.

Mining algorithms are the functions that make the task of mining cryptocurrency possible. There are various algorithms, each with its own characteristics adapted to the cryptocurrencies that make use of them.

Mining algorithms are the algorithms in charge of making possible the cryptocurrency mining. Normally these algorithms are cryptographic hash functions very complex and they can adjust the mining difficulty. A process that makes it more or less difficult for you to put together the puzzles that must be solved by the miners. This is to get miners to do complex computational work that, once solved, allows them to access a reward for that work.

In this article we will show some of the most used mining algorithms in the world of cryptocurrencies, showing some of their characteristics and potential.

Mining algorithm: which are the most used?

SHA-256, the Bitcoin algorithm

SHA-256 is a cryptographic algorithm that began its history as a hashing system for data. Basically, what SHA-256 does is take a given amount of information and summarize it into a single alphanumeric block 64 characters long that is generated deterministically. This means that if you enter the same data an infinity of times you will have the same output each time.

This is vital to protect data integrity, as the slightest change completely alters the output of the SHA-256 hash. It is for this reason that it is used extensively on the Internet to protect documents and other valuable information that you want to keep intact. It should be noted that SHA-256 is not an encryption algorithm, but rather it is only a data integrity algorithm and the only way to check it is to enter the same information obtaining the same result. Likewise, the opposite process is practically impossible to carry out.

SHA-256 was designed by the US National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) in 2001 as a data integrity standard. The system can be implemented to be generated by means of CPUs, GPUs, FPGAs and ASICs. Hence, Bitcoin mining, which uses SHA-256, can be done on all these media without problems. Of course, the power is different in each case, the least being that which we can obtain in CPUs, passing through FPGAs, GPUs and finally ASICs, which are the ones that currently dominate SHA-256 mining.

Cryptocurrency projects using SHA-256 as the mining algorithm include Bitcoin, Bitcoin Cash, Bitcoin SV, Namecoin (using merged mining), RSK (merged mining), and Stacks (merged mining). There are many other projects that use SHA-256, but most of them are projects without any innovation and therefore of little value within the community.

Ethash, "the Ethereum algorithm"

Ethash was Ethereum's Proof of Work mining algorithm. Proof of work on Ethereum was completely disabled with The Merge, and now Ethereum is secured using proof of stake instead.

This was the hash function designed for Ethereum and one of its main characteristics was its high memory requirement thanks to the use of an extended DAG for mining. In principle, Ethash was designed to prevent ASIC mining. However, the cost of memory was so high that Ethash mining was still possible with GPUs, where GPUs benefit from the large amount of memory they have, making it easy to create the DAG for mining.

Ethash relied on a function called Keccak or SHA-3, in addition to using versions of the Dagger-Hashimoto hashes, so the algorithm was initially known as Dagger-Hashimoto and later changed its name to Ethash.

Scrypt, the most complete cryptographic function

Scrypt is a hash/encryption function designed by well-known FreeBSD developer Colin Percival. The feature was designed to be part of a commercial product he had created called tarsnap, whose purpose is to create remote data backups for users and companies. Tarsnap is a product known for its very high security and speed, something in which Scrypt plays a fundamental role.

Scrypt is an extremely optimized hash function designed to process large amounts of data, offer cryptographic guarantees of integrity and also facilitate data recovery if necessary. Its ability to do secure encryption and decryption adds extra functionality that other hash functions do not have, which is why Scrypt is considered one of the most complete and secure functions that exist, as well as being a free software implementation, thanks to its license BSD 2. Scrypt is an algorithm that can be mined using implementations for CPUs, GPUs, FPGAs, and ASICs, the latter being the most powerful.

Among the main cryptocurrencies that use Scrypt as a mining function are Litecoin and Dogecoin.

X11, the Dash algorithm

The X11 mining algorithm is not actually a hash algorithm, but the union of 11 of them that are applied serially so that the final hash is obtained at the end. The idea behind its creation is to ensure the complete security of the resulting hashes and to add a certain complexity that will prevent the creation of ASICs that centralize mining.

It is worth saying that the first idea is considered by many cryptographic specialists, as a complete absurdity. This is because many algorithms used in X11 do not even have formal verification of their operation. This undermines the security of the system by betting on a "security by obscurity" scheme, since that obscurity is the lack of specific cryptographic tests that ensure that these functions are really secure.

While the second idea of offering ASIC resistance was true, it didn't take long for ASIC developers to overcome this challenge and start offering ASICs for X11. In response, developers began creating variations on the X11 algorithm that prevented ASIC mining until a future firmware update would get the machines back up and running. From these unproductive efforts, derivatives such as X13 (applying 13 different hash functions), X15 and even X17 were born.

The X11 algorithm was designed by Evan Duffield, the creator of Dash, being the first cryptocurrency to use X11 and the only currency of any value to use it.

Equihash, an algorithm based on a complex mathematical problem

Equihash was created thanks to the work of Alex Biryukov and Dmitry Khovratovich, who sought to create a hash algorithm that would offer resistance to ASIC mining. To achieve this, Biryukov and Khovratovich used a curious mathematical problem on which they designed their hash function: the "Birthday Problem" and the results of their work were presented in 2016 at the University of

Luxembourg. This project was run by a group called CryptoLUX, of which they were a part in the Symposium on Security of Networks and Distributed Systems 2016 in San Diego.

The "Birthday Problem" tells us that:

Out of a set of 23 people, there is a 50,7% chance that at least two of them have birthdays on the same day. For 57 or more people the probability is greater than 99,666%. Strictly speaking this is not a paradox since it is not a logical contradiction.

However, it is a mathematical truth that contradicts common intuition. Many people think that the probability is much lower, and that it takes many more people to reach the 50,666% probability. If a room had 367 people, by the Pigeonhole Principle we know that there would be at least two people having a birthday on the same date, since a normal year has 365 days, and a leap year has 366.

Based on this, the Equihash function leads computers to perform memory-intensive operations that make parallel computation difficult. This is because it is extremely expensive to create ASICs with large amounts of high-speed, high-bandwidth memory.

As a result, Equihash is one of the most problematic ASIC resistant algorithms. In fact, even today this algorithm represents quite a challenge for ASICs (which finally managed to overcome the resistance), since they are not capable of reaching high levels of solutions to the problem, which makes these devices quite energy inefficient, albeit much faster than their CPU, FPGA and GPU counterparts.

The main currency that uses this algorithm is Zcash, although it is also used by Bitcoin Gold and Komodo.

Cryptonight, the first algorithm for anonymous coins
CryptoNight is a unique algorithm for a well-known reason in the community: it is meant to make it easy to build anonymous coins. In fact, the person (or group of people) who built the algorithm is a complete mystery, on the same level as Satoshi Nakamoto. Different users claim that the creator of CryptoNote (the base consensus algorithm for CryptoNight) is Satoshi Nakamoto himself acting under a new pseudonym: Nicholas van Saberhagen. To add more mysticism, CryptoNote was presented on 12/12/12, a complete riddle that no one has been able to solve to this day.

In any case, CryptoNight was developed as a hash function for CryptoNote and the first coin to implement it was Bytecoin. The algorithm is designed from the ground up to provide a very high level of privacy, anonymity, and resistance to ASICs and GPUs. To provide a high level of security and anonymity, one of its main features is its high resistance to ASIC and GPU mining, making it extremely difficult to develop for these devices.

However, with the abandonment of Bytecoin, Monero, the second coin to implement the function for its mining, took the reins of development thanks to a larger and more specialized development group, together with a more active community. Thus, Monero became the main developer of CryptoNight and constantly updated it to prevent ASICs from wreaking havoc against it. Despite the effort, CryptoNight lost the battle and understanding this point, the Monero developers announced that they were working on its successor, declaring CryptoNight to be abandoned soon.

Currently, CryptoNight is a little used and abandoned algorithm. In fact, most of the projects that use it are abandoned.

RandomX, the evolution of CryptoNight
The Monero community, seeing that it had lost the battle in CryptoNight, understood the need to develop a new algorithm from scratch. In this way, a new front could be opened for privacy coins.

The result of all that effort is RandomX. This is an algorithm for privacy coins so complex that it is theoretically impossible to implement in an ASIC. In fact it is extremely complex to implement efficiently for GPUs and FPGAs.

RandomX owes its operation to an implementation that works based on a computational introspection virtual machine. Basically, RandomX creates a virtual machine with certain cryptographic characteristics that are randomly generated. On this virtual machine, its cryptographic function for Monero mining is launched. All of this makes RandomX demanding. It requires RAM memory capacity, CPU instructions and their cache, as well as the cryptographic calculation necessary for its operation, which is based on AES-256, and also makes use of the Blake2b and Argon2d functions.

The implementation has been so successful that almost 3 years after the algorithm was created, there is still no efficient implementation for GPUs and FPGAs. And indeed, the ASCI implementation is still theoretically impossible. All this ends up making the use of these tools unfeasible, leading everyone to mine with the CPU, the goal of RandomX.

CuckooCycle, Cuckaroo and Beam, mining for GPUs and private coins
CuckooCycle is a PoW mining algorithm used by the Aeternity project. The algorithm is intended to be used on GPUs, where it is efficient and resistant to ASIC mining. CuckooCycle is memory intensive requiring at least 4GB of GPU RAM in order to start the mining process. At the moment there is no ASIC that operates on this algorithm and the only currency of relevance that uses it is Aeternity.

For its part, Cuckaroo is a mining algorithm used by privacy coins like Grin y MimbleWimble. The algorithm is intended to be used on GPUs and resist ASIC mining. However, the algorithm has undergone several updates, as many of its old iterations are no longer considered ASIC-resistant. This has led to the creation of variants such as Cuckarood29, Cuckatoo31 or Cuckatoo32, which seek to solve this problem.

Finally, Beam is the mining algorithm used by privacy cryptocurrency Beam. This algorithm is a derivative of Equihash and is designed to be used on GPUs. In terms of Beam mining, Nvidia cards show the best results, although the difference with AMD GPUs is minimal and the energy efficiency of the latter is much higher.

Mining hardware

However, to do this, you must have the right hardware on hand. If you hope to become a cryptocurrency miner, then you will have to have more than just a simple computer to get the job done. Here is what you'll need:

● CPU The CPU or the Central Processing Unit is the key component in your computer that handles the everyday processes that your system needs. Its primary purpose is to make the big decisions for your computer's functions. It is comprised of the electronic circuitry and performs all the functions of a

computer program. While in the beginning, this was the only way to mine for currency, it was not the most efficient. While the CPU is no longer the primary way to mine cryptocurrency, it is still used to earn a little money on the network. Many miners will use their CPU to join a mining pool. By doing this, they can combine their computing power with others to earn money. The potential for earning will still be limited in this way, but if you're just interested in a few earnings, you can definitely garner a little cash this way.

● GPU The GPU of a computer is responsible for the real heavy lifting a computer does. It manages the graphics processing and does all the complex mathematical computations involved in running videos. It is much faster than CPU mining and is considerably more powerful. Many miners may have a system that maintains multiple GPU units to get the most power and speed possible.

● FPGA The Field Programmable Gate Array is a piece of hardware that is solely dedicated to mining. It is considered to be the next level of mining as it has increased the speed and efficiency of mining many times over. An added bonus of setting up your mining platform using the FPGA is that it draws very little power and you can keep it running 24-hours a day earning your profit around the clock.

● ASIC The last in a long line of mining technology is the ASIC (Application Specific Integrated Circuit chips. First introduced in 2013, they have been steadily improving with each passing year. Like the FPGA, they have only one job, and that is to mine 24/7.

When it comes to mining, speed is extremely important, and with new hardware like the FPGA and the ASIC, older and slower systems will never be able to compete. While you can still mine with CPUs and GPUs, your potential for profit in the world of mining will depend largely on how fast your computer can troll the network for those transactions. Getting set up to mine for cryptocurrency doesn't have to be hard. Before you can do that, however, you need to decide if you're going to be a lone miner or join a pool. Depending on which avenue you choose to take you'll have to set up your mining business differently. Let's start with the individual miner and how to get set up.

1. Set up your own virtual private server (VPS) to perform the mining. This should be set aside to only use for your mining operations

2. Access your VPS

3. Follow the commands to set up the system to start mining.

4. Start mining

It is important to know that the energy required to mine can be quite extensive, so many choose to join mining pools. While you won't make as much money as you would individually, you'll save on energy in the process. You also have the option of installing specialized mining software that can run on your local machine and it can be run on as many servers as you want to speed up the process. Once you're registered on your server, all you need is your email address you used to sign up and follow the commands. When all of that is in place, you're ready to start mining and make money.

Consensus mechanisms: Proof-ofWork (PoW), Proof-of-Stake (PoS)

What Is Proof-of-Stake (PoS)?

Proof-of-stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. In the case of cryptocurrency, the database is called a blockchain—so the consensus mechanism secures the blockchain.

Learn more about proof-of-stake and how it is different from proof-of-work. Additionally, find out the issues proof-of-stake attempts to address within the cryptocurrency industry.

KEY TAKEAWAYS

- Under proof-of-stake (POS), validators are chosen based on the number of staked coins they have.
- Proof-of-stake (POS) was created as an alternative to proof-of-work (POW), the original consensus mechanism used to validate transactions and open new blocks.
- While PoW mechanisms require miners to solve cryptographic puzzles, PoS mechanisms require validators to hold and stake tokens for the privilege of earning transaction fees.
- Proof-of-stake (POS) is seen as less risky regarding the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous.
- The next block writer on the blockchain is selected at random, with higher odds being assigned to nodes with larger stake positions.

Understanding Proof-of-Stake (PoS)

Proof-of-stake reduces the amount of computational work needed to verify blocks and transactions. Under proof-of-work, hefty computing requirements kept the blockchain secure. Proof-of-stake changes the way blocks are verified using the machines of coin owners, so there doesn't need to be as much computational work done. The owners offer their coins as collateral—staking—for the chance to validate blocks and earn rewards.1

Validators are selected randomly to confirm transactions and validate block information. This system randomizes who gets to collect fees rather than using a competitive rewards-based mechanism like proof-of-work.1

To become a validator, a coin owner must "stake" a specific amount of coins. For instance, Ethereum requires 32 ETH to be staked before a user can operate a node.1 Blocks are validated by multiple validators, and when a specific number of validators verify that the block is accurate, it is finalized and closed.

To activate your own validator, you'll need to stake 32 ETH; however, you don't need to stake that much ETH to participate in validation. You can join validation pools using "liquid staking" which uses an ERC-20 token that represents your ETH.2
Different proof-of-stake mechanisms may use various methods to reach a consensus. For example, when Ethereum introduces sharding, a validator will verify the transactions and add them to a shard block, which requires no more than 128 validators to form a voting "committee."3 Once shards are validated and a block created, two-thirds of the validators must agree that the transaction is valid, then the block is closed.

How Is Proof-of-Stake Different From Proof-of-Work?

Both consensus mechanisms help blockchains synchronize data, validate information, and process transactions. Each method has proven successful at maintaining a blockchain, although each has pros and cons. However, the two algorithms have very different approaches.

Under PoS, block creators are called validators. A validator checks transactions, verifies activity, votes on outcomes, and maintains records. Under PoW, block creators are called miners. Miners work to solve for the hash, a cryptographic number, to verify transactions. In return for solving the hash, they are rewarded with a coin.

To "buy into" the position of becoming a block creator, you need to own enough coins or tokens to become a validator on a PoS blockchain. For PoW, miners must invest in processing equipment and incur hefty energy charges to power the machines attempting to solve the computations.

The equipment and energy costs under PoW mechanisms are expensive, limiting access to mining and strengthening the security of the blockchain. PoS blockchains reduce the amount of processing power needed to validate block information and transactions. The mechanism also lowers network congestion and removes the rewards-based incentive PoW blockchains have.

Proof of Stake	**Proof of Work**
Block creators are called validators	Block creators are called miners
Participants must own coins or tokens to become a validator	Participants must buy equipment and energy to become a miner
Energy efficient	Not energy efficient
Security through community control	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards

Goals of Proof-of-Stake

Proof-of-stake is designed to reduce network congestion and address environmental sustainability concerns surrounding the proof-of-work (PoW) protocol. Proof-of-work is a competitive approach to verifying transactions, which naturally encourages people to look for ways to gain an advantage, especially since monetary value is involved.

Bitcoin miners earn bitcoin by verifying transactions and blocks. However, they pay their operating expenses like electricity and rent with fiat currency. So what's really happening is that miners exchange energy for cryptocurrency, which causes PoW mining to use as much energy as some small countries.4

The PoS mechanism seeks to solve these problems by effectively substituting staking for computational power, whereby the network randomizes an individual's mining ability. This means there should be a drastic reduction in energy consumption since miners can no longer rely on massive farms of single-purpose hardware to gain an advantage. For example, Ethereum's transition from PoW to PoS reduced the blockchain's energy consumption by 99.84%.5

The first cryptocurrency to adopt the PoS method was Peercoin. It was followed by Nxt, Blackcoin, and ShadowCoin soon after.6

Proof-of-Stake Security

Long touted as a threat to cryptocurrency fans, the 51% attack is a concern when PoS is used, but there is doubt it will occur. Under PoW, a 51% attack is when an entity controls more than 50% of the miners in a network and uses that majority to alter the blockchain. In PoS, a group or individual would have to own 51% of the staked cryptocurrency.

It's very expensive to control 51% of staked cryptocurrency. Under Ethereum's PoS, if a 51% attack occurred, the honest validators in the network could vote to disregard the altered blockchain and burn the offender(s) staked ETH. This incentivizes validators to act in good faith to benefit the cryptocurrency and the network.1

Most other security features of PoS are not advertised, as this might create an opportunity to circumvent security measures. However, most PoS systems have extra security features in place that add to the inherent security behind blockchains and PoS mechanisms.1

What Is Proof-of-Stake vs. Proof-of-Work?

Proof-of-Stake (POS) uses randomly selected validators to confirm transactions and create new blocks. Proof-of-Work (POW) uses a competitive validation method to confirm transactions and add new blocks to the blockchain.

Is Proof-of-Stake a Certificate?

Proof-of-Stake is a consensus mechanism where cryptocurrency validators share the task of validating transactions. There are currently no certificates issued.

How Do You Earn Proof-of-Stake?

Proof of Stake (POS) is a built-in consensus mechanism used by a blockchain network. It cannot be earned, but you can help secure a network and earn rewards by using a cryptocurrency client that participates in PoS validating or becoming a validator.7

Can Bitcoin Be Converted to Proof-of-Stake?

It's possible that Bitcoin can change to proof-of-stake. However, it takes years to implement successfully, and the community would need to agree to the change.

The Bottom Line

Proof-of-stake is a mechanism used to verify blockchain transactions. It differs from proof-of-work significantly, mainly in the fact that it incentivizes honest behavior by rewarding those who put their crypto up as collateral for a chance to earn more.

Mining pools

What Is a Mining Pool?

A mining pool is a joint group of cryptocurrency miners who combine their computational resources over a network to strengthen the probability of finding a block or otherwise successfully mining for cryptocurrency.

KEY TAKEAWAYS

- Cryptocurrency mining pools are groups of miners who share their computational resources.
- Mining pools utilize these combined resources to strengthen the probability of finding a block or otherwise successfully mining for cryptocurrency.
- If the mining pool is successful and receives a reward, that reward is divided among participants in the pool.

How a Mining Pool Works

Individually, participants in a mining pool contribute their processing power toward the effort of finding a block. If the pool is successful in these efforts, they receive a reward, typically in the form of the associated cryptocurrency.

Rewards are usually divided between the individuals who contributed, according to the proportion of each individual's processing power or work relative to the whole group. In some cases, individual miners must show proof of work in order to receive their rewards.

Rewards are usually split among the miners based on the agreed terms and on their respective contributions to the mining activity.

Anyone who wants to make a profit through cryptocurrency mining has the choice to either go solo with their own dedicated devices or to join a mining pool where multiple miners and their devices combine to enhance their hashing output. For example, attaching six mining devices that each offers 335 megahashes per second (MH/s) can generate a cumulative 2 gigahashes of mining power, thereby leading to faster processing of the hash function.

Mining Pool Methods

Not all cryptocurrency mining pools function in the same way. There are, however, a number of common protocols that govern many of the most popular mining pools.

Proportional mining pools are among the most common. In this type of pool, miners contributing to the pool's processing power receive shares up until the point at which the pool succeeds in finding a block. After that, miners receive rewards proportional to the number of shares they hold.

Pay-per-share pools operate somewhat similarly in that each miner receives shares for their contribution. However, these pools provide instant payouts regardless of when the block is found. A miner contributing to this type of pool can exchange shares for a proportional payout at any time.

Peer-to-peer mining pools, meanwhile, aim to prevent the pool structure from becoming centralized. As such, they integrate a separate blockchain related to the pool itself and designed to prevent the operators of the pool from cheating as well as the pool itself from failing due to a single central issue.

Benefits of a Mining Pool

While success in individual mining grants complete ownership of the reward, the odds of achieving success is very low because of high power and resource requirements. Mining is often not a profitable venture for individuals. Many cryptocurrencies have become increasingly difficult to mine in recent years as the popularity of these digital currencies has grown and the costs associated with expensive hardware necessary to be a competitive miner as well as electricity oftentimes outweigh the potential rewards.

Mining pools require less of each individual participant in terms of hardware and electricity costs and increase the chances of profitability. Whereas an individual miner might stand little chance of successfully finding a block and receiving a mining reward, teaming up with others dramatically improves the success rate.

Disadvantages of a Mining Pool

By taking part in a mining pool, individuals give up some of their autonomy in the mining process. They are typically bound by terms set by the pool itself, which may dictate how the mining process is approached. They are also required to divide up any potential rewards, meaning that the share of profit is lower for an individual participating in a pool.

A small number of mining pools, such as AntPool, Poolin, and F2Pool dominate the bitcoin mining process, according to blockchain.com.1 Although many pools do make an effort to be decentralized, these groups consolidate much of the authority to govern the bitcoin protocol. For some cryptocurrency proponents, the presence of a small number of powerful mining pools goes against the decentralized structure inherent in bitcoin and other cryptocurrencies.

UNIT-3 Cryptocurrency Wallets and Security

Types of cryptocurrency wallets

A crypto wallet is used to interact with a blockchain network. The three major types of crypto wallets are hardware, software, and paper wallets. Based on their work, they can be further classified as cold or hot wallets. Software-based wallets are more accessible and more convenient, whereas hardware ones are the most secure. Paper wallets are printed out on paper and are now unreliable and obsolete. In reality, crypto wallets don't store the currency but act as a tool of interaction with blockchain, i.e., generating the necessary information to receive and send money via blockchain transactions.

The information comprises pairs of private and public keys. Based on these keys, an alphanumeric identifier called address is generated. In essence, this address specifies the location to which coins can be sent to the blockchain. The address can be shared to receive funds, but private keys are to be never disclosed. The private key can be used on any wallet for accessing the cryptocurrency. As long as the private key is known, funds are accessible on any device. Also, coins are just transferred from one address to another, never leaving the blockchain.

Types of wallets

A wallet is a combination of a public address and a private key. The wallets can be categorized based on the method and location of storage in the following segments:

Hot and Cold Wallets

Internet connectivity defines a wallet in terms of hot or cold. Hot wallets are connected to the Internet and thus are less secure and pose more risks but are user-friendly. Cold wallets, on the other hand, are stored offline and don't require internet connectivity. Thus, improving security and less risk. When compared to a safe or a vault, more substantial sums of money can be stored than that in a carry-around wallet. Hot wallets are more likely to be used for daily transactions, and cold wallets for more long-term holdings. Hot wallets are easy to set up, and the funds are quickly accessible. Traders conveniently use them. Cold wallets are hack resistant, and thus the cold storage is suitable for HODLers. As a protection method, only a small percent is stored in hot wallets while being able to trade directly from their cold storage devices.

Hardware wallets

Hardware wallets are hardware devices that individually handle public addresses and keys. It looks like a USB with an OLED screen and side buttons. It is a battery-less device and can be connected to a PC and accessed by native desktop apps. It costs up to 70-150 dollars, but it is worth it. They have received a mixed response. They are more secure than hot wallets and user-friendlier than paper wallets but less than web and desktop wallets. They are available in different forms and offer reasonable amounts of control. They are difficult for beginners to use when the investment is significant. The Most popular hardware wallets are Ledger Nano S and Trezor.

Paper Wallets

It is a physically printed QR coded form wallet. Some wallets allow downloading the code to generate new addresses offline. They are not prone to hacks, but the number of flaws has made them dangerous. A major flaw is not being able to send partial funds. Thus, it can't be reused. They used to be very popular for cold storage, but not after hardware wallets came onto the scene. All in all, if stringent security precautions are taken, then paper wallets can be set up.

Desktop Wallets

These are installable software packs available for operating systems and are becoming serious with time. Anti-virus is required because a system connected to the Internet poses fundamental security issues. Instead of keeping cryptos on an exchange, desktop wallets for bitcoins should be used. They are the third most secure way to store cryptocurrencies and the best method for cold storage in a completely clean system. They are easy to use, give privacy and anonymity, and involve no third party. Regular backing up of the computer is needed. Popular desktop wallets are Exodus, Bitcoin core, Electrum, etc.

Mobile Wallets

Mobile wallets are just like desktop wallets made for smartphones. They are quite convenient as it uses QR codes for transactions. They are suitable for daily operations but are vulnerable to malware infection. Encryption of mobile wallets is necessary. They are practical and can be used on the go but open to viruses. Some mobile wallets are Coinomi and Mycelium.

Web Wallets

As the name suggests, these wallets are accessed by internet browsers. The private keys are held in some web wallets and are prone to DDOS attacks. They can be hosted or non-hosted. Non-hosted is preferred as funds are always in control. They are the least secure wallets. They are not the same as hot wallets. They are ideal for small investments and allow quick transactions. Some of these are MetaMask and Coinbase.

Public and private keys in cryptocurrencies

Every new crypto wallet comes with a corresponding pair of cryptographically generated keys, one public and one private. Public keys can be safely shared with anybody attempting to send crypto to your wallet. Private keys, on the other hand, should be carefully protected, as anyone with a wallet's private keys gains total control over the funds associated with them. Depending on the type of wallet you use (custodial vs. non-custodial), you may never even interact with your private keys. But rest assured they're being used anytime you buy, sell, swap or spend crypto, whether you're aware of it or not.

Public keys vs. Private keys

Private keys and public keys perform very different functions, and both are necessary bookends to ensure crypto transactions are conducted securely. These keys usually take the form of lengthy strings of alphanumeric characters which are cryptographically linked, meaning any transaction encrypted by a public key can only be decrypted using its corresponding private key. This encryption method is known as "asymmetric-key cryptography".

What is a public key?

A public key, as the name suggests, is viewable by others. You can think of it like your checking account and routing numbers. You can safely provide your public key to anybody trying to send you funds, whether it's in an email signature, on a website or on a social media post. The only thing somebody with your public key will be able to do is send funds to your wallet and see your wallet balance, so sharing it

presents no immediate security risk. Public keys are actually mathematically generated from their corresponding private key, but the process is not reversible.

What is a private key?

Unlike public keys, your private key should never be shared with anyone, as whoever has a wallet's private key can access the funds it contains. To more privacy minded crypto users, this unwillingness to share private keys even extends to centralized exchanges, many of which provide custodial wallets that manage private keys on users' behalf. The alternative side to custody services is using a self-custody wallet in which you are in full control of your private keys. Possession of private keys is a rather contentious issue in the world of cryptocurrency, with many believing you don't actually "own" your crypto unless you are the sole possessor of your private key. This point of view has given rise to the popular "not your keys, not your crypto" adage in some crypto circles.

Back up your wallet! Always remember to record your recovery phrase (aka seed phrase). This is the best way to protect your private key and keep your funds secure in case you lose access to your wallet.

What is the role of public and private keys during crypto transactions?

No matter which type of wallet you use, whether you self-custody or use a custodial exchange wallet, all crypto transactions must be digitally "signed" with a private key to be completed.

Once you initiate a transaction, your wallet constructs the transaction containing the to address, from address and amount (in addition to other metadata). Your keys are used to create a digital signature confirming the transaction is legitimate. Once the signed transaction is sent to the network, the nodes verify the signature and that the from address has enough funds to complete the transaction.

Learn more about consensus mechanisms used to confirm transactions.

In the case of custodial wallets, the exchange or service provider holds on to your keys, automatically signing transactions for you whenever a request is made. Some crypto users prefer this set up as it lessens their responsibility – regaining access to a lost account is as easy as tapping "Forgot password?". However, this also means that a custodial service has the power to make transactions without your consent, restrict access to your assets or even lose your funds in hacks, liquidation or bankruptcy (see examples like Mt. Gox and FTX). More security-minded crypto users prefer to take banking into their own hands, opting instead for a non-custodial wallet (aka self-custody). With a non-custodial option like the BitPay Wallet, you'll be the only one with access to your private keys, and therefore, to your funds.

How should I protect my private keys?

If using a custodial wallet service, there is no surefire way to protect your keys since you do not control them. Only work with a company you feel you can trust. Do your homework, and read up on an exchange or wallet provider's reputation and business practices before allowing an institution to custody your funds.

If you're self-custodying, losing your private key could render your funds irretrievable. The best way to keep your private keys safe are:

Never share your private keys with anyone (aside from trusted next of kin)

Use a recovery phrase/seed phrase to back up private key; similarly, only share this recovery phrase with someone you wish to have access to your funds

Never take a screenshot of your private key/seed phrase, or any kind of digital photo for that matter. If you have a large amount of cryptocurrency, it's always best to keep your private keys offline, such as with hardware wallets, which only connect to the internet to sign transactions. A far less technical but still very much offline method is to simply write your recovery phrase on a piece of paper which you then hide or keep under lock and key. Just make sure nobody else can find it, except any designated next-of-kin who may be unable to access the funds without it if something unexpected happens to you.

Wallet security measures & Best practices for securing cryptocurrency assets.

How to protect your crypto wallet

1. Use a secure platform

When choosing a digital wallet, use a secure and reputable platform. Do some research to ensure that the platform has a good reputation and has security measures to protect users' private keys.A bit of research can go a long way in ensuring the security of your digital wallet. By only dealing with good actors in the space, you can minimize your risk.

2. Use a strong password

When creating your account, use a strong password that can't be easily guessed by someone else. Avoid common words like "password" or your date of birth. Instead, use a combination of letters, numbers, and special characters.You can use a password generator like LastPass to create a strong, unique password for your account.

3. Use a hardware wallet to store your private keys offline

One of the most secure ways to store your private keys is on a hardware wallet. Hardware wallets are physical devices that allow you to store your private keys offline. This means that even if your computer is hacked, your private keys will be safe.Two reputable hardware wallets are the Ledger Nano S and the Trezor.

4. Enable two-factor authentication

If a platform offers two-factor authentication, be sure to enable it. This adds an extra layer of security to your account by requiring you to enter a code from your phone or another device in addition to your password.While not foolproof, two-factor authentication can go a long way in protecting your account from being hacked.

5. Keep your software up to date

Keep your digital wallet software up to date with the latest security patches. By doing this, you'll be able to protect yourself against any new security vulnerabilities discovered.

6. Make use of multiple crypto wallets

You don't have to rely on just one digital wallet. In fact, it's often a good idea to use multiple wallets. This way, if one wallet is compromised, your other assets will still be safe.

7. Avoid public Wifi

When accessing your digital wallet, avoid doing so from public Wifi. This could be a hot spot for hackers looking to steal people's private keys. Here we prepared for you a guide on how to use public WiFi safely, so don't forget to check it too.Better yet, always use a good VPN for crypto wallets. This will encrypt your traffic and make it much harder for hackers to steal your private keys. We recommend using ClearVPN service for it's high connection speed and security. Download ClearVPN app for you device here.

8. Don't share your private keys

It goes without saying that you need to keep your private keys safe and secure. Avoid sharing them with anyone other than a family with whom you'll entrust your estate in the event something happens to you.

9. Backup your digital wallet

Be sure to back up your digital wallet in case you lose access to your account or device. This will ensure that you don't lose your funds if something happens to your device.Come up with a schedule for backing up your digital wallet and stick to it. That way, you'll always have a recent backup to fall back on.

10. Keep your recovery phrase safe

If you're using a software wallet, you'll be given a recovery phrase when you set it up. This is a string of words that can be used to regain access to your account if you forget your password. Keep this phrase safe and secure in a location only you have access to

11. Cold Storage

A cold wallet is used offline for storing bitcoins or other cryptocurrencies. With a cold wallet, also originally known as cold storage, the digital wallet is stored on a platform not connected to the internet, thereby protecting the wallet from unauthorized access, cyber hacks, and other vulnerabilities that a system connected to the internet is susceptible to.

Cold storage methods are useful for individual investors, but cryptocurrency exchanges and companies involved in the crypto space also make use of this type of wallet. Cold storage also can refer more broadly to other modes of operation for storing inactive data, such as data for regulatory compliance, video, photographs, and backup information.

UNIT-4 Cryptocurrency Trading and Investment strategies

Cryptocurrency market analysis and trends

Cryptocurrency Market Analysis

The Cryptocurrency Market size in terms of transaction value is expected to grow from USD 1.33 trillion in 2023 to USD 5.02 trillion by 2028, at a CAGR of 30.40% during the forecast period (2023-2028).

Cryptocurrency is the new age financial innovation designed not only to become an alternative to cash but also to support the existing systems.

Cryptocurrencies which are designed to use for peer-to-peer transactions without being liable to any government or a central bank are the latest financial innovations explored not only for the reasons of their being but also for potential risks and opportunities in the financial industry. There are thousands of cryptocurrencies with various design goals. These design goals are to provide a digital currency alternative to cash (Bitcoin, Monero, and Bitcoin cash), to support a payment system at low cost (Ripple, Particl, and Utility Settlement Coin), to support peer-to-peer trading activity by creating tokens (RMG and Maecenas), to facilitate secure access to a good or service in peer-to-peer trading (Golem, Filecoin) and to support underlying platform or protocol (Ether and NEO). These design goals mentioned won't be exhaustive as new cryptocurrencies are being created every week. Blockchain is the underlying technology for most cryptocurrencies.

The cryptocurrency market is segmented based on the market capitalization of a large number of cryptocurrencies. Cryptocurrencies overlap with key areas of the monetary and financial system. Given their rapid growth, complexity, high volatility, and potentiality for facilitating illicit activities, regulators and policymakers across the world are bothered about their inclusion into the existing system and revising the existing systems to fit them, if included.

Cryptocurrency Industry Segmentation

An understanding of the present status of the cryptocurrency market, along with detailed market analysis, their structural intricacies explained in simple terms, risks and opportunities, current regulatory frameworks, and impact on existing systems. In-depth analysis of the impact on monetary and fiscal policies. Cryptocurrency is the new age financial innovation designed not only to become a cash alternative but also to support the existing systems. Cryptocurrencies are segmented based on the market capitalization of cryptocurrencies (Bitcoin, Ethereum, Ripple, Bitcoin Cash, Cardano, and others) and cryptocurrency adoption by geography (Middle East & Africa, Americas, Europe, APAC). The report offers market size and forecast values for the Cryptocurrency Market in USD million for the above segments.

Geography

Americas (US, Canada, Latin America and Caribbean)

Europe

UK

Asia-Pacific

Middle East & Africa

By Market Capitalization

Bitcoin

Ethereum

Ripple

Bitcoin Cash

Cardano

Others

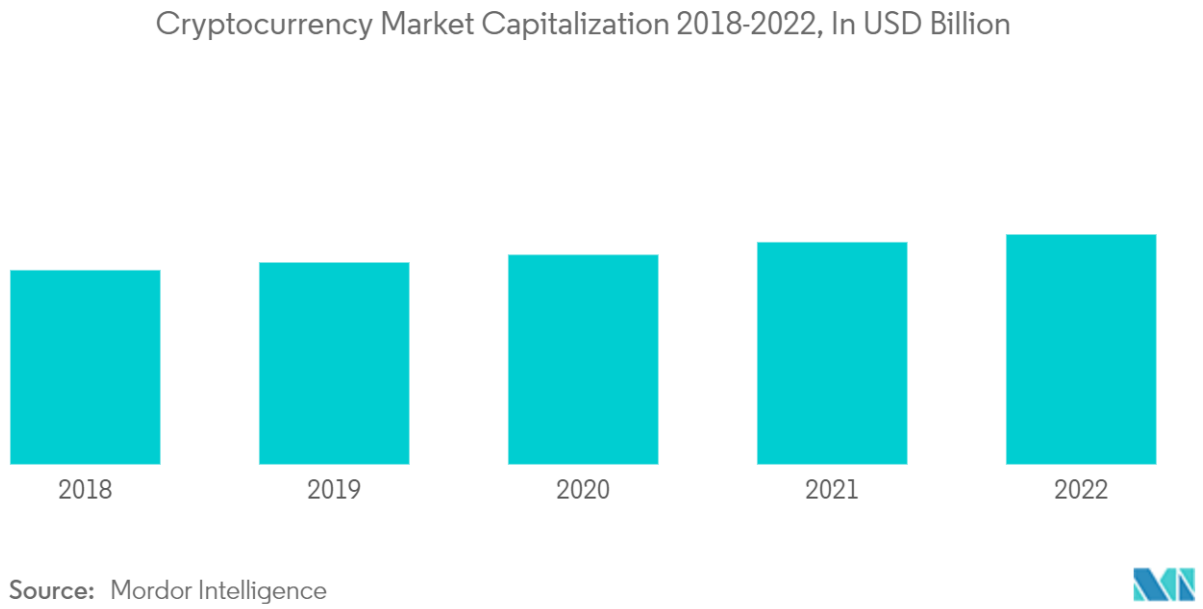
Cryptocurrency Market Trends

This section covers the major market trends shaping the Cryptocurrency Market according to our research experts:

A Brief on the Volatility in the Market Capitalization of Cryptocurrencies

With the evolving nature of this market with new cryptocurrencies created every week, it is difficult to know how big the cryptocurrency market is. A wide scope of market exchanges for cryptocurrency trading, spread across the globe because of their privacy protection features as well as rapid growth, extreme price volatility, and market illiquidity add to the complexity of the cryptocurrency market. The market capitalization of cryptocurrencies over the years shows how high the price volatility of the market is.

The estimated cryptocurrency market capitalization, for example, during January 2022, varied between 400 billion USD and 800 billion USD which was 566 billion USD at the beginning of the year 2022 and finally settled at 128 billion USD by the end of the year 2022. In terms of transaction volumes, bitcoin alone had the highest number of 200,000 average daily transactions.



Trading strategies

What is a trading strategy?

We can describe a trading strategy as an extensive plan for all your trading activities. It's a framework you create to guide you in all your trading endeavors.

A trading plan can also help mitigate financial risk, as it eliminates a lot of unnecessary decisions. While having a trading strategy is not mandatory for trading, it can be life-saving at times. If something unexpected happens in the market (and it will), your trading plan should define how you react – and not your emotions. In other words, having a trading plan in place makes you prepared for the possible outcomes. It prevents you from making hasty, impulsive decisions that often lead to big financial losses.

For instance, a comprehensive trading strategy may include the following:

what asset classes you trade

what setups you take

what tools and indicators you use

what triggers your entries and exits (your stop loss placement)

what dictates your position sizing

how you document and measure your portfolio performance

In addition, your trading plan may also contain other general guidelines, even down to some minor details. For example, you can define that you will never trade on Fridays or that you will never trade if you are feeling tired or sleepy. Or you can establish a trading schedule, so you only trade on specific days of the week. Do you keep checking the Bitcoin price during the weekend? Always close your positions before the weekend. Personalized guidance like this can also be included in your trading strategy.

Devising a trading strategy may also include verification by backtesting and forward testing. For instance, you could do paper trading on the Binance Futures testnet.

In this article, we'll consider two types of trading strategies: active and passive.

As you'll shortly see, the definitions of trading strategies aren't necessarily strict, and there may be overlap between them. In fact, it may be worth considering a hybrid approach by combining multiple strategies.

Active trading strategies

Active strategies require more time and attention. We call them active because they involve constant monitoring and frequent portfolio management.

Day trading

Day trading might be the most well-known active trading strategy. It's a common misconception to think that all active traders are by definition day traders, but that isn't true.Day trading involves entering and exiting positions on the same day. As such, day traders aim to capitalize on intraday price movements, i.e., price moves that happen within one trading day.The term "day trading" stems from the traditional markets, where trading is open only during specific hours of the day. So, in those markets, day traders never stay in positions overnight, when trading is halted.

Most digital currency trading platforms are open 24 hours a day, 365 days a year. So, day trading is used in a slightly different context when it comes to the crypto markets. It typically refers to a short-term trading style, where traders enter and exit positions in a timespan of 24 hours or less.

Day traders will typically use price action and technical analysis to formulate trade ideas. Besides, they may employ many other techniques to find inefficiencies in the market.

Day trading cryptocurrency can be highly profitable for some, but it's often quite stressful, demanding, and may involve high risk. As such, day trading is recommended for more advanced traders.

Swing trading

Swing trading is a type of longer-term trading strategy that involves holding positions for longer than a day but typically not longer than a few weeks or a month. In some ways, swing trading sits in the middle between day trading and trend trading.Swing traders generally try to take advantage of waves of volatility that take several days or weeks to play out. Swing traders may use a combination of technical and fundamental factors to formulate their trade ideas. Naturally, fundamental changes may take a longer time to play out, and this is where fundamental analysis comes into play. Even so, chart patterns and technical indicators can also play a major part in a swing trading strategy.Swing trading might be the most convenient active trading strategy for beginners. A significant benefit of swing trading over day trading is that swing trades take longer to play out. Still, they're short enough so that it's not too hard to keep track of the trade.This allows traders more time to consider their decisions. In most cases, they have enough time to react to how the trade is unfolding. With swing trading, decisions can be made with less haste and more rationality. On the other hand, day trading often demands fast decisions and speedy execution, which isn't ideal for a beginner.

Trend trading

Sometimes also referred to as position trading, trend trading is a strategy that involves holding positions for a longer period of time, typically at least a few months. As the name would suggest, trend traders try to take advantage of directional trends. Trend traders may enter a long position in an uptrend and a short position in a downtrend.Trend traders will typically use fundamental analysis, but this may not always be the case. Even so, fundamental analysis considers events that may take a long time to play out – and these are the moves that trend traders try to take advantage of.

A trend trading strategy assumes that the underlying asset will keep moving in the direction of the trend. However, trend traders also have to take into account the possibility of a trend reversal. As such, they may also incorporate moving averages, trend lines, and other technical indicators in their strategy to try and increase their success rate and mitigate financial risks.Trend trading can be ideal for beginner traders if they properly do their due diligence and manage risk.

Scalping

Scalping is one of the quickest trading strategies out there. Scalpers don't try to take advantage of big moves or drawn-out trends. It's a strategy that focuses on exploiting small moves over and over again. For example, profiting off of bid-ask spreads, gaps in liquidity, or other inefficiencies in the market. Scalpers don't aim to hold their positions for a long time. It's quite common to see scalp traders opening and closing positions in a matter of seconds. This is why scalping is often related to High-Frequency Trading (HFT).Scalping can be an especially lucrative strategy if a trader finds a market inefficiency that happens over and over again, and that they can exploit. Each time it happens, they can make small profits that add up over time. Scalping is generally ideal for markets with higher liquidity, where getting in and out positions is relatively smooth and predictable.Scalping is an advanced trading strategy that isn't recommended for beginner traders due to its complexity. It also requires a deep understanding of the mechanics of the markets. Other than that, scalping is generally more suitable for large traders (whales). The percentage profit targets tend to be smaller, so trading larger positions makes more sense.

Passive investment strategies

Passive investment strategies enable a more hands-off approach, where the management of the portfolio requires less time and attention. While there are differences between trading and investment strategies, trading ultimately means buying and selling assets in the hopes of making a profit.

Buy and hold

"Buy and hold" is a passive investment strategy where traders buy an asset intending to hold it for a long time, regardless of market fluctuations.This strategy is typically used in long-term investment portfolios, where the idea is simply to get in the market without any regard for timing. The idea behind this strategy is that on a long enough time frame, the timing or entry price won't matter much.The buy and hold strategy is almost always based on fundamental analysis and typically won't concern itself with technical indicators. The strategy also probably won't involve monitoring the performance of the portfolio frequently – only once in a while.While Bitcoin and cryptocurrencies have only been around for a little more than a decade, the HODL phenomenon could be compared to the buy and hold strategy. However, cryptocurrencies are a risky and volatile asset class. While buying and holding Bitcoin is a well-known strategy within the cryptocurrency space,, the buy and hold strategy may not be suitable for other cryptocurrencies.

Index investing

Typically, index investing means buying ETFs and indices in the traditional markets. However, this type of product is also available in the cryptocurrency markets. Both on centralized cryptocurrency exchanges and within the Decentralized Finance (DeFi) movement.The idea behind a crypto index is to take a basket of cryptoassets and create a token that tracks their combined performance. This basket may be made up of coins from a similar sector, such as privacy coins or utility tokens. Or, it could be something else entirely,as long as it has a reliable price feed. As you'd imagine, most of these tokens heavily rely on blockchain oracles.How can investors use crypto indexes? For example, they could invest in a privacy coin index instead of picking an individual privacy coin. This way, they can bet on privacy coins as a sector while eliminating the risk of betting on a single coin.Tokenized index investing will likely become more popular over the coming years. It enables a more hands-off approach to investing in the blockchain industry and cryptocurrency markets.

We went through some of the most common crypto trading strategies, so hopefully, you can figure out which one may suit you best.To find out what is really working and what is not, you should follow and track each trading strategy – without breaking the rules you set. It's also helpful to create a trading journal or sheet so you can analyze each strategy's performance.But it's worth noting that you don't have to follow the same strategies forever. With enough data and trading records, you should be able to adjust and adapt your methods. In other words, your trading strategies should be constantly evolving as you gain trading experience.

Riskmanagement in cryptocurrency investments

Cryptocurrencies are often considered to be volatile and trading them can sometimes be risky. The crypto market has also been known to experience price swings, and like every other investment, there is the chance your investment may sink in value, irrespective of how sure-shot things may seem. That said, risk management is undoubtedly one of the most important aspects of investing in cryptocurrencies.

Here are some ways to manage crypto risk.

Only invest what you can afford to lose

As with any investment, you should never invest more than you can afford to lose. This rule applies to all markets and even more so to cryptocurrencies, which can experience double-digit losses in a span of hours.

There's no doubt that cryptocurrencies have turned several early investors into millionaires. But at the other end of the spectrum, they have left a number of novice investors in financial peril. Apart from the fact that these assets can quickly lose their value in response to ever-changing government policies, crypto trading platforms can fall victim to a hack or shutdown operations.In 2021, dozens of people in Singapore filed police reports against a crypto trading platform called Torque. A rogue employee of the company reportedly performed unauthorized trading activities that led to significant losses and customers were restricted from using the platform.

Optimism can affect rational decision-making during market peaks, but it's important to avoid getting caught up in the hype cycles and unsubstantiated promises. Think before investing your life savings or selling a property to buy crypto.

Move your crypto assets into cold storage

You've probably heard this saying from crypto folks: "Not your keys, not your coins." Storing your assets on a centralized exchange can come with a number of risks, like site crashes, hacks and even bankruptcy. Crypto platform FTX halted withdrawals and filed for bankruptcy in November 2022, dragging much of the crypto industry down with it as it crumbled.

Transferring crypto assets to a cold storage device can mitigate some of the risks associated with trusting a centralized exchange to safeguard your funds. To clarify, a cryptocurrency exchange holds your private keys and therefore controls your assets. Cold storage, on the other hand, gives you full custody over your assets. Moreover, cold storage devices are not connected to the internet, which drastically decreases the ability of hackers and cybercriminals to access your funds. Some of the most popular cold storage devices are hardware-based and come from companies like Ledger and Trezor.

Hedge your crypto portfolio

Hedging has long been used in traditional financial markets as a form of risk management. It involves buying or selling an asset to potentially help reduce the risk of loss of an existing position or adverse price movements in an asset.

It is worth mentioning that although hedging allows you to protect your investment from adverse market swings, it also limits the potential gains from your crypto investment. Nevertheless, this is a better option than losing a significant portion of your investment.There are several ways to hedge your crypto portfolio, such as dollar cost averaging, buying options, futures and even yield farming.The "Dollar Cost

Averaging" (DCA) strategy is one of the simplest ways to hedge a crypto investment. It entails incrementally buying or selling crypto at regular intervals rather than deploying capital in one large purchase or selling one's entire holdings at once.

For example, let's assume you have $1,000 to invest in Bitcoin. Instead of purchasing $1,000 worth of Bitcoin in one fell swoop, you can split your investment into $250 every week spread across a month. While you might lose some potential gains if the price of Bitcoin shoots up after your initial purchase, you'd have also saved yourself from potential losses if the price crashes.

Diversify your portfolio

When it comes to crypto or any other investment, avoid putting all your eggs in one basket. In May 2022, the price of algorithmic stablecoin terraUSD (UST), which was supposed to be pegged to the U.S. dollar, fell to 35 cents. A few days later, its accompanying cryptocurrency, LUNA, plunged from $80 to a few cents.Do not invest in only one cryptocurrency, regardless of your conviction. Instead, spread your investment across several digital assets. You can diversify your crypto holdings by investing in projects based on their use case or technology. For instance, Bitcoin has been touted as a store of value and might be a good way to preserve wealth. Ethereum, on the other hand, has become the largest platform for decentralized applications and smart contracts. Meanwhile, a stablecoin's value is pegged to an underlying asset, making it typically less erratic than other digital assets. It's good to remember that there are hundreds of cryptocurrency projects trying to achieve different things.

Avoid excessive leverage

This is more of an advanced tip, but you'd be shocked at the number of beginner traders that try to margin trade. Margin is used to increase the order size and gives you the option of going long or short. Some crypto exchanges may offer leverage as high as x100.While the idea sounds good in theory, a 1% move against you could wipe out your entire portfolio. You could lose your entire principal during a forced liquidation.A safer approach would be sticking to lower leverage amounts, which provide more room to not only increase your gains but also a buffer zone to exit a bad trade.

Practicing caution

As with any investment, risk is a part of the cryptocurrency trading experience and cannot be entirely removed. Rather than assume that everything will go as planned, a smart trader identifies risky areas and finds a way around them.

Initial Coin Offerings (ICOs)

What Is an Initial Coin Offering (ICO)?

An initial coin offering (ICO) is the cryptocurrency industry's equivalent of an initial public offering (IPO). A company seeking to raise money to create a new coin, app, or service can launch an ICO as a way to raise funds.Interested investors can buy into an initial coin offering to receive a new cryptocurrency token issued by the company. This token may have some utility related to the product or service that the company is offering or represent a stake in the company or project.

KEY TAKEAWAYS

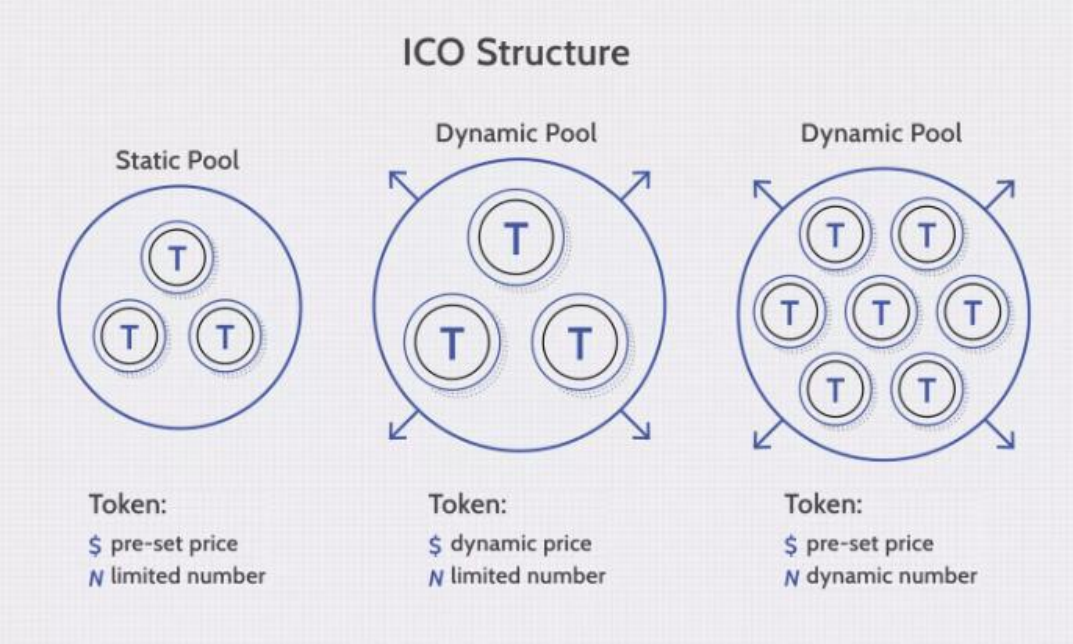
- Initial coin offerings (ICOs) are a popular way to raise funds for products and services usually related to cryptocurrency.
- ICOs are similar to initial public offerings (IPOs), but coins issued in an ICO also can have utility for a software service or product.
- A few ICOs have yielded returns for investors. Numerous others have turned out to be fraudulent or have performed poorly.
- To participate in an ICO, you usually need to first purchase a more established digital currency, plus have a basic understanding of cryptocurrency wallets and exchanges.
- ICOs are, for the most part, completely unregulated, so investors must exercise a high degree of caution and diligence when researching and investing in them.nds of 1 minute, 54 secondsVolume 75%

How an Initial Coin Offering (ICO) Works

When a cryptocurrency project wants to raise money through an ICO, the project organizers' first step is determining how they will structure the coin. ICOs can be structured in a few different ways, including:

- **Static supply and static price**: A company can set a specific funding goal or limit, which means that each token sold in the ICO has a preset price, and the total token supply is fixed.
- **Static supply and dynamic price**: An ICO can have a static supply of tokens and a dynamic funding goal—this means that the amount of funds received in the ICO determines the overall price per token.
- **Dynamic supply and static price**: Some ICOs have a dynamic token supply but a static price, meaning that the amount of funding received determines the supply.

These three different types of ICOs are illustrated below:



Token sales

A token sale, sometimes called an Initial Coin Offering (ICO), is the first stage of a token offering, where a group of buyers become the first to reserve a portion of the project's token supply.

Function

Token sales may serve one or more of the following functions:

a method for distributing tokens to a community of participants

a way to align the interests of a community behind a new project

a way to fund a project's early development.

Participation

Buying in a token sale typically entails registration or "whitelisting" via the project's website. This often involves a Know-Your-Customer (KYC) procedure, where buyers are filtered to ensure the token sale complies with local regulations. Whitelisted buyers are eligible to purchase in the sale when it goes live and orders are typically accepted on a first-come, first-serve basis.

Method of payment

Major cryptocurrencies such as Bitcoin, Ethereum, and U.S. dollar stablecoins like USDT and USDC are the most common methods of payment for token sales. In some cases, payment is accepted in local currencies like dollars or euros.

Use of funds

Funds received in a token sale are often converted to U.S. dollar stablecoins and held in the project's treasury. From there, the funds are used to pay project-related expenses such as compensation for developers, bounties for project-related tasks, marketing, and so on.

Allocations

The tokens made available to buyers in a token sale are usually just a portion of all the tokens that will ultimately be issued by the project. For example, a token sale may offer 20% of the planned total supply of tokens. The remaining 80% may be reserved for team members, a development fund, airdrops, ecosystem incentives, and more. Note that some projects, such as Ethereum, don't have a pre-defined token supply. In that case, the amount allocated in the token sale can't be expressed as a percentage of the token supply.

Structure

Token sales come in a wide variety of shapes and sizes, and have evolved significantly over time. The best token sales are typically structured to consider ways to:

balance the need to compensate the earliest buyers while ensuring later buyers also get a fair price

ensure a wide distribution of tokens beyond just buyers

incentivize buyers to support the project in the long-term

control the rate at which tokens hit the market in order to reduce secondary market price volatility.

The following are some common features that have evolved as ways to achieve the above:

The sale takes place in rounds. Rounds are usually structured such that the price per token is higher the later it is purchased. Some token sales are dynamically priced, where the price per token depends on the dollar amount contributed (the more money contributed, the higher the price per token).

Token sale buyers must wait to receive their purchased tokens. In some cases, all buyers will receive the tokens at the same time. In other cases, tokens will vest or "unlock" over a pre-defined schedule that is

written in the smart contract that defines the token sale. Vesting schedules may depend on which round tokens were purchased in. For example, a sale might be structured such that in the first unlock 25% of tokens purchased in round 1 vest whereas 50% of round 2 tokens vest. This structure would ensure that the earliest buyers (who got the best price) hold more of their tokens for longer.

Tokens distributed via the token sale account for a small fraction of the total supply of tokens. This ensures there are plenty of tokens available for market participants other than token sale buyers. In some cases a large percentage of tokens are reserved for airdrops, where tokens are given away to ecosystem participants. This can help to ensure a wide distribution of the token and strengthen the project's community.

UNIT-5 Regulatory and Legal Aspects of Cryptocurrencies

Government policies and regulations surrounding cryptocurrencies

The growth of cryptocurrency from speculative investment to a new asset class has prompted governments around the world to explore ways to regulate it. Below, we summarize the current digital currency regulatory landscape in several countries.

KEY TAKEAWAYS

As cryptocurrency has become a more significant factor in the global investment landscape, countries have taken different approaches to regulating the asset class.

The European Union became the first to adopt measures requiring crypto service providers to detect and stop illicit cryptocurrency uses.

1 In the United States, the Biden administration clarified crypto use and regulation in 2022, paving the way for the digital dollar.

2 In other countries, cryptocurrency is subject to different classifications and tax treatment.

United States

The U.S. announced a new framework in 2022 that opened the door to further regulation. The new directive has handed power to existing market regulators such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).The SEC has already moved toward regulating the sector with its widely publicized lawsuit against Ripple, alleging that it raised more than $1.3 billion by selling its native token, XRP, in unregistered securities transactions. More recently, the SEC has been targeting exchanges and companies such as Coinbase (COIN) and Binance (BNB) over their crypto products. SEC Chairman Gary Gensler has been vocal about cryptocurrency and has referred to it as “a Wild West.”

“Nothing about the crypto markets is incompatible with the securities law,” Gensler said. “Investor protection is just as relevant, regardless of underlying technologies.”We will likely see U.S. regulators coming down hard on cryptocurrency in the coming years. The SEC’s suit against Ripple Labs concluded in July 2023, with the judge ruling that coin offerings to institutional investors represented an investment contract, while sales to retail investors did not.

Previous statements from Federal Reserve officials have discussed systemic risks arising from stablecoins. That focus will likely gain importance in light of the 2022 Terra stablecoin collapse, which cost investors $60 billion.

Pathway Is Open to a Digital Dollar

The Biden administration’s new framework also sees “significant benefits” from creating a central bank digital currency (CBDC) or a digital form of the U.S. dollar.Federal Reserve Chairman Jerome Powell has remarked that the key reason to release a CBDC would be to eliminate the need for alternative coin use in the country.

"You wouldn't need stablecoins; you wouldn't need cryptocurrencies if you had a digital U.S. currency," Powell said in congressional testimony. "I think that's one of the stronger arguments in its favor."

China

China classifies cryptocurrencies as property for the purposes of determining inheritances.The People's Bank of China (PBOC) bans crypto exchanges from operating in the country, stating that they facilitate public financing without approval.Furthermore, China placed a ban on Bitcoin mining in May 2021, forcing many engaging in the activity to close operations entirely or relocate to jurisdictions with a more favorable regulatory environment.

And in September 2021, cryptocurrencies were banned outright.

However, the country has been working on developing the digital yuan (e-CNY). In August 2022, it officially began rolling out the next round of its central bank digital currency (CBDC) pilot test program.

Canada

While crypto is not considered legal tender in Canada, the country has been more proactive than others about crypto regulation. Canada became the first country to approve a Bitcoin exchange-traded fund (ETF), with several trading on the Toronto Stock Exchange.As for crypto trading platforms, the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) require that crypto trading platforms and dealers in the country register with provincial regulators.

Canada classifies all crypto investment firms as money service businesses (MSBs) and requires that they register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

From a taxation standpoint, Canada treats cryptocurrency similarly to other commodities.

United Kingdom

While there are no cryptocurrency-specific laws in the U.K., the country considers cryptocurrency as property (not legal tender), and crypto exchanges must register with the U.K. Financial Conduct Authority (FCA). Crypto derivatives trading is banned in the U.K. as well. There are cryptocurrency-specific reporting requirements relating to know your client (KYC) standards, as well as anti-money laundering (AML) and combating the financing of terrorism (CFT).

Although investors still pay capital gains tax on crypto trading profits, more broadly, taxability depends on the crypto activities undertaken and who engages in the transaction.Crypto exchange and custodian wallet providers must comply with the reporting obligations implemented by the Office of Financial Sanctions Implementation (OFSI). Crypto firms must notify the OFSI as soon as possible if they know or have reasonable suspicion that a person is subject to sanctions or has committed a financial sanctions offense.

In October 2022, the lower house of the British Parliament recognized crypto assets as regulated financial instruments. The draft bill extends current laws regarding payments-focused instruments to stablecoins.

Japan

Japan takes a progressive approach to crypto regulations, recognizing cryptocurrencies as legal property under the Payment Services Act (PSA). Meanwhile, crypto exchanges in the country must register with

the Financial Services Agency (FSA) and comply with AML/CFT obligations. Japan established the Japanese Virtual Currency Exchange Association (JVCEA) in 2020, and all crypto exchanges are members.Japan treats trading gains generated from cryptocurrency as miscellaneous income and taxes investors accordingly.

The country has been working on several aspects when it comes to regulation, including taxation. In September 2022, the government announced it would introduce remittance rules as early as May 2023 to prevent criminals from using cryptocurrency exchanges to launder money. The Act on Prevention of Transfer of Criminal Proceeds will be revised to collect customer information.

Australia

Australia classifies cryptocurrencies as legal property, subjecting them to capital gains tax.Exchanges are free to operate in the country, provided that they register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and meet specific AML/CTF obligations.In 2019, the Australian Securities and Investments Commission (ASIC) introduced regulatory requirements for initial coin offerings (ICOs). It banned exchanges from offering privacy coins, which are cryptocurrencies that preserve anonymity by obscuring the flow of money across their networks.

In 2021, Australia announced plans to create a licensing framework around cryptocurrency and potentially launch a central bank digital currency (CBDC).

Singapore

Like the U.K., this island state classifies cryptocurrency as property but not legal tender. The country's Monetary Authority of Singapore (MAS) licenses and regulates exchanges as outlined in the Payment Services Act (PSA).Singapore, in part, gets its reputation as a cryptocurrency safe haven because long-term capital gains are not taxed.

However, the country taxes companies that regularly transact in cryptocurrency, treating gains as income.

Singapore issued guidance in 2022 warning digital payment token (DPT) providers to avoid advertising their services to the public.

South Korea

In South Korea, cryptocurrency exchanges and other virtual asset service providers must register with the Korea Financial Intelligence Unit (KFIU), a division of the Financial Services Commission (FSC).South Korea also banned all privacy coins from exchanges in 2021.

In 2021, the country's Parliament approved a 20% tax on digital assets to take effect in 2022, but it has been delayed until 2025.

The government is working on legislation called the Digital Asset Basic Act to begin regulating crypto.

India

India remains on the fence regarding crypto regulation, neither legalizing nor penalizing its use. There is a bill in circulation that prohibits all private cryptocurrencies in India, but it has yet to be voted on.There is a 30% tax levied on all crypto investments and a 1% tax deduction at source (TDS) on crypto trades.

Overall, India continues to hesitate to ban crypto outright or to regulate it. Current regulations are unclear at best and don't provide much guidance for investors. The country launched its tokenized rupee pilot program in late 2022.

European Union

Cryptocurrency is legal throughout most of the European Union (EU), although exchange governance depends on individual member states.Meanwhile, taxation also varies by country within the EU, ranging from 0% to 50%.

Recently, the EU's Fifth and Sixth Anti-Money Laundering Directives (5AMLD and 6AMLD) have come into effect, tightening KYC/CFT obligations and standard reporting requirements.

In September 2020, the European Commission proposed the Markets in Crypto-Assets Regulation (MiCA)—a framework that increases consumer protections, establishes clear crypto industry conduct, and introduces new licensing requirements. It was provisionally agreed on in 2022.

In April 2023, Parliament approved measures that allow legislation requiring certain crypto service providers to seek an operating license. This legislation is intended to give regulators the tools they need to track crypto being used for money laundering and terrorism funding.

Are There Any Regulations on Crypto?

Cryptocurrency regulations are still being researched and developed worldwide. Many countries are creating policies and legislation, while others lag for various reasons.

What Year Will Crypto be Regulated?

Partial regulation exists in some countries, with others taking steps to regulate as much of the space as possible. For example, crypto exchanges in the U.S. are subject to regulations. In the EU, laws are developing requiring crypto service providers to identify illicit crypto uses.

Who Is the Crypto Regulator?

In the U.S., who regulates crypto depends on how and where it is used. The Securities and Exchange Commission, the Chicago Mercantile Exchange, Commodity Futures Trading Commission, and the Financial Industry Regulatory Authority are all involved in some regard. Cryptocurrency transactions between private users—private wallet to private wallet—are not regulated.

Taxation and accounting considerations for cryptocurrencies

The tax situation becomes more complex when investors use cryptocurrency to pay for purchases. In this scenario, every transaction counts as a sale of crypto, potentially triggering a capital gains tax liability as well as any applicable sales taxes, such as GST and VAT on the underlying purchase.

Not all countries are following the lead of the US and UK, however. Notable exceptions include Switzerland, Hong Kong, Germany and the Netherlands, where tax rules for selling crypto are different, and countries like Japan and New Zealand which adopt an income tax approach.

Wider adoption of stablecoins, which have a value pegged to a currency or commodity, and central bank digital currencies may also require new tax rules. As these coins are less volatile, they may be less likely to result in capital gains or losses; changes in value will be more akin to foreign exchange differences.

Meanwhile, according to Mercy Joseph, Director, Customer Tax Operations and Reporting Services, EY Corporate Advisors Pte. Ltd in Singapore, the evolution of digital assets taxation in Asia is generally being directed by the attitude of the regulators. "In Singapore, the financial regulators are comfortable and supportive of blockchain technology and innovative use of digital assets, and therefore from a tax perspective there's an increasing level of clarity around taxation for digital assets in general," she says. "However, given the cautiousness of the regulator on trading of digital assets, there isn't the same clarity at the moment in areas such as availability of fund tax incentive upon investment in crypto."

Taxing income from crypto mining and proof-of-staking

Owning and disposing of cryptocurrencies are not the only taxable events in the digital assets area. The process of creating new cryptocurrency, known as mining, which involves using powerful computers to validate transactions, is one of a growing list of other taxable activities.

Although there is no global tax consensus on crypto mining, Wren says jurisdictions are increasingly applying income tax if an individual earns cryptocurrency by mining it, or if they receive it as a promotion or as payment for goods or services. If an individual retains ownership of cryptocurrency they have mined or earned as a result of mining, and it grows in value before the owner sells or spends it, the owner can then also be liable for capital gains taxes on the profits.

Staking – a process of digitally validating blockchain transactions – is another activity that may be subject to income tax. While the US tax authorities have yet to issue specific guidance in this area, the UK's HMRC clearly states that any profits from staking are subject to income tax. HMRC's guidance says: "…The pound sterling value (at the time of receipt) of any crypto-assets awarded for successful staking will generally be taxable as income, with any appropriate expenses reducing the amount chargeable."

Wren points out that tax positions around mining and staking are not always clear-cut, however. "With crypto mining and staking activities, UK rules treat receiving a coin under those circumstances as an income event," he says. "But if the owner doesn't sell the coin, then actually they have a tax liability with no cash to back it up.

"This is a great example of the complexity investors encounter when they move away from simply holding, buying and selling crypto," Wren continues. "They start to encounter areas where the tax may not be particularly suitable for the asset class."

Cryptocurrency mining is also a massively energy-intense activity, requiring many data warehouses filled with computer servers to solve complex mathematical calculations. According to Cambridge University's Bitcoin Consumption Index, the act of creating this specific cryptocurrency alone consumes approximately 128TWh of electricity annually – more than Norway and enough energy to power all the tea kettles in the UK for 29 years. This raises environmental, social and governance (ESG) concerns at a time when whole sectors of the global economy are attempting to reduce energy consumption and decarbonize.

Utility tokens and security tokens, and how they are taxed

While utility tokens are created using the same blockchain technology as cryptocurrency, the similarities end there. Tech start-ups typically sell utility tokens to raise funding for their digital products or services. An investor buys a utility token in order to access the product or service offered by the token issuer. A ride-hailing token, for example, could be used to pay for a taxi journey but not anything else, although it may be exchanged for either government-issued currency or a crypto coin.

Security tokens, however, derive their value from a physical, tradeable asset, such as a stock or real estate. An investor who buys a tokenized version of a stock enjoys the same rights as someone who buys a stock from a traditional stockbroker, including profit share and voting rights. Security tokens also fall under the same regulatory oversight as other investment products. The major difference is that a security token exists in digitized and decentralized form on blockchain.

Most jurisdictions have yet to issue guidance on the tax treatment of utility tokens or security tokens, but that guidance will almost certainly come. "I think most tax practitioners would welcome a tax approach that looks through to the underlying asset and matches it to the underlying asset class," says Wren. "But the reality is that neither the existing regulatory rules, nor the tax rules, do that at present, and tax authorities may be reluctant to go down that path until they fully understand the implications and risks of doing so."

Anti-money laundering (AML) regulations

What is Anti-Money Laundering in Cryptocurrency?

Anti-Money Laundering (AML) in Cryptocurrency refers to a set of regulations, policies, and procedures designed to prevent cryptocurrencies from being used to launder money. The aim is to ensure that cryptocurrencies are not used to fund illegal activities or support terrorism. Cryptocurrencies, such as Bitcoin and Ethereum, are decentralized and operate outside the traditional banking system. This makes it easy for criminals to use them to launder money, as there are no regulations or oversight. AML in Cryptocurrency is, therefore, necessary to ensure that cryptocurrencies are not misused.

Why is Anti-Money Laundering in Cryptocurrency important?

Anti-Money Laundering in Cryptocurrency is essential to prevent the use of cryptocurrencies for illegal activities. Cryptocurrencies are highly liquid, and they can be transferred across borders quickly and easily. This makes it easy for criminals to move funds without detection. Without AML regulations, cryptocurrencies can be used to fund terrorist activities, drug trafficking, human trafficking, and other illegal activities. The lack of regulation and oversight also makes cryptocurrencies vulnerable to hacking and theft.

How is Anti-Money Laundering in Cryptocurrency Enforced?

Anti-Money Laundering in Cryptocurrency is enforced by governments and regulatory bodies around the world. Cryptocurrency exchanges and other businesses that deal with cryptocurrencies are required to comply with AML regulations. They are required to verify the identities of their customers and report any suspicious transactions to the authorities. The regulatory bodies monitor these businesses to ensure that

they are complying with the regulations. The penalties for non-compliance can be severe and can include fines, imprisonment, and revocation of licenses.

The Role of Know Your Customer (KYC) and Customer Due Diligence (CDD) in AML:

KYC and CDD are two essential elements of AML regulations. KYC refers to the process of verifying the identity of customers. This process includes collecting personal information such as name, address, and government-issued identification documents. KYC helps to prevent identity theft and ensures that the customers are who they claim to be. CDD is the process of assessing the customer's risk profile. This includes identifying the source of funds and the purpose of the transaction. CDD helps to identify any suspicious activity and prevent money laundering.

The Role of Suspicious Activity Reports (SARs) in AML:

SARs are reports submitted by financial institutions and other businesses to the authorities when they suspect that a transaction is related to money laundering or other illegal activities. SARs help the authorities to investigate and prosecute criminals who use cryptocurrencies for illegal activities. SARs are an essential tool in the fight against money laundering.

Financial institutions and businesses that deal with cryptocurrencies are required to report any suspicious transactions to the authorities as part of their Anti-Money Laundering (AML) compliance. These reports must include all relevant information about the transaction, including the parties involved, the amount transferred, and any other relevant details. SARs are vital in identifying and preventing money laundering and other illegal activities, as they provide crucial information for law enforcement agencies to investigate and prosecute criminal activities related to cryptocurrency. As cryptocurrencies continue to gain popularity, SARs will remain a crucial tool in the fight against financial crimes, ensuring the integrity of the financial system and protecting consumers from the risks associated with cryptocurrency.

Legal challenges and future prospects of cryptocurrencies.

Legal Aspects and Issues Associated with Crypto-Currencies

Virtual currencies, depending on the nation, have different legal elements to consider. Some nations classify them as cash and legal, some classify them as assets and legal, while some nations like India do not classify them as illegal or legal, without legal frameworks. Bitcoin is produced illegally in nations like Bangladesh and Russia. Its status is somewhat complex in other nations. Cryptocurrencies are prohibited in some nations due to existing legislation, such as Iceland. However, cryptocurrencies in India, like many other countries, currently have no legal framework in place and are unregulated. Cryptocurrencies related legal issues are as follows,

Decentralized nature: Unlike government-issued currencies (i.e. banknotes, coins, etc.) that are directly under the control of the issuing authority and derive their value from the promise of the issuing authority and stored gold, Cryptocurrencies are decentralized in nature, making it difficult for them to be regulated by the government.Absence of a well-defined legal framework: Most nations lack an adequate legal framework to regulate the value and flow of virtual currencies both inside and outside the nation, creating additional hurdles to regulate a decentralized currency.

The volatility of Virtual Currencies: As can be seen from latest modifications in the value of most renowned cryptocurrency bitcoin, which in 2010 had a base value of $0.30 and in 2017 grew to nearly $4000, virtual currencies follow a volatile track of ups and downs that further bring market and economy instability.

Independent Wallets: Wallets holding cryptocurrencies and engaged in transactions are established and managed by private companies that have no control over any organization owing to the lack of any binding international laws in place. They, therefore, have no liability for the loss of the customer as well as for any form of financial crime committed by and through the use of these wallets.

Taxation: Taxation issue is one of the major cryptocurrencies issues. Because of their pseudo-anonymity, if properly used, they can readily be used by hiding the property for tax evasion purposes. Cryptocurrencies are often categorized as a taxable asset, for example in the United States. While bringing big amounts of foreign currency into a nation may de-stabilize its economy and may cause taxation problems, it also presents financial market volatility. Online path to take and store cryptocurrencies makes it simpler to get them across border checkpoints, where they can be cashed out when they are inside the nation, efficiently avoiding border taxes. Loopholes current in some countries ‘ legal and tax scheme allow an individual to use cryptocurrencies features such as anonymity and lack of or outdated or improperly enforced cryptocurrencies schemes.

Money Laundering: Money laundering is typically taken into account when developing a country’s legal framework when discussing Cryptocurrency. But since its emergence, many countries are struggling through cryptocurrencies with problems related to money laundering. Due to the ease of their motion between nations with little or no oversight, money laundering is a main legal complication with such currencies. While organizations can monitor virtual currency purchased through banks, it becomes difficult when purchasing or selling the coins using money or other hard-to-trace techniques. Other safety provided in connection with trading in cryptocurrency are:

Spoofing and Phishing Payment Information

Like ordinary e-money, phishing attacks also affect cryptocurrency users because they can be redirected to a fake website that requires them to enter their crypto-wallets user I d and passwords. While transaction spoofing may be performed by an attacker when a user attempts to copy the wallet address for a transaction that is replaced by malware and the user is unaware of the changes as not everyone is watchful to double-check a long address copied by them.

Error in User Address

There is also a prospective loss danger when an error is made in the address of the recipient that can result in cash loss. For example, in the case of Ethereum, if some of the last digits of the recipient address are mistakenly entered, the money will disappear or be transferred to the exact address, but the intended value multiplied by 256 will be transacted.

Loss of a Wallet File

One of the cryptocurrencies ‘ significant issues is the loss or theft of local wallet documents due to hard disk crashes or other interruptions. So, a paper wallet is usually recommended to store local passwords or a hardware wallet backup.

Insecure ICOs

Investing in cryptocurrency-funding can be achieved via Initial Coin Offering (ICO) through virtual currencies. Generally, an ICO is awarded to increase a lump sum of money through the purchase and sale of cryptocurrency that needs an Internet connection. Another obstacle when managing virtual currencies is the lack of a risk-free access system to control the cryptocurrency market to track down and de-anonymize a payee on the cryptocurrency market.

Payment Gateway Hacking

Hacking can be performed by convincing the hosting provider that they are the true domain owners and then the cash flows are intercepted. Many well-known financial services have fallen prey to hackers using such tactics.

Fraud at the Trading Exchange

With Bitcoin’s popularity and latest price increase, many potential platforms for exchange and trading are flourishing around the globe. These trade exchanges store in their local servers the public and private keys

of all the wallets of their clients. If any, a trading exchange supplier will decide to run away with the cryptocurrencies of all their customers. Then there is not much that can be done against such offences owing to the absence of legislation and legal frameworks, which in turn puts all traders in a fragile position.

Precautionary Measures and Initiatives by Regulatory Authorities and Government Agencies

Virtual currencies ' legal status differs widely from nation to nation, and many of them are still undefined or undergoing modifications. While many nations do not illegalize the use of cryptocurrencies, their status as cash (or commodity) differs, with different legislative consequences. While some nations have explicitly permitted their use and trade, others have in any way limited or prohibited their use. Similarly, separate public organizations, departments, and courts differ on cryptocurrencies views. For instance, cryptocurrencies are unregulated in India, UK, Brazil, etc. because there is no legal framework yet in place, or their use has been deregulated and is free to use with no or minor legal constraints. While these are regulated in nations like France, Finland and Germany, use is legal but specifically regulated for tax or other purposes, and sometimes classified as cash. In some nations, the use of cryptocurrency is limited but legal in certain conditions, such as in China, people may be able to transact, while corporations and banks are unable to do so. It is illegal in Iceland to buy or sell bitcoins, but they can be mined. Nations like Russia, Bangladesh, and Ecuador have outright banned bitcoins. Recently CME Group Inc. in the U.S. has opened up a future exchange in bitcoins while SEBI, India has established a Financial and Regulatory Technology (CFRT) Committee to examine, deliberate and advise on cryptocurrencies issues. Reserve Bank of India also issued warnings about the volatile nature of cryptocurrencies to customers engaged in bitcoin trading. Below are some suggestions and precautions for cryptocurrency owners and crypto-investors,

Always check the address of a Web wallet and prevent following suspect connections to a Web bank or Web wallet.

Always double-check the address of the recipient, the amount entered, details of the transaction fees and other charges before the transaction.

Recover expired account passwords and other details and maintain them secure and personal.

Investment in cryptography is dangerous. Common procedures must, therefore, be followed while investing in unforeseen conditions such as diverse investment, provider reliability and a powerful mindset.

It is advisable to use cryptocurrency wallets and paper wallets. Use excellent antivirus programs to safeguard pcs and devices that are used to access crypto-wallets, as well as other cryptocurrencies operations.

Conclusion

Most use of Virtual Currency worldwide is currently under a vacuum in terms of legality and controlled. Some nations have included it in their financial system, but some have totally prohibited it. If Virtual Currencies ' popularity rises further, it may be regulated by more and more nations, although it is not the case that many consider bans on it. With the increasing client base and the latest upsurge in the value of Bitcoin, which is one of the most popular virtual currency available, there are increasing hurdles such as the need for a legal framework and regulatory authority, awareness of wallet use, transaction processing as well as hazards associated with virtual currency transactions. Cryptocurrencies can, therefore, be said to have excellent potential for becoming a global currency. Even in nations where the courts prohibit its use, it is still a matter of restricting the use completely without internet censorship. Thus, it can be ascertained that the integration of Virtual Currencies into legal frameworks and the current financial system has enormous growth potential and advantages. Indian banking and finance are prepared to leverage transaction processing from the capacities of blockchain technology and distributed ledgers. There is likely to be more discussion about the legality and recognition of cryptocurrencies around digital currencies in the next few years. The key legal problems surrounding cryptocurrencies were discussed in this article and these are the primary concerns that nations need to consider when establishing Virtual Currencies legislation.