UNIT III
BITCOIN CONSENSUS

BITCOIN CONSENSUS

Consensus plays a key role in building trust among crypto coin traders worldwide. Due to the decentralised nature of the crypto world, it is essential to have complete transparency while trading a particular coin. This minimises the chances of a buyer becoming a victim of fraud.

If you are a beginner in crypto trading, you must know the vital details about consensus regarding blockchain.

What Is the Meaning of Consensus?

Generally, consensus means that the majority of a group has agreed in favour of a decision. When it comes to blockchain, reaching a consensus is important. At least 51% of the traders and miners associated with a particular coin must agree to finalise the next global status of the coin.

What Is a Consensus Mechanism?

In the blockchain, a consensus mechanism is a system that validates a transaction and marks it as authentic. This mechanism lists all valid transactions of a coin in a blockchain to build trust in the coin among traders. Several currencies, such as Bitcoin, Ethereum etc., use this system for security purposes.

How Does the Consensus Mechanism Work?

It achieves the agreement of most users on a single network. The consensus mechanism maintains the security of the blockchain by keeping a record of all legitimate transactions. Since crypto trading is a decentralised process, this becomes important to stop sellers from deliberately cheating a buyer.

To build trust for a blockchain, the consensus mechanism ensures that a transaction is reflected in the blockchain as soon as it gets validated. There are a variety of methodologies that are essential to ensure security and trust and achieve agreement across a blockchain network. Consensus mechanisms also ensure that all the transactions for a coin are rightly listed in the blockchain.

What Are the Types of Consensus Mechanisms?

Several mechanisms are used as a consensus mechanism during coin trading. These mechanisms are as follows:

Proof of Work

'Proof' refers to the solution of a highly-complex problem, and 'work' refers to the process of solving the same. Crypto coin miners compete to solve the problem and gain the right to process the transaction. The fastest solver receives a mining fee from the traders of these coins.

Proof of Stake

This mechanism randomly chooses a maximum coin owner to validate a transaction. It also allows the owner to create a block for the same coin. This mechanism requires comparatively less energy, transaction time and a lower fee. Coins like Etherium 2.0, Polkadot, Cosmos, Cardano, ThorChain, Nxt and Algorand use this mechanism extensively. There is a security risk as if an owner owns 51% or more coins of a particular coin, then that person will get sole ownership of its network.

Proof of Capacity

The PoC mechanism heavily relies on free space available in the hard drive. This is because there are many solutions to a coin's hash problem that a trader needs to store. It is highly efficient as compared to PoW and PoC mechanisms. Coins such as Burst, Storj, SpaceMint and Chia use these mechanisms.

Proof of Activity

This mechanism is a combination of both Proof of Work and Proof of Stake. It has been designed to combine the best features of PoW and PoS. In the beginning, the Proof-of-Activity mechanism functions like PoW. Once a new block is completed, it starts to function like a Proof-Of-Stake mechanism. Coins such as DCR (Decred) use this mechanism.

Proof of Authority

Different organisations and private companies created this unique mechanism. There are validators with approved accounts which authorise transactions and the creation of new blocks. These validators must disclose their true identity to get the right to validate a transaction.

Proof of Burn

PoB aims to improve the quality of blockchain so that it can be used easily and extensively as a tool for faster and more secured transactions. After PoW and PoS, PoB is designed to prevent fraud activities on a blockchain network. Cryptocurrencies such as Bitcoin use this mechanism to offer secure transactions to traders.

Proof of Elapsed Time

Intel Corporation created this mechanism to permit blockchain to decide the person who will create the next block. It uses a lottery system to decide the next block creator. Thus, it gives a fair chance to all traders to create the next block. It is an efficient process involving utilising lesser resources and low energy consumption.

PROOF OF WORK (POW)

Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain. The idea for Proof of Work(PoW) was first published in 1993 by Cynthia Dwork and Moni Naor and was later applied by Satoshi Nakamoto in the Bitcoin paper in 2008. The term “proof of work” was first used by **Markus Jakobsson** and **Ari Juels** in a publication in 1999.

Cryptocurrencies like Litecoin, and Bitcoin are currently using PoW. Ethereum was using PoW mechanism, but now shifted to Proof of Stake(PoS).

Principle: *A solution that is difficult to find but is easy to verify.*

Purpose of PoW

The **purpose** of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don't trust each other.

- All the transactions in the new block are then validated and the new block is then added to the blockchain.
- The block will get added to the chain which has the longest block height(see blockchain forks to understand how multiple chains can exist at a point in time).
- Miners(special computers on the network) perform computation work in solving a complex mathematical problem to add the block to the network, hence named, Proof-of-Work.
- With time, the mathematical problem becomes more complex.

Features of PoW

There are mainly two features that have contributed to the wide popularity of this consensus protocol and they are:

- It is hard to find a solution to a mathematical problem.
- It is easy to verify the correctness of that solution.

How Does PoW Work?

The PoW consensus algorithm involves verifying a transaction through the mining process. This section focuses on discussing the mining process and resource consumption during the mining process.

Mining:

The Proof of Work consensus algorithm involves solving a computationally challenging puzzle in order to create new blocks in the Bitcoin blockchain. The process is known as 'mining', and the nodes in the network that engages in mining are known as 'miners'.

- The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 6.25 bitcoins and a small transaction fee.
- This reward will get reduced by half its current value with time.

Energy and Time consumption in Mining:

The process of verifying the transactions in the block to be added, organizing these transactions in chronological order in the block, and announcing the newly mined block to the entire network does not take much energy and time.

- The energy-consuming part is solving the 'hard mathematical problem' to link the new block to the last block in the valid blockchain.
- When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the PoW protocol.

Mining reward:

- Currently, mining a block in the bitcoin network gives the winning miner 6.25 bitcoins.
- The amount of bitcoins won halves every four years. So, the next deduction in the amount of bitcoin is due at around 2024(with the current rate and growth).

- With more miners comes the inevitability of the time it takes to mine the new block getting shorter.
- This means that the new blocks are found faster. In order to consistently find 1 block every 10 minutes. (That is the amount of time that the bitcoin developers think is necessary for a steady and diminishing flow of new coins until the maximum number of 21 million is reached (expected some time with the current rate in around 2140)), the Bitcoin network regularly changes the difficulty level of mining a new block.

Challenges With PoW

The Proof-of-Work consensus mechanism has some issues which are as follows:

- **The 51% risk**: If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.
- **Time-consuming**: Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time-consuming process.
- **Resource consumption**: Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that 0.3% of the world's electricity will be spent to verify transactions by the end of 2028.
- **Not instantaneous transaction:** Transaction confirmation takes about 10–60 minutes. So, it is not an instantaneous transaction; because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.

HASH CASH POW

Hash cash worked as follows: In order to send an email to a Hash cash user, the sender would have to find a **hash** of the email that fell within a certain range. Since a hash is a large, unpredictable number, producing such a hash takes many guesses. This system imposes a cost on sending email. The cost would come in the form of time and compute power, and would discourage spammers and make DoS attacks less efficient.

➤ Learn more about Bitcoin's predecessors.

The size of the range of valid hashes is a direct measure of the difficulty of finding a valid hash, and thus, of the time and work required to produce a valid hash. Users who wanted strong spam prevention could set a small range, requiring more work for all those wishing to send them emails. Users who were satisfied with weaker spam prevention could set a larger range, requiring less work.

Proof-of-Work and Bitcoin

When Bitcoin was invented, **Satoshi Nakamoto** applied Proof-of-Work to Bitcoin. In order to add a Bitcoin block to the blockchain, a **miner** must generate a hash that falls within a certain range, just like with Hash cash.

Proof-of-Work serves three purposes for Bitcoin:

- Analogous to Hash cash and email, PoW imposes a cost on producing blocks, preventing spam and DoS attacks.

- PoW serves as an objective way for decentralized parties to agree on which version of the blockchain is valid. It is a solution to the Byzantine Generals Problem.
- PoW imposes costs on the creation of new bitcoin, making it scarce and encouraging decentralization in the mining industry.

Bitcoin's Difficulty Adjustment

Hashcash allowed every user to individually set the range of valid hashes, which we call the difficulty. However, since Bitcoin is a consensus system, there must be exactly one difficulty. One of Bitcoin's greatest and most innovative features was its difficulty adjustment algorithm. Bitcoin's difficulty is adjusted roughly every four weeks, in order to ensure that a valid hash (and thus a Bitcoin block) is found on average every 10 minutes.

If, during a given four week period, blocks are produced at a faster rate, then the difficulty will be increased, meaning the range of valid hashes will shrink. Conversely, if blocks are produced at a slower rate, the difficulty will drop, and the range of valid hashes will rise.

When Bitcoin was launched in 2009, Satoshi Nakamoto served as the only miner. Slowly, others joined him, and dedicated more compute power to guessing hashes for blocks. Without the difficulty adjustment, this increase in the number of miners would have caused blocks to come in faster and faster, enabling spam and causing rapid accrual of all bitcoin to the earliest miners.

The difficulty adjustment ensures that no matter how many miners join the network, spam is unprofitable and the emission rate of new bitcoin stays relatively stable.

Proof-of-Work and the Byzantine Generals Problem

The Proof-of-Work and difficulty adjustment system described above also provides an objective solution to the Byzantine Generals Problem, allowing all members of the Bitcoin network to agree on which version of the blockchain is objective.

BITCOIN POW

Bitcoin's PoW System

Bitcoin uses the Hashcash Proof of Work system as the mining basis. The **'hard mathematical problem'** can be written in an abstract way like below :

Given data A, find a number x such as that the hash of x appended to A results is a number less than B.

- The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be solved.
- This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid.
- The answer to the problem needs to be a lower number than the hash of the block for it to be accepted, known as the '**target hash**'.

*A **target hash** is a number that the header of a hashed block must be equal to or less than for a new block, along with the reward, to be awarded to a miner.*

The lower a target is, the more difficult it is to generate a block.

- A miner continues testing different unique values (known as a nonce(s)) until a suitable one is produced.
- The miner who manages to solve the problem gets the bitcoin reward and adds the block to the blockchain by broadcasting that the block has been mined.

PROOF OF STAKE

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.

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.

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.

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.

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%

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

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.

PROOF OF BURN

Proof of burn is a type of consensus algorithm that is used by some cryptocurrencies. With proof of burn, miners show that they have burned (destroyed) some coins to prove their commitment to the network. This can help to secure the network and prevent double-spending.

Working:
To participate in a proof of burn system, miners must send some coins to an un-spendable address. This act of burning the coins serves as proof of their commitment to the network. The more cash burned, the more committed the miner is considered to be.

Over time, the proof of burn algorithm can help to secure the network as it becomes stringent for attackers. This is because they would need to control most of the mining power and have a large number of coins they are willing to burn.

Benefits
Proof of burn can help to secure a network and prevent double-spending. However, it can also make it more expensive for attackers to mount a 51% attack.

Drawbacks
One drawback of proof of burn is that it can lead to centralization as only those with enough money to burn coins will be able to participate. Another disadvantage is that it can be challenging to track how many coins have been burned, making it hard to assess miners' actual level of commitment.

Examples
Several cryptocurrencies use proof of burn as their consensus algorithm, including Slimcoin Namecoin and Ethereum Classic.

Namecoin is a decentralized DNS system that uses proof of burn to secure its network. Users must destroy some bitcoins to participate in Namecoin’s proof of burn system. This act serves as a way of proving their commitment to the network.

Slimcoin is another cryptocurrency that uses proof of burn. In Slimcoin’s system, miners must first burn some coins before they can start mining. The more coins burned, the more

committed the miner is considered to be. It also allows them to receive rewards for a longer time.

PROOF OF ELAPSED TIME

Proof-of-Elapsed-Time, or PoET, is a consensus algorithm introduced by Intel, primarily associated with the Hyperledger Sawtooth project. Unlike PoW and PoS, which rely on computational power or token ownership, PoET introduces a novel method for achieving consensus. It leverages a randomized waiting period as a fundamental component of its operation.

PoET is fundamentally different from the widely recognized Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanisms. PoW relies on miners solving complex mathematical puzzles to validate transactions, while PoS uses the stake (the number of coins held) to determine who gets the right to validate transactions. PoET, on the other hand, takes a unique approach, relying on a randomized waiting period as the basis for consensus.

Working:

Following is the complete process of the working of PoET:

- **Node Selection:** Nodes (or participants) within the blockchain network are chosen to propose and validate blocks. The selection procedure plays a vital role in the PoET consensus mechanism.
- **Randomized Wait:** Upon selection, the chosen node initiates a cryptographic timer. This timer mandates that the node waits for a randomized period, akin to a lottery.
- **Block Proposal:** The node that successfully completes the waiting period is granted the right to propose a new block. It includes cryptographic proof that it indeed waited for the specified duration.
- **Validation:** Other nodes in the network scrutinize the proposed block, ensuring that the cryptographic proof of the elapsed time is legitimate.
- **Consensus:** If the majority of nodes agree that the proposed block is valid, it is added to the blockchain, thereby achieving consensus.

Advantages of Proof-of-Elapsed-Time (PoET)

#1 Energy Efficiency

One of the primary advantages of PoET is its energy efficiency. Traditional PoW algorithms, as used in Bitcoin, rely on energy-intensive mining processes. PoET eliminates this resource-intensive aspect, making it an appealing choice for organizations and networks where energy consumption is a significant concern.

Proof-of-Work (PoW) consumes a substantial amount of energy, which leads to concerns about the environmental impact of cryptos. In contrast, PoET doesn't require energy-intensive calculations, making it more environmentally friendly.

#2 Fairness

PoET offers a fairer system for participants. It does not favor those with greater computational power or token ownership. Instead, it allows a broader range of users to participate in block proposal and validation processes, enhancing inclusivity and fairness.

In PoW and PoS systems, participants with more computational resources or a larger stake in the crypto often have an advantage in block validation. This can lead to centralization, where a few entities control most of the network. PoET mitigates this issue by introducing a random

waiting period, ensuring the opportunity to propose blocks is distributed fairly among participants.

#3 Security

The randomized wait period introduced by PoET enhances security. It ensures that no single entity can consistently control block proposal rights. This randomness makes it exceedingly difficult for malicious actors to predict when they will have the opportunity to propose blocks, bolstering the network's overall security.

Traditional PoW and PoS systems are susceptible to attacks from entities with significant computational power or coin ownership. PoET's randomized approach reduces this vulnerability, making it more secure against centralized control and external threats.

Limitations of Proof-of-Elapsed-Time (PoET)

#1 Centralization

While PoET reduces the energy consumption associated with PoW, it can still suffer from centralization issues. In cases where a few nodes consistently win the waiting period lottery, it can undermine the decentralization goals of blockchain networks.

Centralization is a common concern in various consensus mechanisms, and PoET is no exception. If a few nodes consistently win the waiting period lottery, they could accumulate significant influence over the network, similar to the centralization issues in PoW and PoS.

#2 Complexity

Implementing PoET can be more complex than traditional consensus mechanisms. The need for cryptographic timers and a secure randomization process can add complexity to the blockchain's codebase and its overall operation.

The complexity of implementing PoET can make the development and maintenance of PoET-based blockchains more challenging compared to simpler consensus mechanisms like PoW.

Conclusion

Proof-of-Elapsed-Time (PoET) is a novel consensus mechanism that brings energy efficiency, fairness, and security to blockchain networks. While it has clear advantages, its potential for centralization and increased complexity must be carefully considered when choosing the right consensus mechanism for a specific blockchain project.

As blockchain technology continues to evolve, PoET remains an interesting alternative to more established consensus algorithms, offering new possibilities for the future of blockchain networks. Whether it finds widespread adoption in the crypto and blockchain world remains to be seen, but it certainly contributes to the ongoing innovation within the industry.

Ultimately, PoET represents a significant step towards more sustainable, inclusive, and secure blockchain networks. Its success will depend on its effective implementation, user adoption, and ability to address centralization.

BITCOIN MINER

Bitcoin is a digital currency that requires a process called mining. Bitcoin mining is a network-wide competition to generate a cryptographic solution that matches specific criteria. When a correct solution is reached, a reward in the form of bitcoin and fees for the work done is given to the miner(s) who reached the solution first.

This reward process continues until 21 million bitcoins are circulating. Once that number is reached, the Bitcoin reward is expected to cease, and Bitcoin miners will be rewarded through fees paid for the work done.

- Validating transaction information, maintaining the integrity of the blockchain, and opening new blocks are mining's purposes, while the Bitcoin reward is the incentive to mine.
- Bitcoin mining is necessary to maintain the ledger of transactions upon which Bitcoin is based.
- Miners have become very sophisticated over the past several years, using complex machinery and grouping to speed up mining operations.
- Bitcoin mining has generated controversy because it is not considered environmentally friendly.

MINING DIFFICULTY

Every blockchain has a mining process by which miners can generate fresh coins. An algorithm regulates how difficult it is for the miners to mine a certain block. This difficulty is known as mining difficulty.

For mining a block, a miner must solve complex mathematical problems by finding a valid hash. As the process progresses, the network adjusts the rate so miners can find valid hashes. Each blockchain has its algorithm to regulate this adjustment. The algorithm increases or decreases the mining difficulty based on the rate at which miners can mine a block.

In recent times, the number of miners has increased manifold. Thus automatically, the mining difficulty of blockchains has also increased. Let's take an example for you to understand better. Bitcoin is a cryptocurrency that has become very popular. As a result, the number of miners on that blockchain has also increased.

The more the number of miners, the more computing power is used in the peer-to-peer network. And as a result, greater is the competition for the limited block rewards. Thus to adjust the rate at which miners can find blocks, the network raises its hash power.

This maintains the time a miner or a mining pool can successfully mine a block. The more the hash power, the more difficult it will be to find valid hashes for a block. Currently, it takes about 10 minutes to mine a Bitcoin block.

After every 2,016 blocks are mined, Bitcoin adjusts its mining difficulty. The difficulty will increase based on the number of miners and their combined hash power.

Benefits:

Mining difficulty may seem to you as a hindrance on your path to getting block rewards. However, it has its benefits too. They are:

Security of the network

As the mining difficulty increases, it becomes more difficult for a hacker to conduct a malicious attack on the network. Due to the increasing difficulty, miners use special ASIC mining computers that make trillions of guesses each second to find the correct hash for a block. A mining pool has scores of such systems on its floor to conduct the process. Thus, it

is very difficult for hackers to get enough computing power for majority control and launch an attack.

A steady mining rate

A miner's computing power differs from person to person and pool to pool. Thus to maintain parity in the mining process, the blockchain network raises or lowers its mining difficulty. This ensures that the network is generating blocks at a steady rate.

To overcome mining difficulty, you can simply join a mining pool. It will help you team up your computing power and get better results. Mining has its challenges; however, teaming up with other miners makes those difficulties much easier to bear.

MINING POOL

- A mining pool is a group of miners who work together to solve the cryptographic problems required by certain blockchains which reward the miners with cryptocurrency. Pools were created when cryptocurrency mining reached a difficulty level that only miners with enormous capacity could accomplish. Mining pools combine the efforts of individual or smaller mining groups to make them more competitive with the large mining operations that dominate the network.
- Mining has three purposes: it is the first verification of transactions, opens new blocks on the blockchain, and introduces new cryptocurrency into circulation.
- Mining pools split rewards based on how much work a miner contributes to the pool.
- Pools are essentially the only way to earn Bitcoin due to the centralization of the network's mining capacity.

Understanding the Mining Process

Cryptocurrency mining involves two functions—releasing new cryptocurrency into the system and verifying and adding transactions to the blockchain. It is performed using internet-connected devices and software programs which perform the mining process.

Crypto mining is a calculation-intensive, puzzle-solving-like computation process that requires high processing power and electricity consumption. The miner(s) who first solves the puzzle gets to place the next block on the blockchain and claim the rewards. Mining rewards include newly released Bitcoin and fees for the work done. All transaction fees on the Bitcoin blockchain are paid for by the user to whoever solves the problem.

The cryptocurrency discovery process is configured so that if more miners are working, the difficulty level goes up. A decline in the number of miners eases the difficulty level. The rewards make mining a lucrative activity for monetary gains. As more miners attempt to grab a piece of the pie, finding new blocks becomes computationally more difficult, requiring more computing power. This is often impractical and too expensive for individual miners who can't afford multiple mining-specific machines.

Pooling Resources: Let's Mine Better, Together

Enter the mining pool, a collection or group of miners working together to increase their chances of finding a block at the group level compared to that at the individual level. Through these pools, miners combine their individual computational resources with those of the other members. This enhances their joint processing power and helps them become more competitive, increasing their chances of receiving a reward.

To draw an analogy, imagine a gold digger has the capacity to dig 100 square meters of land in one day. It would take them 100 days to explore one hectare of land for gold. Combining 100 gold diggers with the same capacity can complete the job in just one day. Any gold discovered can be split among all 100 diggers evenly, assuming all have put in equal effort to explore their assigned portions of land.

Similarly, one can combine nine mining devices, each generating mining power of 335 megahashes per second (MH/s), to generate a combined output of around three gigahashes. The output is faster and has an increased chance to solve the puzzle.

Pooling Resources: Let's Mine Better, Together

Enter the mining pool, a collection or group of miners working together to increase their chances of finding a block at the group level compared to that at the individual level. Through these pools, miners combine their individual computational resources with those of the other members. This enhances their joint processing power and helps them become more competitive, increasing their chances of receiving a reward.

To draw an analogy, imagine a gold digger has the capacity to dig 100 square meters of land in one day. It would take them 100 days to explore one hectare of land for gold. Combining 100 gold diggers with the same capacity can complete the job in just one day. Any gold discovered can be split among all 100 diggers evenly, assuming all have put in equal effort to explore their assigned portions of land.

Similarly, one can combine nine mining devices, each generating mining power of 335 megahashes per second (MH/s), to generate a combined output of around three gigahashes. The output is faster and has an increased chance to solve the puzzle.

PERMISSIONED MODEL AND USE CASES

Some permissioned blockchain use cases include:

- Banks and **financial institutions** use these blockchains to facilitate faster and cost-effective **cross-border payments** and settlements. They streamline trade and **finance** processes, reducing fraud and improving transparency in international trade transactions.
- Companies in the food, pharmaceutical, and luxury goods industries use these blockchains to track the origin and journey of products, ensuring authenticity and compliance with regulations. They help manage inventory levels, automate reorder processes, and enhance **supply chain** visibility.
- Healthcare providers use such blockchains to securely and efficiently manage patient records, ensuring data privacy and integrity. Moreover, the pharmaceutical industry

employs them to trace the production and **distribution** of medications, reducing the risk of counterfeit drugs.

- One of the crucial permissioned blockchain use cases is to develop secure and transparent electronic voting systems, reducing the potential for fraud. Additionally, Governments can use these blockchains for identity verification, enhancing security in passport issuance and border control areas.
- They help artists and creaators protect their **intellectual property** rights by transparently recording ownership and usage rights. Furthermore, legal firms and businesses use these blockchains to automate contract execution and ensure compliance.
- Educational institutions utilize these blockchains to verify and share academic credentials securely. It aids in reducing fraud in the hiring process.

Advantages And Disadvantages

The advantages of Permissioned blockchains are as follows:

- They provide a higher degree of privacy and security. Access is restricted to authorized users, reducing the risk of data exposure and unauthorized transactions. It benefits industries like healthcare and finance, where sensitive data and regulatory compliance are critical.
- A select group of trusted entities governs these blockchains. This centralized governance structure enables quicker decision-making and facilitates network management.
- This blockchain often employs efficient consensus that offers faster transaction processing and requires less computational power, making it suitable for high-speed transactions where low latency is crucial.
- Due to controlled participation and efficient consensus, these blockchains can handle more transactions per second, making them scalable for enterprise-level applications.

The disadvantages of Permissioned blockchains are:

- They are often criticized for being less decentralized than public blockchains. The control and governance by a select group of participants can lead to concerns about centralization. This centralized control can undermine the fundamental principles of blockchain technology.
- Since these blockchains have fewer participants, they may be more susceptible to **collusion** or attacks from within the network. The network's security relies heavily on the trustworthiness of the participants and makes it vulnerable if any participant becomes compromised or malicious.
- Building and maintaining this blockchain can be expensive because of its initial development costs and ongoing operational **expenses**. Smaller organizations and startups may find it challenging to invest in the **infrastructure** and resources required for these blockchains.
- They have restricted access, which limits the **network effects** and potential benefits that can be achieved from a more extensive, open network. In contrast, the smaller networks may not offer the same innovation, **liquidity**, and ecosystem growth level.

Permissioned Blockchain vs Permissionless Blockchain

The differences between the two are as follows:

Permissioned Blockchain

- In these blockchains, access to the network and participation is restricted to authorized entities or participants who are granted permission. This controlled access allows for higher privacy, security, and regulatory compliance, making it suitable for applications where data access must be limited to trusted parties.
- These blockchains often have a more centralized governance model, with a select group of entities or consortium members making network rules and operations decisions.
- Thus, it prioritizes privacy and confidentiality by limiting data access to authorized participants and allowing for confidential transactions.

Permissionless Blockchain

- Permissionless blockchains are open to anyone who wants to participate without permission or approval. This open access promotes inclusivity, censorship resistance, and global participation. It aligns with the principles of decentralization.
- These blockchains are characterized by a high degree of decentralization, where no single entity or group controls the network.
- Thus, this blockchain prioritizes transparency, as anyone can view the transaction history and ledger contents.