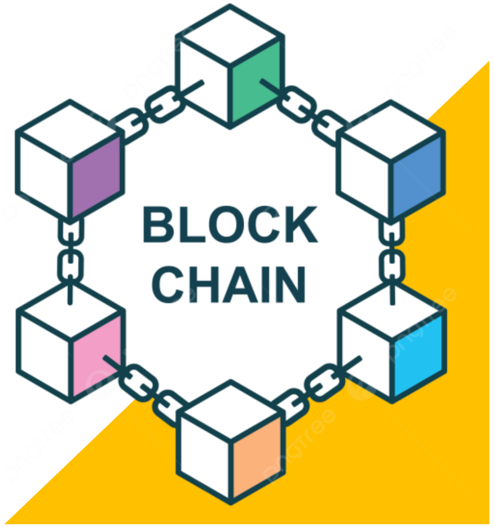
ARYA College of Engineering (ACE)
(Affiliated to RTU | Approved by AICTE, New Delhi)
- SP-40, RIICO Industrial Area, Delhi Road,
Kukas, Jaipur-302028 | Tel. Ph. 0141-2820700
- www.aryainstitutejpr.com
- Toll Free: 1800 102 1044

# Fundamentals of Blockchain

## Unit-1
## Basics



Er. Harsh Raj
(Assistant Professor, CSE)

# Course Objectives

1. The students should be able to understand a broad overview of the essential concepts of blockchain technology.

2. To familiarize students with Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming.

3. Students should be able to learn about different types of blockchain and consensus algorithms.

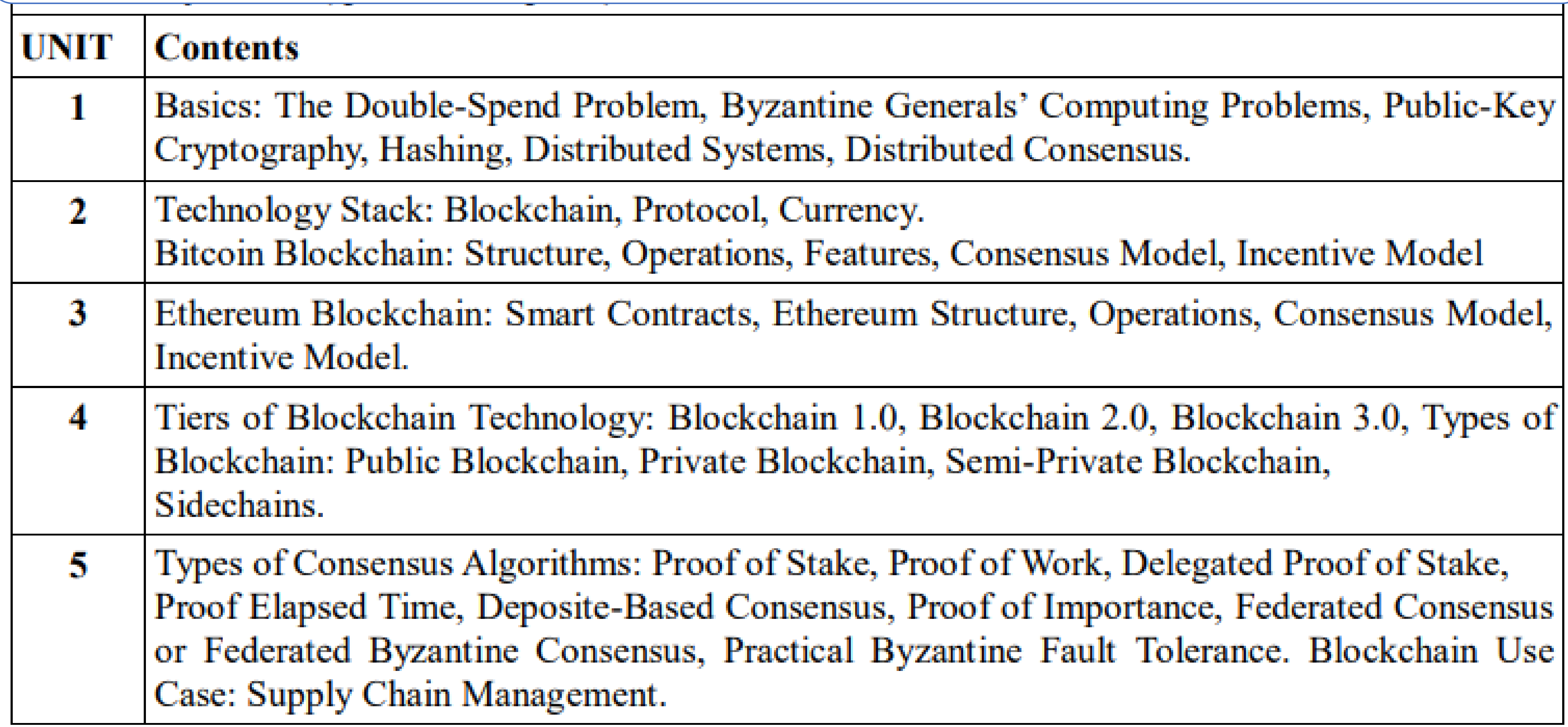
# Expected Course Outcome

1. To explain the basic notion of distributed systems.

2. To use the working of an immutable distributed ledger and trust model that defines blockchain.

3. To illustrate the essential components of a blockchain platform.

# Syllabus



| UNIT | Contents |
|---|---|
| 1 | Basics: The Double-Spend Problem, Byzantine Generals' Computing Problems, Public-Key Cryptography, Hashing, Distributed Systems, Distributed Consensus. |
| 2 | Technology Stack: Blockchain, Protocol, Currency.<br>Bitcoin Blockchain: Structure, Operations, Features, Consensus Model, Incentive Model |
| 3 | Ethereum Blockchain: Smart Contracts, Ethereum Structure, Operations, Consensus Model, Incentive Model. |
| 4 | Tiers of Blockchain Technology: Blockchain 1.0, Blockchain 2.0, Blockchain 3.0, Types of Blockchain: Public Blockchain, Private Blockchain, Semi-Private Blockchain, Sidechains. |
| 5 | Types of Consensus Algorithms: Proof of Stake, Proof of Work, Delegated Proof of Stake, Proof Elapsed Time, Deposite-Based Consensus, Proof of Importance, Federated Consensus or Federated Byzantine Consensus, Practical Byzantine Fault Tolerance. Blockchain Use Case: Supply Chain Management. |

# Text Books

1. Kirankalyan Kulkarni, Essentials of Bitcoin and Blockchain, Packt Publishing.
2. Anshul Kaushik, Block Chain & Crypto Currencies, Khanna Publishing House.
3. Tiana Laurence, Blockchain for Dummies, 2nd Edition 2019, John Wiley & Sons.
4. Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks by Imran Bashir, Packt Publishing (2017).

# Reference Books

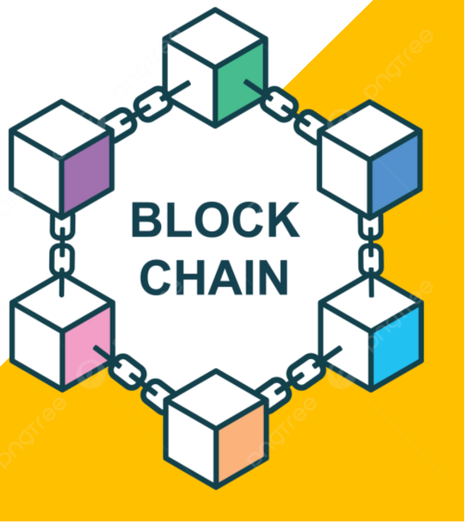
1. Blockchain: Blueprint for a New Economy by Melanie Swan, Shroff Publisher O'Reilly Publisher Media; 1st edition (2015).
2. Mastering Bitcoin: Programming the Open Blockchain by Andreas Antonopoulos.

# Topics

## Basics:

- The Double-Spend Problem
- Byzantine Generals' Computing Problems
- Public-Key Cryptography
- Hashing
- Distributed Systems
- Distributed Consensus

# Double-Spend Problem



# Double-Spend Problem

- Double spending means spending the same money twice.

- Any of the transactions can be processed only in two ways either offline or online.
  **Offline:** A transaction which involves physical currency or cash is known as an offline transaction.
  **Online:** A transaction which involves digital cash is known as an online transaction.

- The double spending problem is a fundamental challenge in digital currencies and blockchain technology.

- It refers to the risk of spending the same cryptocurrency tokens more than once, essentially creating a duplicate or counterfeit of the digital currency.

- In a traditional financial system, when you spend money, that amount is subtracted from your account, and you can't spend the same money again.

- This is because centralized authorities, such as banks, ensure that you have the necessary balance and prevent double-spending.

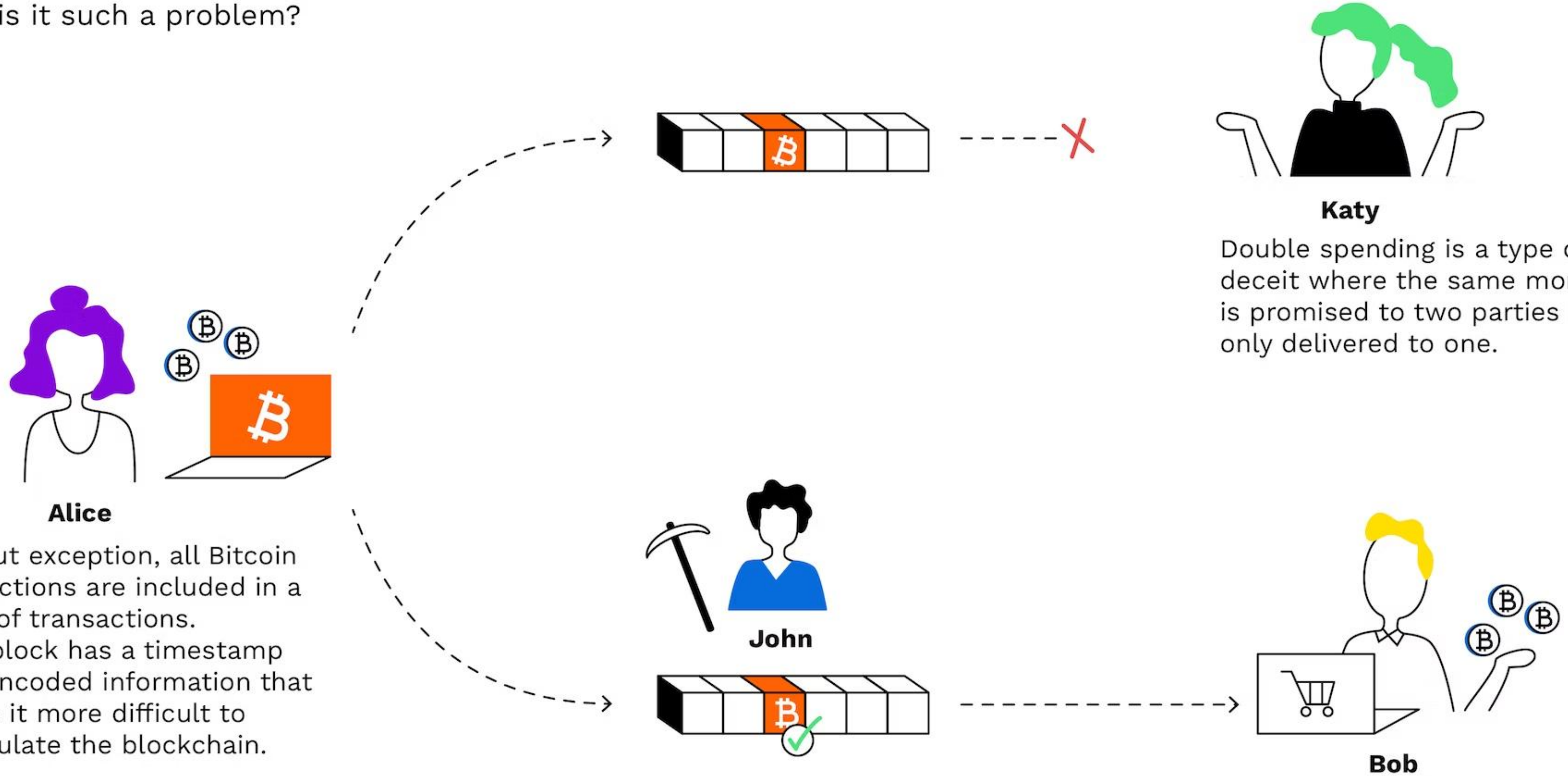
However, in the context of cryptocurrencies and blockchain:

1. Transactions are recorded on a decentralized and immutable ledger (the blockchain).
2. There is no central authority overseeing these transactions.
3. Cryptocurrencies exist only in digital form, making it theoretically possible for a malicious user to create multiple conflicting transactions using the same funds.

- The double spend problem arises when someone attempts to send the same cryptocurrency to two different recipients simultaneously or in quick succession.
- This can disrupt the integrity and trustworthiness of a digital currency system.
- Blockchain networks employ various mechanisms, such as consensus algorithms (e.g., Proof of Work or Proof of Stake), to prevent double-spending.
- These mechanisms ensure that transactions are validated and recorded in a way that makes it extremely difficult for a malicious actor to spend the same cryptocurrency tokens twice.
- Multiple confirmations of a transaction, achieved through the addition of new blocks to the blockchain, also help reduce the risk of double spending.

# What is Double Spending

and why is it such a problem?



**Alice**

Without exception, all Bitcoin transactions are included in a block of transactions.
Each block has a timestamp with encoded information that makes it more difficult to manipulate the blockchain.

**Katy**

Double spending is a type of deceit where the same money is promised to two parties but only delivered to one.

**John**

The mechanism of the blockchain ensures that the party spending the bitcoins is the real owner.

**Bob**

The technology behind Bitcoin ensures that the party who spends the bitcoins is the real owner by only processing verified transactions.

# Blockchain & Its Importance

Blockchain technology has gained significant importance and is being applied in various industries and applications due to its unique features and capabilities.

Key areas where blockchain is making an impact are:

1. **Cryptocurrencies:** The most well-known application of blockchain is in cryptocurrencies like Bitcoin and Ethereum. Blockchain provides a secure and decentralized ledger for recording transactions, enabling digital currencies to function without the need for traditional banks or intermediaries.

2. **Supply Chain Management:** Blockchain is used to improve transparency and traceability in supply chains. It allows companies to track the movement of products and raw materials in real time, reducing fraud, ensuring authenticity, and enhancing the efficiency of supply chain processes.

3. **Smart Contracts:** Smart contracts are self-executing contracts with the terms of the agreement directly written into code. Blockchain platforms like Ethereum enable the development of smart contracts, which automate and enforce contractual agreements, reducing the need for intermediaries and improving contract execution efficiency.

4. **Identity Verification:** Blockchain can be used to create secure and tamper-proof digital identity systems. Users have control over their identity information and can share it selectively with trusted parties, reducing the risk of identity theft and fraud.

5. **Voting Systems:** Blockchain-based voting systems can enhance the integrity and transparency of elections. Votes are recorded immutably on the blockchain, making it nearly impossible to manipulate or tamper with election results.

6. **Finance and Banking:** Blockchain is disrupting the financial industry by enabling faster and more cost-effective cross-border payments and remittances. It also has applications in trade finance, reducing paperwork and fraud risks.

7. **Real Estate:** Blockchain can streamline the real estate industry by reducing the complexity of property transactions. Property records can be securely stored on a blockchain, making it easier to verify ownership and transfer properties.

8. **Energy Trading:** Blockchain is used in peer-to-peer energy trading platforms, allowing individuals and organizations to buy and sell excess energy directly to each other, reducing the reliance on centralized energy providers.

9. **Education:** Blockchain can be used to verify educational credentials and certifications, reducing the risk of credential fraud.

# Importance of Trust & Security in Blockchain Transaction

Trust and security are paramount in blockchain transactions for several reasons, and they are fundamental to the success and adoption of blockchain technology in various applications.

Here's why trust and security are crucial in blockchain transactions:

1. **Preventing Fraud:** Trust and security mechanisms in blockchain prevent fraudulent activities like double-spending, where someone attempts to spend the same cryptocurrency twice. Through cryptographic techniques and consensus mechanisms, blockchain ensures that once a transaction is confirmed, it cannot be altered or reversed without the network's consensus.

2. **Enabling Decentralization:** Blockchain's trust model eliminates the need for intermediaries, such as banks or payment processors, by allowing direct peer-to-peer transactions. This decentralization reduces the risk of manipulation, censorship, and unauthorized access, promoting financial inclusivity and independence.

3. **Enhancing Transparency:** The transparent nature of blockchain transactions means that anyone can view the transaction history on the ledger. This transparency builds trust by allowing participants to verify the integrity of transactions and ensure that they are fair and accurate.

4. **Privacy and Control:** While blockchain transactions are transparent, they can also be designed to protect user privacy. Participants have control over their private keys and can choose what information to disclose. This balance between transparency and privacy is essential, especially in applications like healthcare and identity management.

5. **Smart Contracts:** Smart contracts are self-executing agreements with predefined rules. Trust in the underlying blockchain technology is crucial for the automation of contract execution. Users trust that the code will perform as intended, without the need for intermediaries.

6. **Financial Services:** In the financial industry, trust and security are essential for providing services like custody, asset management, and lending. Blockchain technology enhances security and reduces counterparty risk in these financial processes.

7. **Data Integrity:** Blockchain's immutability ensures the integrity of data stored on the ledger. Once data is recorded, it becomes extremely challenging to alter or delete, reducing the risk of data tampering or manipulation.

# How Traditional System Prevent Double Spending

Traditional financial systems, like those involving physical cash or centralized digital databases, prevent double spending through a combination of centralized control, account management, and transaction validation.

How typical to achieve this:

1. **Centralized Ledger:** Traditional financial systems operate with a centralized ledger that is maintained and controlled by a trusted authority, such as a bank or a payment processor. This ledger records all financial transactions and account balances.

2. **Account-Based System:** In these systems, each user has an account with a trusted authority. The account records the user's balance, and when a transaction occurs, the system subtracts the appropriate amount from the sender's account and adds it to the recipient's account.

3. **Authorization and Verification:** Before a transaction is processed, the traditional financial system ensures that the sender has sufficient funds to cover the transaction. This is done by checking the sender's account balance. If the balance is insufficient, the transaction is rejected.

4. **Transaction Settlement:** Once a transaction is authorized and verified, it is settled in the ledger, updating the account balances accordingly. This settlement is typically irreversible and cannot be easily altered.

5. **Trust in Central Authority:** Users of traditional financial systems trust the central authority (e.g., a bank) to maintain the integrity of the ledger and prevent double-spending. The authority has mechanisms in place to detect and prevent fraudulent activities.

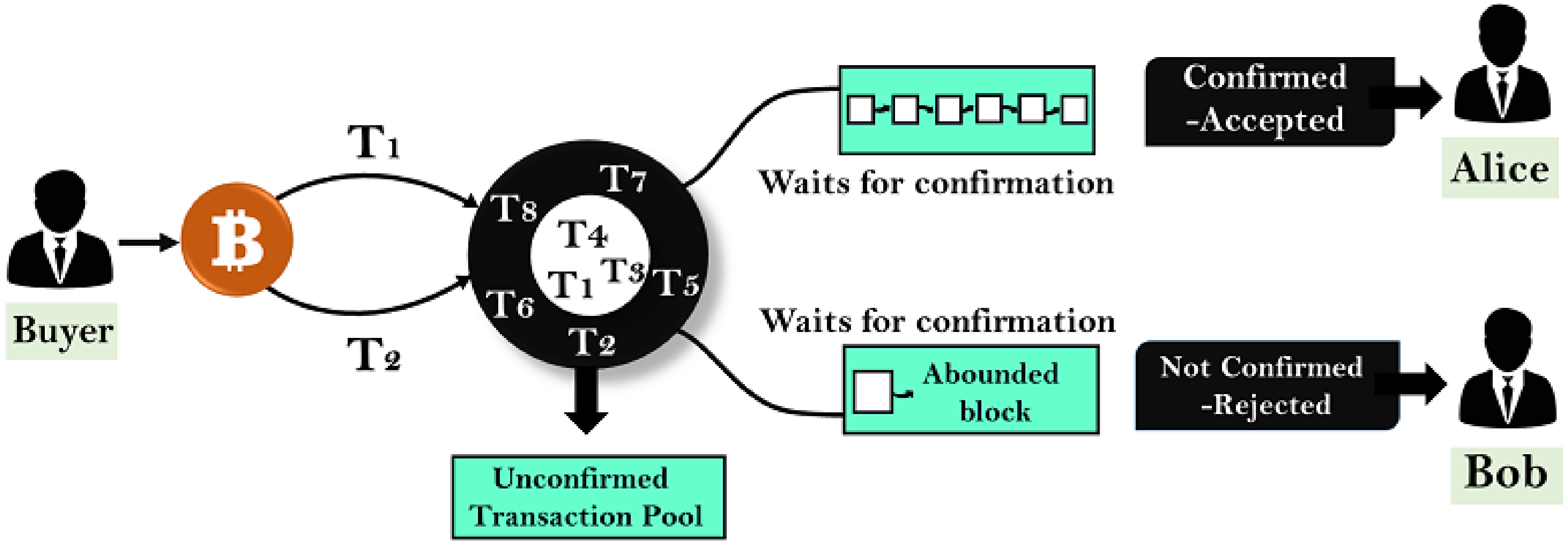
6. **Paper Currency:** In the case of physical cash, the prevention of double spending is inherent in the physical nature of the currency. When you give someone a physical banknote, you no longer possess it, making it impossible to spend the same note again unless it is physically counterfeit.

7. **Digital Transactions:** For digital transactions (e.g., credit card payments), central authorities use encryption, authentication, and authorization mechanisms to ensure that each transaction is processed only once.

8. **Account Reconciliation:** Centralized systems regularly reconcile and audit their ledgers to identify and rectify any discrepancies or irregularities.

Note: Traditional financial systems are effective in preventing double spending within their centralized frameworks, but they also come with drawbacks, including the need for intermediaries, potential points of failure, and limitations on financial inclusivity.

In other words, blockchain technology, used in cryptocurrencies like Bitcoin, was developed to address these limitations by providing a decentralized and trustless solution to the double-spending problem.
Blockchain achieves this through cryptographic techniques, consensus mechanisms, and a distributed ledger that makes it virtually impossible to double-spend without controlling most of the network's computational power.



- ***Proof of Work (PoW)*** is a consensus mechanism in blockchain where miners compete to solve complex puzzles. The first to find a valid solution adds a new block, validating transactions and earning rewards. PoW ensures network security, but it's energy-intensive and has environmental concerns, leading to the exploration of more efficient alternatives.

- ***Proof of Stake (PoS)*** is a consensus mechanism in blockchain networks where validators are chosen to create new blocks and confirm transactions based on the number of cryptocurrency tokens they hold and "stake" as collateral. PoS is energy-efficient compared to Proof of Work (PoW) and aims to secure the network while reducing environmental impact. Validators earn rewards for their participation and can lose their stake for malicious behaviour.

# Blockchain's Solution to Double Spending

Blockchain technology provides an innovative and effective solution to the double spending problem in digital currencies and transactions.

How blockchain addresses this issue are:

1. **Decentralization:** Blockchain operates on a decentralized network of computers (nodes) where there is no central authority overseeing transactions. Instead of relying on a single trusted entity, like a bank, to maintain a ledger and prevent double spending, blockchain transactions are verified and recorded by multiple nodes spread across the network.

2. **Immutable Ledger:** Once a transaction is confirmed and added to a blockchain, it becomes part of an immutable and tamper-proof ledger. Transactions are grouped into blocks and linked together in a chronological chain, with each block containing a reference to the previous one. This makes it exceptionally difficult to alter or delete a transaction once it's on the blockchain.

3. **Consensus Mechanisms:** Blockchain networks use consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate and agree on the state of the ledger. Consensus ensures that all participants on the network agree on the order and validity of transactions. It prevents malicious actors from creating multiple conflicting transactions and double-spending.

4. **Transaction Verification:** When a transaction is initiated, it is broadcasted to the network for validation. Nodes on the network verify the transaction by confirming that the sender has the necessary funds and ensuring that the transaction hasn't already been spent. Only valid transactions are added to the blockchain.

5. **Multiple Confirmations:** Most blockchain networks require multiple confirmations, which involve adding new blocks to the blockchain, before considering a transaction as final. The more confirmations a transaction has, the more secure and irreversible it becomes. This significantly reduces the risk of double spending.

6. **Economic Incentives:** In Proof of Work (PoW) systems like Bitcoin, miners are rewarded for their work in securing the network and adding blocks to the blockchain. Attempting to double spend would require controlling most of the network's mining power, which is economically impractical and expensive.

7. **Transparent and Public Ledger:** Blockchain transactions are transparent and can be viewed by anyone on the network. This transparency helps detect and prevent double spending attempts, as any suspicious activity can be easily identified.

# How Blockchain Prevents Double Spending

Blockchain technology prevents double spending, which is a critical issue in digital currency systems, through a combination of cryptographic techniques, decentralized consensus, and a distributed ledger.

How blockchain addresses the double spending problem:

1. **Decentralization:** Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes (computers). This means there is no single central authority controlling the ledger. Transactions are verified and recorded by multiple participants in the network.

2. **Consensus Mechanisms:** Blockchain networks use consensus mechanisms to agree on the state of the ledger and which transactions should be added to it. The most well-known consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS). These mechanisms require participants to solve complex mathematical puzzles or stake cryptocurrency as collateral to validate transactions. Consensus ensures that only valid transactions are added to the blockchain.

3. **Double Spend Prevention:** Blockchain nodes maintain a record of all transactions on the network. When a user attempts to spend the same cryptocurrency twice (a double spend), nodes reject the second transaction because they recognize that the funds have already been spent in a previous, valid transaction. This rejection occurs during the transaction verification process.

# Attack Vector for Double Spending

Double spending is a critical challenge in digital currency systems, including blockchain-based cryptocurrencies. While blockchain technology has robust mechanisms to prevent double spending, there are still some potential attack vectors that malicious actors may exploit to attempt double-spending.

Few attack vectors are:

1. **Race Attack (Race Condition):** In a race attack, the malicious user tries to broadcast two conflicting transactions nearly simultaneously. They send one transaction to a merchant or recipient to make a payment while simultaneously sending another transaction spending the same funds back to themselves. The goal is to get the merchant to accept the first transaction, believing it is valid, and then confirm the second transaction, effectively double spending the funds.

2. **Finney Attack:** Named after Bitcoin pioneer Hal Finney, this attack involves a miner who has a mining reward waiting to be confirmed. The miner includes a double spending transaction in the next block they mine. The idea is to mine a new block quickly and confirm the double-spending transaction before the network can validate the original transaction.

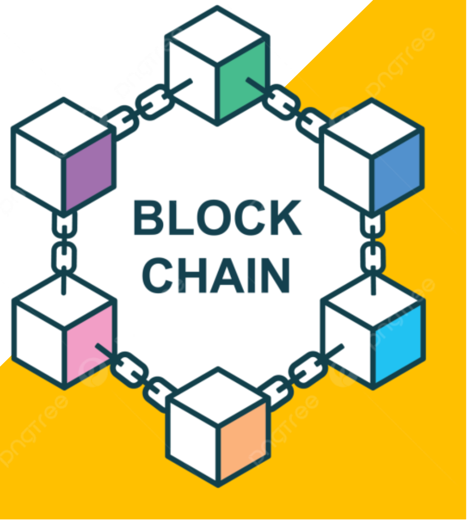
3. **Vector76 Attack (Replace-by-Fee):** This attack relies on the replace-by-fee feature that allows a user to replace an unconfirmed transaction with a higher-fee transaction that spends the same coins. If the attacker sends a transaction with a low fee, they can then send another transaction with a higher fee to miners, encouraging them to confirm the latter transaction instead.

4. **51% Attack:** In a 51% attack, an entity or group of miners controls more than 50% of the mining power in a Proof of Work (PoW) blockchain network. They can manipulate the blockchain's consensus rules with majority control and potentially execute double-spending attacks. However, this kind of attack is extremely expensive and usually not feasible for well-established cryptocurrencies like Bitcoin.

5. **Selfish Mining Attack:** This attack involves a miner or a group of miners withholding their mined blocks from the network. By doing this, they can manipulate the confirmation process and increase their chances of successfully double-spending. However, this attack is also challenging to execute successfully and is less of a threat in large and secure blockchain networks.

It's important to note that while these attack vectors exist, blockchain networks have countermeasures in place to mitigate them.
The security and integrity of blockchain networks rely on the network's decentralization, consensus mechanisms, and economic incentives for miners to follow the rules and act honestly.
The more decentralized and secure a blockchain network is, the more resistant it is to double-spending attacks and other malicious activities.
Additionally, most merchants and services wait for multiple confirmations before considering a transaction as final, further reducing the risk of double-spending.

# Byzantine Generals' Computing Problems

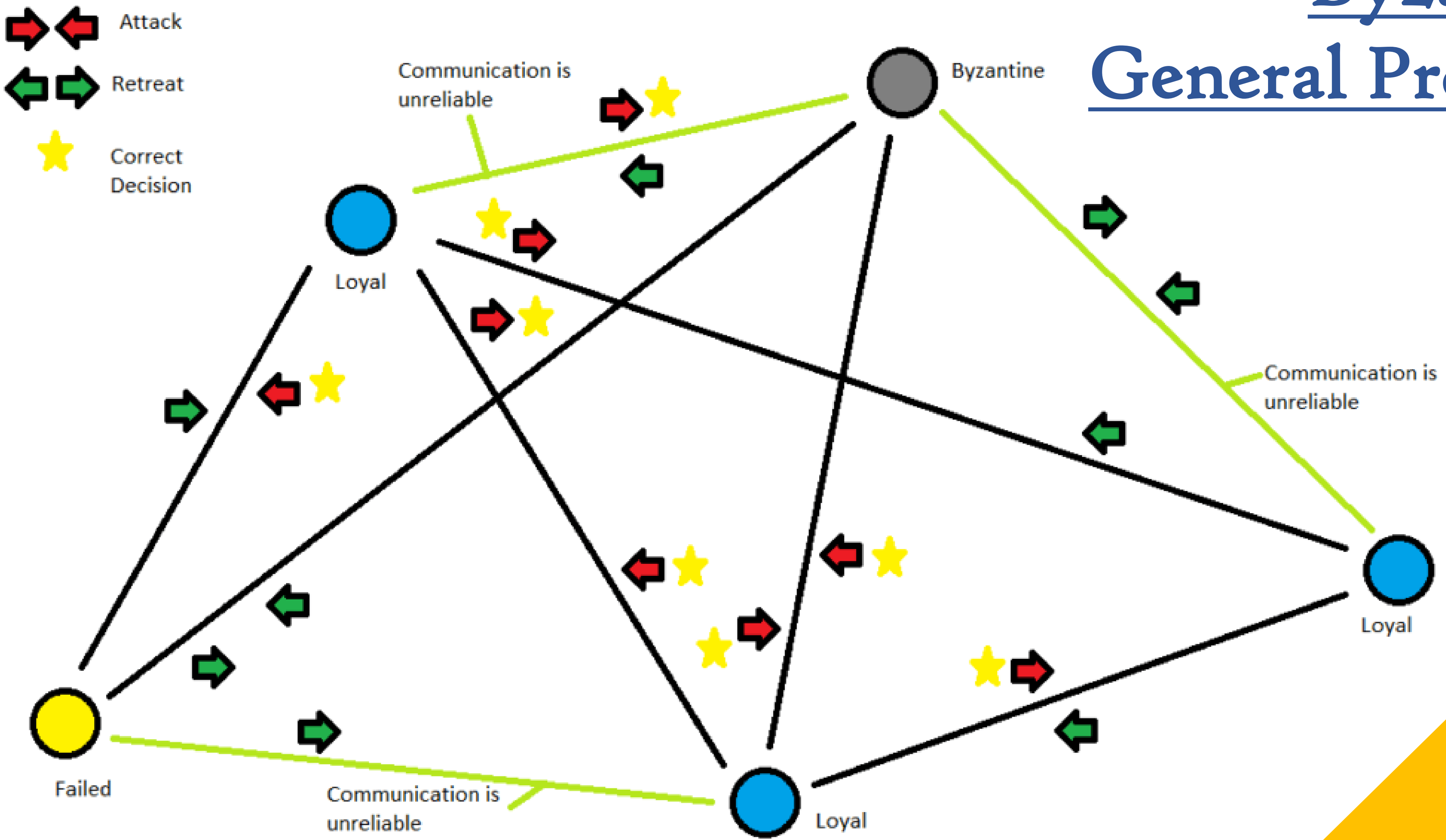


# Byzantine Generals’ Computing Problem

- The Byzantine Generals' Problem, also known as the Byzantine Fault Tolerance problem, is a classic issue in distributed computing and computer science. It describes a scenario where a group of generals, each commanding a portion of a Byzantine army, are encircling an enemy city. The generals need to reach a consensus on whether to attack or retreat.

- The Byzantine Generals' Problem is a classic problem in distributed computing and computer science, often used to illustrate the challenges and solutions in reaching consensus among distributed nodes, even when some of the nodes may be faulty or malicious. The problem is named after the "Byzantine Generals" as a metaphor for distributed systems facing uncertain or untrustworthy communication channels.

# Byzantine General Problem


Attack
Retreat
Correct Decision
Communication is unreliable
Byzantine
Loyal
Communication is unreliable
Loyal
Failed
Communication is unreliable
Loyal

# Scenario

- Imagine a group of Byzantine generals, each commanding a portion of an army, encircling an enemy city. These generals need to decide whether to attack or retreat. They can communicate with each other only through messengers, and some of the messengers may be traitors who provide false information or deliberately alter the messages.

- The problem is to ensure that the loyal generals reach a consensus on whether to attack or retreat, despite the presence of traitorous generals and unreliable messengers. The generals must agree on a common plan of action to avoid disaster, as attacking or retreating independently could lead to defeat.

# Challenges

The Byzantine Generals' Problem highlights several challenges:

1. **Faulty Generals:** Some generals may be traitorous, sending contradictory or false messages to confuse the loyal generals.
   - Some generals may be traitorous and deliberately send conflicting or incorrect messages.
   - These traitorous generals can undermine the decision-making process by spreading misinformation.

2. **Unreliable Messengers:** The messengers may deliver messages incorrectly or modify the content, making it difficult to trust the information received.
   - Messengers can deliver messages incorrectly or tamper with the content.
   - Generals cannot be certain if the messages they receive are trustworthy or have been manipulated.

3. **Asynchronous Communication:** There's no guarantee about the timing of message delivery, which means messages may arrive at different times or get lost.
   - There is no guarantee that messages will be delivered in a timely manner. Messages may arrive at different times, or some may be lost in transit.
   - Asynchronous communication can lead to confusion, as generals may act on outdated or incomplete information.

4. **Need for Unanimity:** The loyal generals must achieve unanimous agreement on the course of action. Even a single traitorous general who persuades a loyal one to deviate from the consensus could lead to a disastrous outcome.
   - In this scenario, it is essential for the loyal generals to achieve unanimous agreement on whether to attack or retreat.
   - A single dissenting or traitorous general, if persuasive enough, can lead some generals to make a decision that differs from the consensus, resulting in failure.

# Solutions

Various algorithms and protocols have been developed to solve the Byzantine Generals' Problem in distributed computing. One well-known solution is the **Byzantine Fault Tolerance (BFT)** algorithm.

Here's a simplified overview of how BFT works:

1. **Commander and Lieutenants:** In the BFT algorithm, one general is designated as the commander, and the others are lieutenants. The commander initiates the decision-making process.

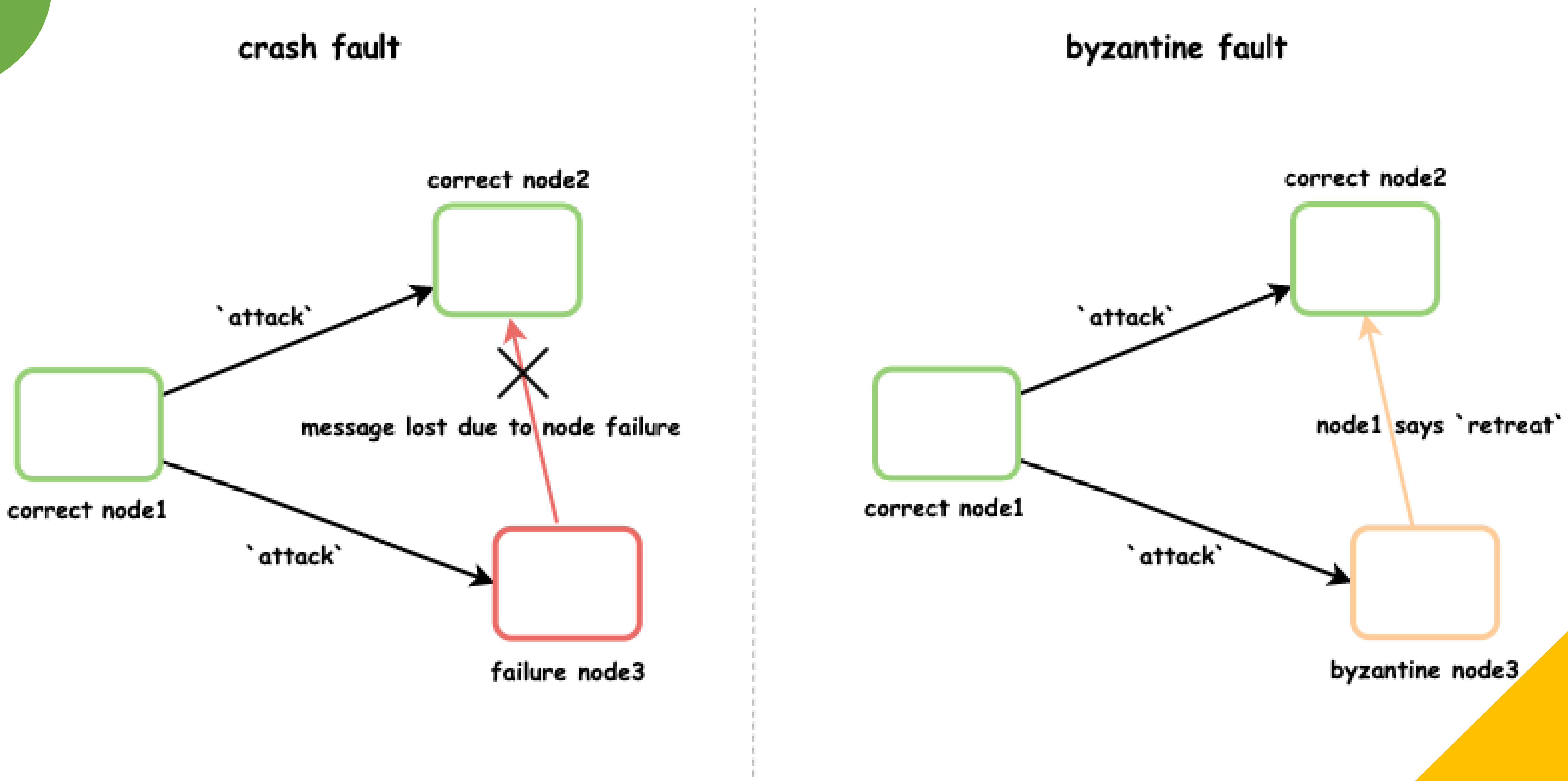
2. **Majority Rule:** The generals communicate with each other by sending messages. To reach a consensus, the loyal generals must have a majority agreement. For example, if there are 3 generals, 2 of them must agree on a plan.

3. **Redundant Communication:** To ensure reliability, the generals exchange messages multiple times. The commander sends the same message to all lieutenants, and lieutenants share their received messages with each other.

4. **Verification:** Each general verifies the messages received from others. If they detect discrepancies or conflicting information, they can conclude that the sender of those messages is traitorous.

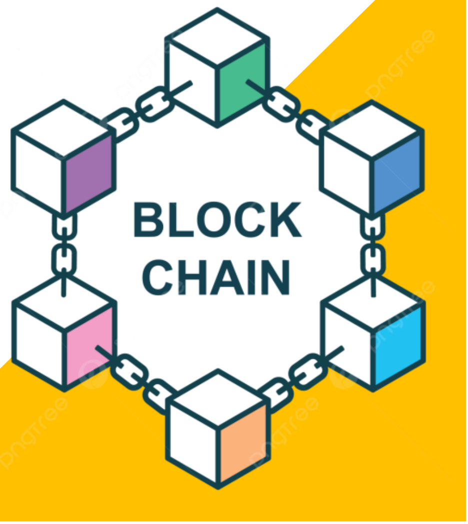
5. **Reaching Consensus:** The commanders and lieutenants continue to communicate and exchange messages until a consensus is reached. Once a majority agrees on a plan, they all execute it.

BFT and similar algorithms ensure that even in the presence of traitorous generals and unreliable messengers, the loyal generals can reach a consensus and make a unified decision, thus solving the Byzantine Generals' Problem. These algorithms have applications in distributed systems, blockchain technology, and other areas where consensus among distributed nodes is critical for reliability and security.



# Byzantine Fault

# Public Key Cryptography



# Public-Key Cryptography

- Public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use.

- The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key.

- Public key cryptography, also known as asymmetric cryptography, is a fundamental cryptographic technique used for securing communications, digital signatures, and data encryption.

- It relies on the use of a pair of cryptographic keys: a public key and a private key, which are mathematically related but serve different purposes.

# Working & Its Key Concept

1. Key Pair Generation:
   - **Public Key:** This key is intended to be shared openly and is used for encryption and verification. It is generated from the private key using a mathematical algorithm. A public key, once generated, can be freely distributed to anyone.

   - **Private Key:** This key must be kept secret and is used for decryption and creating digital signatures. It is generated along with the public key, but its secrecy is crucial to the security of the system.

2. Encryption:
   - When someone wants to send a secure message to another person, they use the recipient's public key to encrypt the message. Once encrypted with the public key, the message can only be decrypted using the corresponding private key, which is held only by the intended recipient. This ensures confidentiality because only the recipient can read the message.

   - Common encryption algorithms used in public key cryptography include RSA (Rivest-Shamir-Adleman) and ElGamal.

3. **Decryption:**

The recipient, who possesses the private key corresponding to the public key used for encryption, can decrypt the message.

The private key is mathematically designed to work in tandem with the public key, allowing the recipient to recover the original message.

4. **Digital Signatures:**

- In public key cryptography, digital signatures are used to verify the authenticity and integrity of a message or document. To create a digital signature, the sender uses their private key to encrypt a hash (a fixed-size value derived from the content) of the message or document. This creates a unique signature that can only be verified using the sender's public key.

- The recipient of the digitally signed message can use the sender's public key to decrypt the signature and verify that it matches the hash of the received message. If the signature is valid, it confirms that the message has not been tampered with and was indeed signed by the holder of the private key.

## 5. Applications:

- Public key cryptography plays a crucial role in securing digital communication over the internet. For example, HTTPS (Hypertext Transfer Protocol Secure) uses public key cryptography to encrypt data exchanged between web browsers and servers.

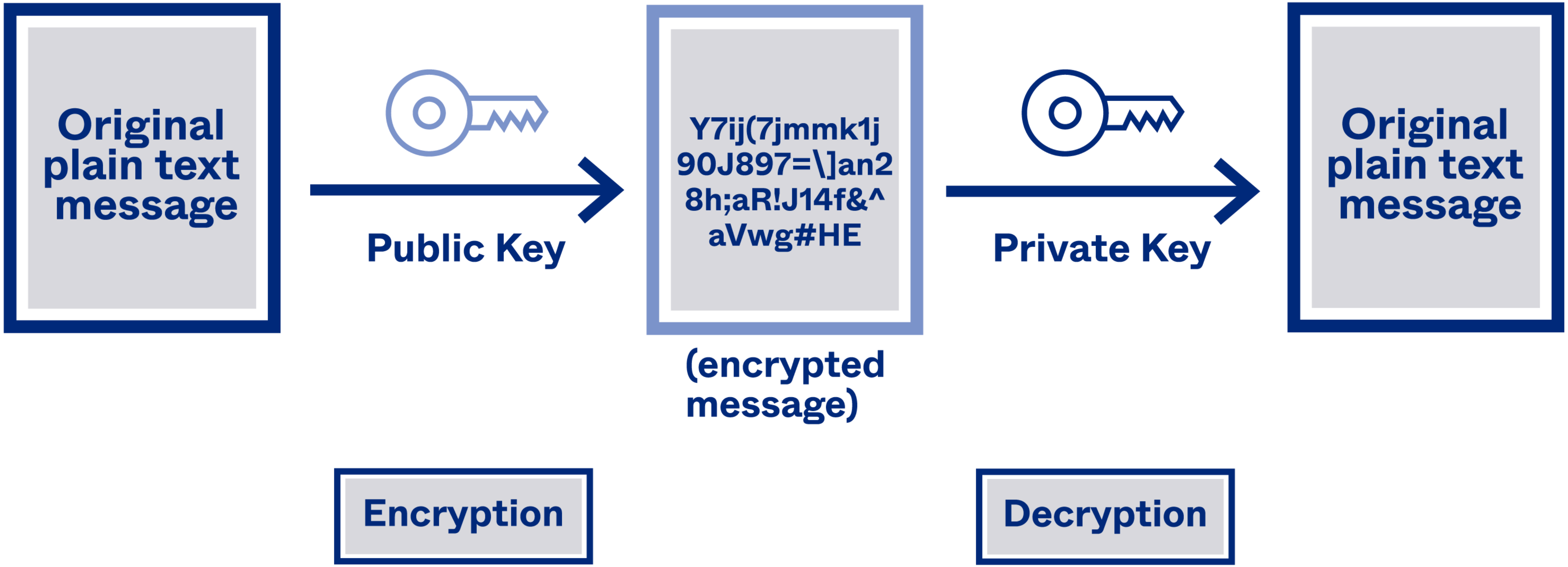
- Secure email communication, as implemented in PGP (Pretty Good Privacy) and GPG (GNU Privacy Guard), relies on public key cryptography.

- Digital wallets for cryptocurrencies use public key cryptography to secure transactions. Users have a pair of keys: a public address (used to receive funds) and a private key (used to sign transactions).

- Secure authentication and digital identity management use public key cryptography to verify the identity of individuals and devices.

***Public key cryptography*** is a cornerstone of modern cybersecurity, providing a robust framework for secure communication and authentication in an open and interconnected digital world. Its mathematical foundations ensure that even though the public key is openly shared, the private key remains a well-guarded secret, enabling secure encryption and digital signatures.

# Public Key Encryption



Original plain text message

Public Key

Y7ij(7jmmk1j
90J897=\]an2
8h;aR!J14f&^
aVwg#HE

(encrypted message)

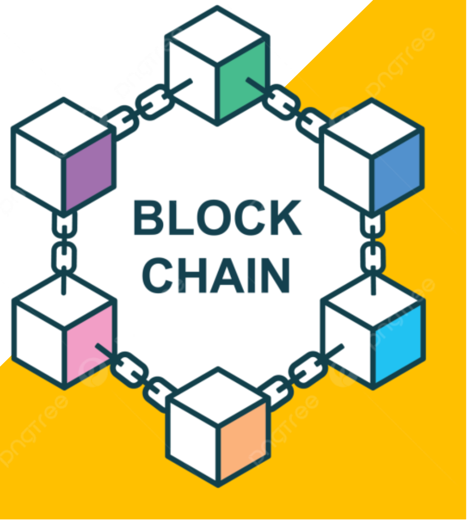
Private Key

Original plain text message

Encryption

Decryption

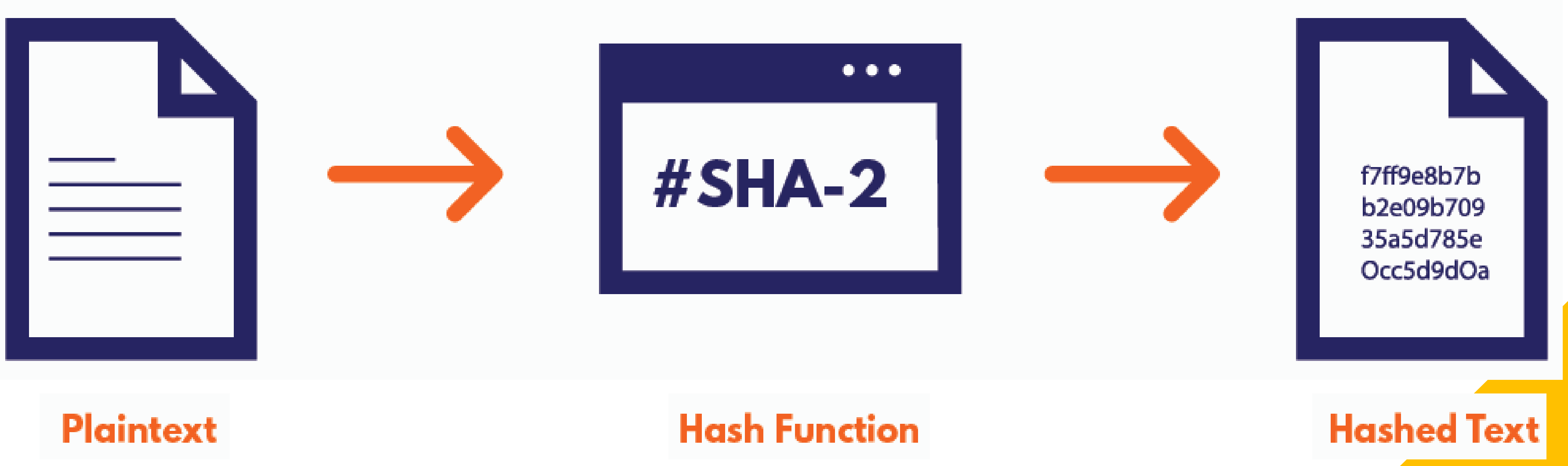
# Hashing



# Hashing

- Hashing plays a crucial role in blockchain technology. It is a fundamental concept that contributes to the security, integrity, and immutability of data stored on a blockchain.

- Hashing is a process of converting input data (also known as a message or plaintext) into a fixed-size string of characters, which is typically a hexadecimal number. This output is called a hash value or simply a hash. Hash functions are designed to take an input and produce a unique, seemingly random output, which is based on the input data.



# How Hashing Works In Blockchain?

1. **Hash Functions:** In the context of blockchain, a hash function is a mathematical algorithm that takes an input (data of arbitrary size) and produces a fixed-size string of characters, which is the hash value. Some commonly used cryptographic hash functions in blockchain include SHA-256 (used in Bitcoin) and Keccak-256 (used in Ethereum).

2. **Data Integrity:** Blockchain uses hashing to ensure the integrity of data within each block. When a block is created, all the transactions within it, along with some additional data (like a timestamp or block number), are concatenated and passed through the hash function. This process generates a unique hash value for that block. If anyone alters even a single bit of data in the block, the resulting hash will be completely different, making it easy to detect tampering.

3. **Chaining Blocks:** In a blockchain, each block contains a reference to the hash of the previous block. This reference is called the "previous hash" or "parent hash." When a new block is created, it includes the hash of the previous block in its data. This linking of blocks via their hashes creates a chain of blocks, which is a fundamental feature of blockchain technology. It ensures the chronological order and immutability of transactions.

4. **Mining and Proof of Work (PoW):** In PoW-based blockchain networks like Bitcoin, miners compete to solve a complex mathematical puzzle by finding a nonce (a random number). Miners repeatedly change this nonce until they produce a hash value that meets certain criteria. The criteria often involve having a hash that starts with a specific number of leading zeros. This process is known as "finding a proof of work." Once a miner finds a valid proof of work, they can broadcast their block to the network. This adds the block to the blockchain and is the basis for achieving consensus in the network. The PoW system relies on the computational difficulty of finding this proof of work, making it costly and time-consuming to create new blocks. It also secures the network by making it prohibitively difficult for an attacker to control a majority of the network's computational power.

5. **Address Generation:** Cryptocurrency addresses in blockchain systems are often derived from a user's public key through a process called "hashing." The user's public key is first hashed to produce a shorter, fixed-length value known as the address. This address is used for sending and receiving cryptocurrencies. Importantly, the original public key remains hidden, preserving user privacy.

***Hashing*** in the blockchain is used for data integrity, creating the chain of blocks, securing the network through PoW, and generating cryptocurrency addresses. It's a foundational concept that underpins the security and functionality of blockchain technology, ensuring that data remains tamper-proof, and the network remains resistant to attacks.

# Hashing Algorithm

Hashing algorithms are mathematical functions that take an input (or "message") and return a fixed-size string of characters, which is typically a hexadecimal number.
These algorithms are designed to efficiently transform input data into a unique hash value.

In the context of computer science and cryptography, hashing algorithms have several important properties:

1. **Deterministic:** The same input will always produce the same hash value. This property is crucial for data integrity and consistency.

2. **Fast Computation:** Hash functions are designed to produce a hash value quickly, even for large inputs.

3. **Fixed Output Length:** Regardless of the size or length of the input data, the hash function produces a fixed-size hash value. For example, the SHA-256 algorithm always produces a 256-bit (32-byte) hash value.

4. **Preimage Resistance:** Given a hash value, it should be computationally infeasible to determine the original input. In other words, it should be difficult to reverse the hash function.

5. **Collision Resistance:** It should be extremely unlikely for two different inputs to produce the same hash value. Collisions can compromise the security of hash functions.

6. **Avalanche Effect:** A small change in the input data should result in a significantly different hash value. This property makes it challenging to predict the impact of changes in the input.

Several widely used hashing algorithms exist, each with its own characteristics and use cases.

A few notable examples are:

1. **SHA-256 (Secure Hash Algorithm 256-bit):** This cryptographic hash function is commonly used in blockchain technologies like Bitcoin. It produces a 256-bit (32-byte) hash value.

2. **MD5 (Message Digest Algorithm 5):** MD5 was once widely used but is now considered weak due to vulnerabilities to collision attacks. It produces a 128-bit (16-byte) hash value.

3. **SHA-1 (Secure Hash Algorithm 1):** SHA-1 is also considered weak due to vulnerabilities, and it is being phased out in favour of stronger hash functions. It produces a 160-bit (20-byte) hash value.

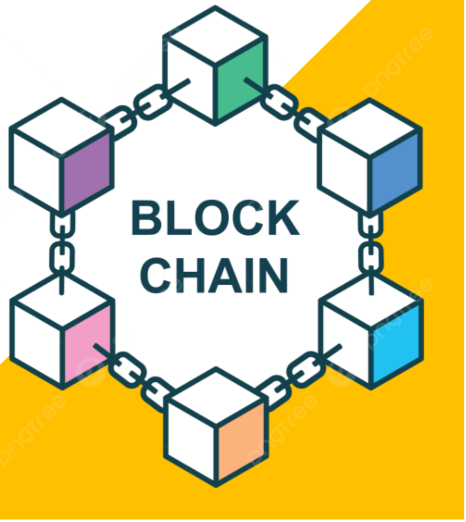
4. **SHA-3 (Secure Hash Algorithm 3):** SHA-3 is part of the Keccak family of hash functions and provides a high level of security. It comes in various bit-length versions, such as SHA-3-256, SHA-3-512, etc.

5. **bcrypt:** Bcrypt is a cryptographic hash function designed for securely hashing passwords. It includes a salt (a random value) to protect against rainbow table attacks.

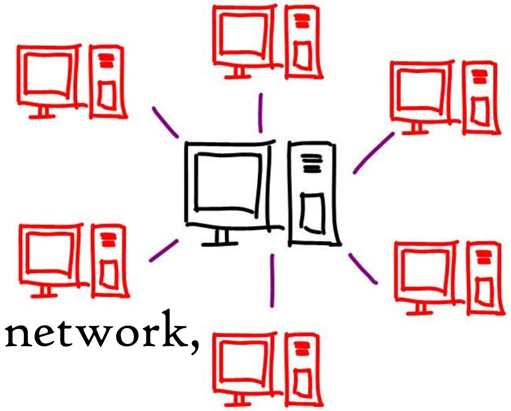
6. **Scrypt:** Like bcrypt, Scrypt is designed for secure password hashing. It is computationally intensive and memory-hard to resist brute-force and dictionary attacks.

The choice of a ***hashing algorithm*** depends on the specific use case and security requirements. For secure applications, it is essential to use well-vetted cryptographic hash functions like ***SHA-256*** or ***SHA-3***, while weaker algorithms like ***MD5*** and ***SHA-1*** should be avoided due to their susceptibility to attacks.

# Distributed Systems



# Distributed Systems



- A distributed system is a collection of independent computers, interconnected via a network, capable of collaborating on a task.
- A distributed system in the context of blockchain refers to the underlying infrastructure and network of computers that work together to maintain and validate the blockchain ledger. Blockchain technology relies on a distributed system to achieve its core principles of decentralization, transparency, and security.
- A distributed system is a network of interconnected computers or nodes that work together as a unified computing resource.
- In a distributed system, the processing tasks, data storage, and communication are distributed across multiple nodes, often geographically dispersed. These nodes collaborate to achieve a common goal, such as solving a complex problem, providing a service, or managing data.
- Distributed systems are designed to improve performance, reliability, and scalability by leveraging the combined computational power and redundancy of multiple nodes.

# Key Aspects Of A Distributed System In Blockchain

## Decentralization

- **Role of Decentralization:** Decentralization in blockchain refers to the absence of a central authority or control in the network. Instead of relying on a single entity (like a bank or government), blockchain distributes power and decision-making among a network of nodes (computers). This ensures that no single entity has the ability to manipulate or control the network's transactions or data.

- **Benefits of Decentralization:** Decentralization offers several advantages, including:
  - **Censorship Resistance:** Transactions cannot be censored or blocked by a central authority.
  - **Trust Minimization:** Users don't need to trust a single entity; they trust the decentralized network.
  - **Enhanced Security:** Decentralization makes it harder for malicious actors to attack the network.
  - **Availability:** The network remains operational even if some nodes fail or go offline.

- **Challenges of Decentralization:** While decentralization offers many benefits, it also comes with challenges, such as:
  - **Scalability:** It can be challenging to scale a decentralized network while maintaining its integrity.
  - **Energy Consumption:** Some consensus mechanisms, like Proof of Work, can be energy-intensive.
  - **Governance:** Decentralized networks often require mechanisms for decision-making and protocol upgrades, which can be complex.

## *Consensus Mechanism*

- **Proof of Work (PoW):** In PoW, nodes (miners) compete to solve complex mathematical puzzles. The first one to solve it gets the right to create a new block of transactions. This process is resource-intensive and requires miners to perform computational work, making it secure but energy-intensive.
- **Proof of Stake (PoS):** PoS operates differently, with validators chosen to create new blocks based on the amount of cryptocurrency they "stake" as collateral. PoS is energy-efficient but relies on the economic incentive of validators not to act maliciously.
- **Delegated Proof of Stake (DPoS):** DPoS further simplifies consensus by allowing a limited number of trusted validators to create blocks. DPoS is known for its scalability and efficiency.

# Peer – to -Peer (P2P) Network

- **P2P Networking in Blockchain:** In blockchain, a P2P network consists of nodes (peers) that communicate directly with each other, without relying on central servers. Each node is equal in status, and they collaborate to maintain the network.

- **Advantages of P2P Networks:** P2P networks offer:
  - **Fault Tolerance:** No single point of failure; if one node goes down, others continue to operate.
  - **Censorship Resistance:** Difficult to censor or shut down as there's no central entity to target.
  - **Resilience:** Robustness in the face of network disruptions or attacks.

- **P2P Security:** P2P networks enhance security by eliminating central targets. Data is distributed across multiple nodes, making it challenging for malicious actors to compromise the network's integrity.

# Replication and Data Consistency

- **Data Replication:** In blockchain, data is replicated across multiple nodes. Each node maintains a copy of the entire ledger, ensuring data availability and redundancy.
- **Consistency Models:** Blockchains use various consistency models, such as eventual consistency or strong consistency, to ensure that all nodes eventually agree on the state of the ledger. Eventual consistency allows temporary inconsistencies to accommodate network latency, while strong consistency ensures immediate agreement.

## Fault Tolerance

**Fault Tolerance Mechanisms:** Blockchain systems employ various techniques, such as redundancy (duplicate data across nodes), data validation (ensuring data integrity), and consensus algorithms to maintain fault tolerance. These mechanisms ensure that the network continues to function even if some nodes experience issues.

## Security

- **Cryptography in Blockchain:** Cryptography is fundamental to blockchain security. It involves techniques like digital signatures to verify the authenticity of transactions and participants, as well as encryption to protect data during transmission.
- **Access Control:** Blockchain uses public and private keys to control access to assets and data. Public keys serve as addresses, while private keys grant ownership and control.

## Interoperability

- **Interoperability Standards:** Interoperability in blockchain is achieved through standards and protocols that allow assets and data to move seamlessly between different blockchains or networks.

## Scalability

- **Scalability Challenges:** Blockchain networks face scalability challenges as they grow. Transaction throughput may become a bottleneck, and larger block sizes can strain the network's performance.
- **Scalability Solutions:** Solutions like sharding (dividing the network into smaller parts), sidechains (parallel chains), and layer-2 solutions (off-chain scaling) are employed to address these challenges and increase the network's capacity.

## Network Topology

- **Blockchain Network Topologies:** Different blockchains use various network topologies, such as fully connected (nodes connect to many peers), hierarchical (structured in layers), or mesh (every node connects to every other node). The choice of topology depends on network requirements.

## Incentive Mechanisms

**Mining Rewards:** Incentive mechanisms, like mining rewards or staking rewards, motivate participants to contribute resources or stake cryptocurrency to secure the network. This ensures that the network has a robust and active set of participants.

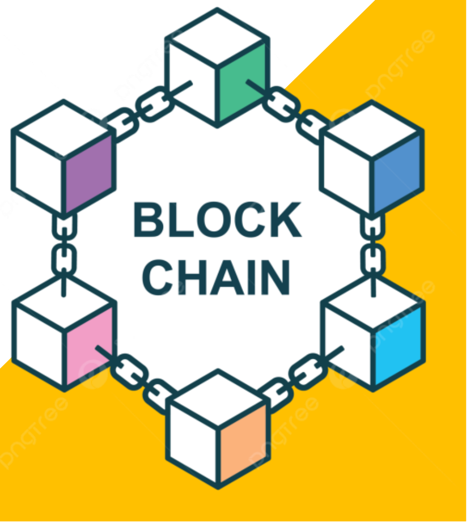
## Governance

- **Decentralized Governance:** Decentralized governance mechanisms, often involving token holders or validators, enable decision-making about protocol upgrades, parameter changes, and other network-related decisions. It ensures that governance power is distributed across the network.

## Immutable Ledger

- **Immutability in Blockchain:** Blockchain's immutability is achieved through cryptographic hashing. Each block contains a reference (hash) to the previous block, creating a secure and unchangeable chain of blocks. Once data is recorded on the blockchain, it becomes nearly impossible to alter or delete, ensuring data integrity and trust.

# Distributed Consensus

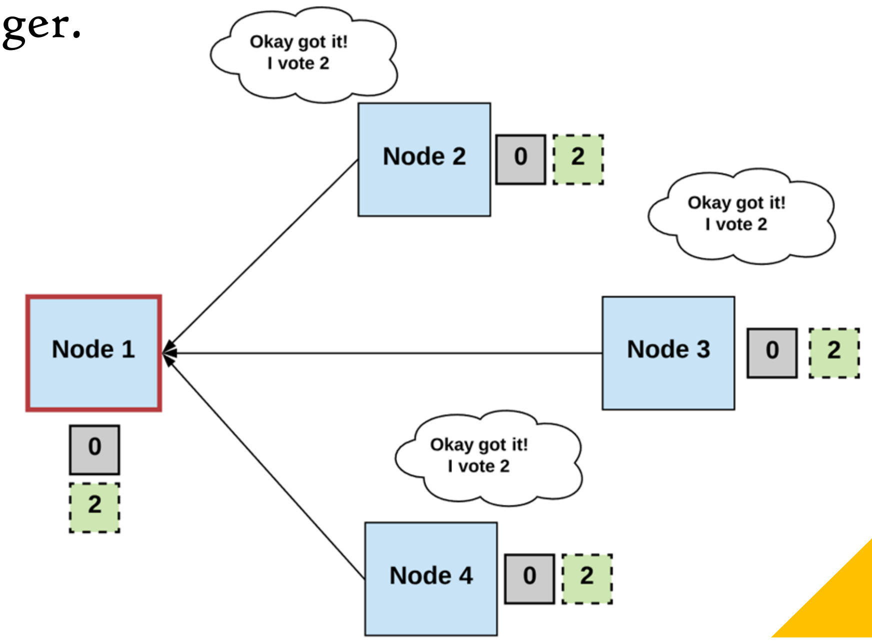


# Distributed Consensus

- Distributed consensus is a fundamental concept in blockchain technology, as it enables multiple nodes in a network to agree on the state of a shared ledger without the need for a central authority.

- Distributed consensus in blockchain refers to the process by which a network of decentralized nodes or participants in a blockchain system reaches an agreement on the validity and order of transactions or data in a trustless and decentralized manner.

- It is a fundamental aspect of blockchain technology and ensures that all nodes within the network maintain a consistent and tamper-proof ledger.



# Key Properties of Consensus Mechanisms

- **Decentralization:** Decentralization in consensus mechanisms means that no single entity or authority has control over the network. Instead, decisions are made collectively by a distributed set of nodes. Decentralization enhances trust because it eliminates the need to rely on a central authority.

- **Security:** Security is a fundamental property of consensus mechanisms. They should be designed to resist various attacks, including double-spending attacks, Sybil attacks, and 51% attacks. The security of a consensus mechanism ensures the trustworthiness of the blockchain network.

- **Immutability:** Immutability means that once a transaction is added to the blockchain, it becomes extremely difficult to alter or delete. This property is achieved through cryptographic techniques and consensus mechanisms, ensuring that historical data remains tamper-proof.

- **Scalability:** Scalability refers to the ability of a consensus mechanism and the underlying blockchain network to handle an increasing number of transactions and participants. Achieving scalability is essential for the widespread adoption of blockchain technology.

# Common Consensus Mechanisms

1. Proof of Work (PoW):
   - **Algorithm Details:** PoW requires miners to solve computationally intensive puzzles to validate transactions and create new blocks. The first miner to solve the puzzle gets the right to add the next block to the blockchain.

   - **Pros and Cons:** PoW is highly secure but consumes substantial computational power and energy, making it resource-intensive.

2. Proof of Stake (PoS):
   - **Validator Selection:** PoS relies on validators who are chosen to create blocks and validate transactions based on the number of cryptocurrency tokens they "stake" as collateral.

   - **Advantages:** PoS is energy-efficient compared to PoW and encourages validators to act honestly to protect their staked assets.

3. **Delegated Proof of Stake (DPoS):**
   - **Delegate System:** DPoS introduces a delegate system where a limited number of nodes are elected to validate transactions and produce blocks. These delegates take turns in block production.

   - **Speed vs. Decentralization:** DPoS offers faster transaction confirmation times but is criticized for potentially being more centralized due to the delegate selection process.

4. **Proof of Authority (PoA):**
   - **Trusted Validators:** PoA relies on a set of trusted validators or authorities who are responsible for validating transactions and maintaining the blockchain.

   - **Use Cases:** PoA is often used in private or consortium blockchains where trust among participants is established.

5. **Practical Byzantine Fault Tolerance (PBFT):**

- **Byzantine Fault Tolerance:** PBFT focuses on achieving consensus in a Byzantine fault-tolerant manner, even when a portion of nodes behaves maliciously.

- **Speed:** PBFT is known for its fast transaction confirmation times and is commonly used in permissioned blockchains.

# Choosing Right Consensus Mechanisms

- **Use Case Considerations:** The choice of consensus mechanism should align with the specific use case of the blockchain. Public, permissionless blockchains often lean toward PoW or PoS, while private blockchains may favour PoA.

- **Security vs. Scalability:** Depending on the project's requirements, developers must weigh the trade-offs between security and scalability. PoW prioritizes security but may be less scalable, while PoS aims for a balance.

- **Environmental Impact:** PoW's energy consumption has raised environmental concerns. PoS and PoA are considered greener alternatives with lower energy requirements.

- **Governance and Decision-Making:** The consensus mechanism can influence governance structures within a blockchain network, affecting decision-making processes and network upgrades.

# Hybrid Consensus Mechanisms

- Hybrid consensus mechanisms refer to a combination of two or more different consensus algorithms or approaches within a single blockchain network.

- These mechanisms are designed to leverage the strengths of each individual consensus method while mitigating their respective weaknesses. By doing so, hybrid consensus mechanisms aim to achieve a balance between various factors such as security, scalability, decentralization, and energy efficiency in blockchain systems.

Key points in the definition of hybrid consensus mechanisms include:

1. **Combination of Methods:** Hybrid consensus mechanisms integrate two or more consensus algorithms or strategies into the same blockchain network. This combination can involve both traditional and novel approaches to achieve agreement among network participants.

2. **Optimizing Strengths:** The goal of hybrid consensus is to optimize the strengths of each consensus method while minimizing their weaknesses. For example, it might combine the security of proof of work (PoW) with the energy efficiency of proof of stake (PoS).

3. **Tailored Solutions:** Hybrid consensus allows blockchain developers to tailor the consensus mechanism to the specific requirements of the network or use case. This adaptability makes it possible to address unique challenges and trade-offs in different blockchain applications.

4. **Enhancing Performance:** By using a combination of methods, hybrid consensus mechanisms can enhance the performance and scalability of blockchain networks, making them suitable for a broader range of applications and transaction volumes.

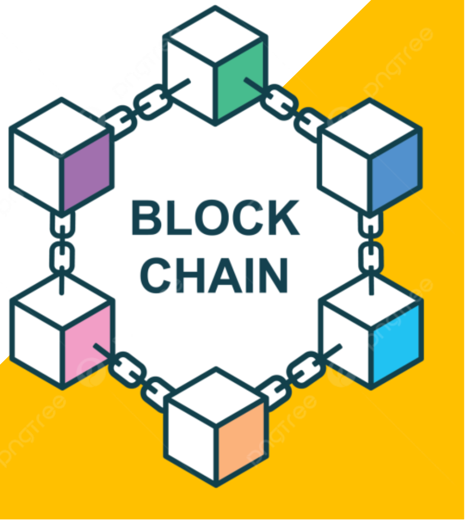
5. **Risk Mitigation:** It can reduce the risk associated with single-consensus mechanisms. For example, in a hybrid PoW/PoS system, if an attacker were to amass a significant amount of computational power (51% attack) to manipulate the blockchain, they would also need to control a significant stake of the network's cryptocurrency to succeed, which is typically more challenging to achieve.

6. **Consensus Switching:** Hybrid consensus mechanisms may allow the blockchain network to switch between different consensus methods dynamically or through governance decisions, adapting to changing network conditions or requirements.

7. **Examples:** Some examples of hybrid consensus mechanisms include Bitcoin's merge-mining (combining PoW with auxiliary PoW chains), Delegated Proof of Stake (DPoS) systems with additional consensus checks and various permissioned blockchain platforms that use a combination of consensus algorithms for different purposes.

Hybrid consensus mechanisms are particularly valuable in situations where no single consensus approach can address all the requirements or where a blockchain network needs to evolve over time. They provide flexibility and adaptability while aiming to strike a balance between the various trade-offs inherent in blockchain consensus algorithms.

# Assignment



# Unit Assignment

1. Explain the overview of blockchain in detail.
2. Explain the concept of the Double-Spend problem in detail.
3. Explain Byzantine General's Computing Problem with its solution of Byzantine Fault Tolerance.
4. What do you understand by Asymmetric Key Cryptography?
5. Explain hashing.
6. Write the difference between centralized, decentralized and distributed systems.
7. What is the consensus mechanism in blockchain?

Thank you

Any Queries