



ARYA College of Engineering (ACE)

(Affiliated to RTU | Approved by AICTE, New Delhi)

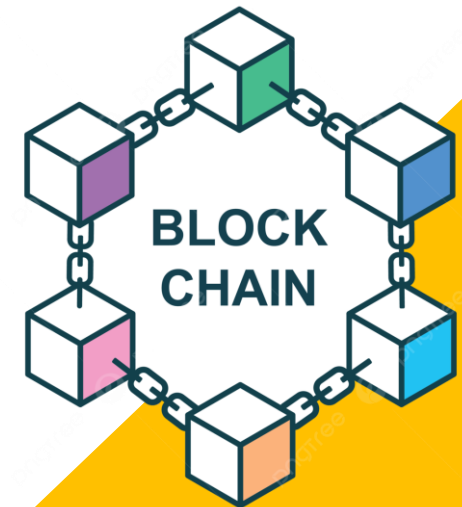
• SP-40, RIICO Industrial Area, Delhi Road,
Kukas, Jaipur-302028 | Tel. Ph. 0141-2820700

• www.aryainstitutejpr.com
• Toll Free: 1800 102 1044

Fundamentals of Blockchain

Unit-3 Ethereum Blockchain

Er. Harsh Raj
(Assistant Professor, CSE)

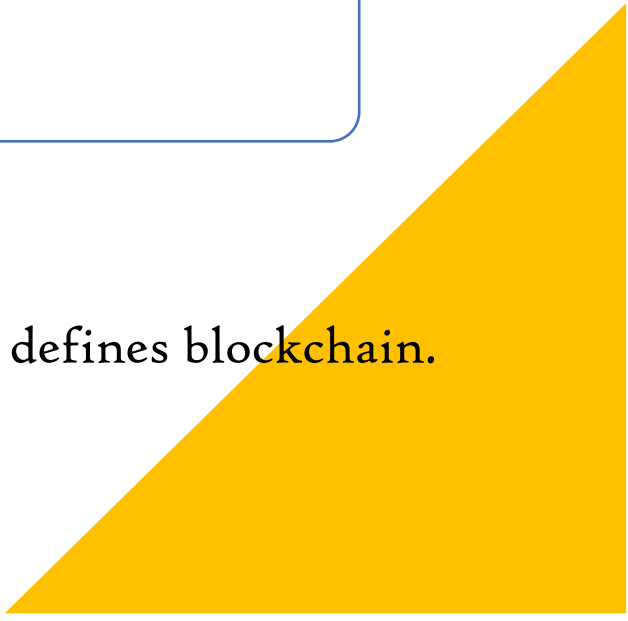




Course Objectives

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

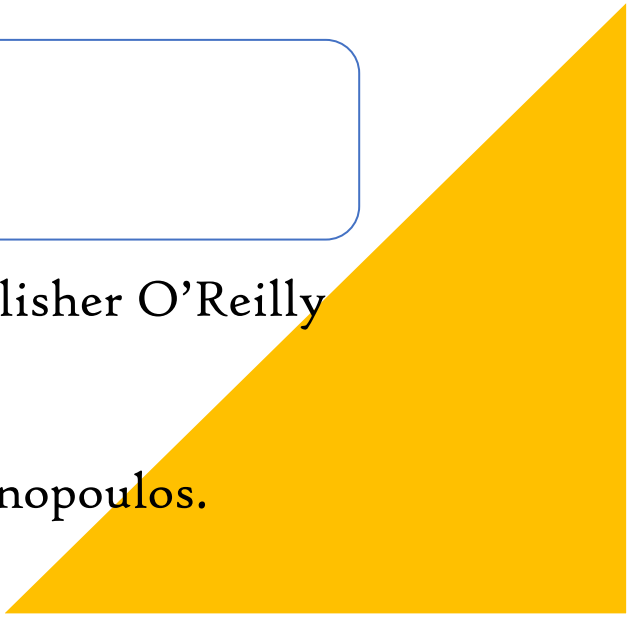
UNIT	Contents
1	Basics: The Double-Spend Problem, Byzantine Generals' Computing Problems, Public-Key Cryptography, Hashing, Distributed Systems, Distributed Consensus.
2	Technology Stack: Blockchain, Protocol, Currency. Bitcoin Blockchain: Structure, Operations, Features, Consensus Model, Incentive Model
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, Deposit-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

Ethereum Blockchain:

- Smart Contracts
 - Ethereum Structure
 - Operations
 - Features
 - Consensus Model
 - Incentive Model
- 

Smart Contracts



Smart Contracts


- A Smart Contract (or crypto-contract) is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions.
- A smart contract works in the same way as a traditional contract while also automatically enforcing the contract. Smart contracts are programs that execute exactly as they are set up(coded, programmed) by their creators.




Key Aspects Of Smart Contracts

1. **Code-Based:** Smart contracts are written in programming languages specifically designed for the blockchain, such as Solidity for Ethereum. These contracts contain instructions and logic that define their behaviour.
2. **Immutable:** Once deployed on a blockchain, smart contracts are immutable, meaning their code and rules cannot be altered or tampered with. This ensures trust and security in the contract's execution.
3. **Decentralized:** Smart contracts operate on decentralized blockchain networks, making them resistant to censorship and control by any single entity. This decentralization is a core feature of blockchain technology.
4. **Automated Execution:** Smart contracts automatically execute actions or transactions when predefined conditions are met. For example, a simple smart contract on Ethereum could release funds to a seller when a buyer confirms receipt of goods.
5. **Trustless:** Smart contracts eliminate the need for trust between parties because the contract's execution is enforced by the blockchain. Parties can trust the code and the blockchain network's consensus mechanism.

6. **Transparency:** Smart contracts are publicly visible on the blockchain, allowing anyone to inspect the code and track the contract's execution and transaction history. This transparency adds a layer of accountability.
7. **Cost-Efficiency:** By removing intermediaries and automating processes, smart contracts can reduce costs associated with traditional contract enforcement, such as legal fees and administrative overhead.
8. **Use Cases:** Smart contracts have a wide range of applications across various industries, including finance (DeFi platforms, lending, and trading), supply chain management, healthcare, real estate, gaming, and more.
9. **Gas Fees:** Executing smart contracts on blockchain networks often requires users to pay gas fees in the native cryptocurrency to compensate miners or validators for processing the contract. Gas fees are proportional to the computational complexity of the contract.
10. **Challenges:** Despite their advantages, smart contracts also face challenges, such as security vulnerabilities in code, scalability issues on some blockchain platforms, and legal recognition and enforcement in many jurisdictions.

- 
- ii. **Oracles:** Some smart contracts require external data to trigger their execution. Oracles are third-party services or mechanisms that provide this external data to smart contracts, bridging the gap between blockchain and real-world information.

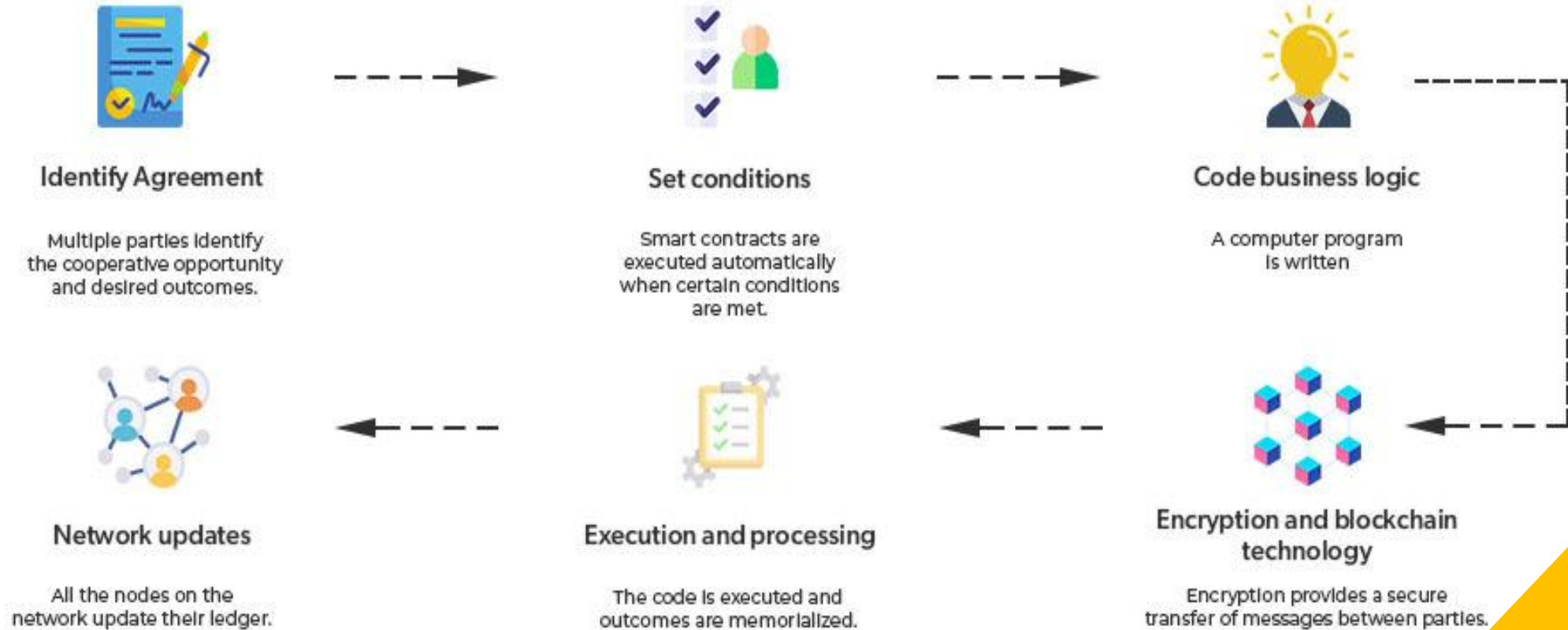
Smart contracts have gained significant attention and are a fundamental building block of blockchain-based decentralized applications (DApps). They have the potential to revolutionize industries by automating processes, reducing fraud, and increasing transparency and efficiency. However, developers must carefully consider security best practices when creating smart contracts to mitigate vulnerabilities and ensure their reliability.



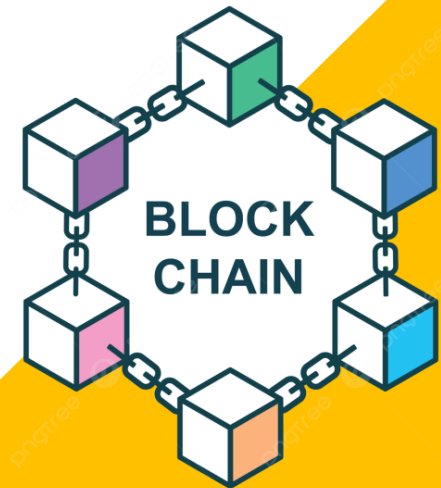
How Does A Smart Contracts Works?

- **Identify Agreement:** Multiple parties identify the cooperative opportunity and desired outcomes and agreements could include business processes, asset swaps, etc.
- **Set conditions:** Smart contracts could be initiated by the parties themselves or when certain conditions are met like financial market indices, events like GPS locations, etc.
- **Code business logic:** A computer program is written that will be executed automatically when the conditional parameters are met.
- **Encryption and blockchain technology:** Encryption provides secure authentication and transfer of messages between parties relating to smart contracts.
- **Execution and processing:** In blockchain iteration, whenever consensus is reached between the parties regarding authentication and verification then the code is executed and the outcomes are memorialized for compliance and verification.
- **Network updates:** After smart contracts are executed, all the nodes on the network update their ledger to reflect the new state. Once the record is posted and verified on the blockchain network, it cannot be modified, it is in append mode only.

How does a Smart Contract Work?



Ethereum



Ethereum



Ethereum is a blockchain network that introduced a built-in Turing-complete programming language that can be used for creating various decentralized applications(also called Dapps).

The Ethereum network is fueled by its own cryptocurrency called ‘ether’.

- The Ethereum network is currently famous for allowing the implementation of smart contracts. Smart contracts can be thought of as ‘cryptographic bank lockers’ which contain certain values.
- These cryptographic lockers can only be unlocked when certain conditions are met.
- Unlike bitcoin, Ethereum is a network that can be applied to various other sectors.
- Ethereum is often called Blockchain 2.0 since it proved the potential of blockchain technology beyond the financial sector.
- The consensus mechanism used in Ethereum is Proof of Stake(PoS) which is more energy efficient when compared to that used in the Bitcoin network, that is, Proof of Work(PoW) PoS depends on the amount of stake a node holds.

History Of Ethereum

- **2013:** Ethereum was first described in Vitalik Buterin's white paper in 2013 with the goal of developing decentralized applications.
- **2014:** In 2014, EVM was specified in a paper by Gavin Wood, and the formal development of the software also began.
- **2015:** In 2015, Ethereum created its genesis block marking the official launch of the platform.
- **2018:** In 2018, Ethereum took second place in Bitcoin in terms of market capitalization.
- **2021:** In 2021, a major network upgrade named London included Ethereum improvement proposal 1559 and introduced a mechanism for reducing transaction fee volatility.
- **2022:** In 2022, Ethereum has shifted from PoW(Proof-of-Work) to PoS(Proof-of-State) consensus mechanism, which is also known as Ethereum Merge. It has reduced Ethereum's energy consumption by ~ 99.95%.

Features Of Ethereum

1. **Smart Contracts:** Ethereum allows the creation and deployment of smart contracts. Smart contracts are created mainly using a programming language called solidity. Solidity is an Object Oriented Programming language that is comparatively easy to learn.
2. **Ethereum Virtual Machine (EVM):** It is designed to operate as a runtime environment for compiling and deploying Ethereum-based smart contracts.
3. **Ether:** Ether is the cryptocurrency of the Ethereum network. It is the only acceptable form of payment for transaction fees on the Ethereum network.
4. **Decentralization Applications (Dapps):** Dapps has its backend code running on a decentralized peer-to-peer network. It can have a frontend and user interface written in any language to make calls and query data from its backend. They operate on Ethereum and perform the same function irrespective of the environment in which they get executed.
5. **Decentralization Autonomous Organization (DAO):** It is a decentralized organization that works in a democratic and decentralized fashion. DAO relies on smart contracts for decision-making or decentralized voting systems within the organization.

Type Of Ethereum Accounts

Ethereum has two types of accounts: An externally owned account (EOA), and a Contract account.

These are explained as following below:

- **Externally owned account (EOA):** Externally owned accounts are controlled by private keys. Each EOA has a public-private key pair. The users can send messages by creating and signing transactions.
- **Contract Account:** Contract accounts are controlled by contract codes. These codes are stored with the account. Each contract account has an ether balance associated with it. The contract code of these accounts gets activated every time a transaction from an EOA or a message from another contract is received by it. When the contract code activates, it allows to read/write the message to the local storage, send messages and create contracts.



How does Ethereum Work?

Ethereum implements an execution environment called Ethereum Virtual Machine (EVM).

- When a transaction triggers a smart contract all the nodes of the network will execute every instruction.
- All the nodes will run The EVM as part of the block verification, where the nodes will go through the transactions listed in the block and run the code as triggered by the transaction in the EVM.
- All the nodes on the network must perform the same calculations to keep their ledgers in sync.
- Every transaction must include:
 - Gas limit.
 - Transaction Fee that the sender is willing to pay for the transaction.
- If the total amount of gas needed to process the transaction is less than or equal to the gas limit then the transaction will be processed and if the total amount of gas needed is more than the gas limit then the transaction will not be processed the fees are still lost.
- Thus it is safe to send transactions with the gas limit above the estimate to increase the chances of getting it processed.

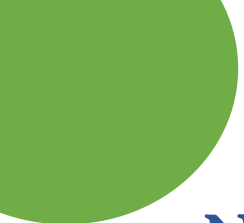

Real World Application Of Ethereum

- **Voting:** Voting systems are adopting Ethereum. The results of polls are available publicly, ensuring a transparent fair system thus eliminating voting malpractices.
- **Agreements:** With Ethereum smart contracts, agreements and contracts can be maintained and executed without any alteration. Ethereum can be used for creating smart contracts and for digitally recording transactions based on them.
- **Banking systems:** Due to the decentralized nature of the Ethereum blockchain it becomes challenging for hackers to gain unauthorized access to the network. It also makes payments on the Ethereum network secure, so banks are using Ethereum as a channel for making payments.
- **Shipping:** Ethereum provides a tracking framework that helps with the tracking of cargo and prevents goods from being misplaced.

- 
- **Crowdfunding:** Applying Ethereum smart contracts to blockchain-based crowdfunding platforms helps to increase trust and information symmetry. It creates many possibilities for startups to raise funds to create their own digital cryptocurrency.
 - **Domain names:** Ethereum name service allows crypto users to buy and manage their own domain names on Ethereum, thus simplifying decentralized transactions without requiring users to remember long, machine-readable addresses.
- 

Benefits Of Ethereum

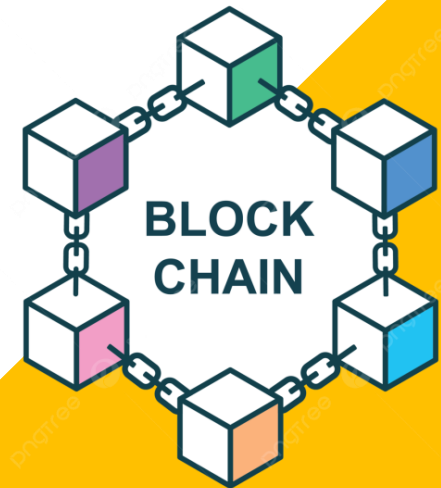
- **Availability:** As the Ethereum network is decentralized so there is no downtime. Even if one node goes down other computing nodes are available.
- **Privacy:** Users don't need to enter their personal credentials while using the network for exchanges, thus allowing them to remain anonymous.
- **Security:** Ethereum is designed to be unhackable, as the hackers have to get control of the majority of the network nodes to exploit the network.
- **Less ambiguity:** The smart contracts that are used as a basis for trade and agreement on Ethereum ensure stronger contracts that differ from the normal traditional contracts which require follow-through and interpretation.
- **Rapid deployment:** On Ethereum decentralized networks, enterprises can easily deploy and manage private blockchain networks instead of coding blockchain implementation from scratch.

- 
- **Network size:** The Ethereum network can work with hundreds of nodes and millions of users.
 - **Data coordination:** Ethereum's decentralized architecture better allocates information so that the network participants don't have to rely on a central entity to manage the system and mediate transactions.
- 

Drawbacks Of Ethereum

- **Complicated programming language:** Learning solidity from programming smart contracts on Ethereum can be challenging and one of the main concerns is the scarcity of beginner-friendly classes.
- **Volatile cryptocurrency:** Ethereum investing can be risky as the price of Ether is very volatile, resulting in significant gains as well as a significant loss.
- **Low transaction rate:** Bitcoin has an average transaction rate of 7TPS and Ethereum has an average speed of 15 TPS which is almost double that of bitcoin but it is still not enough.

Bitcoin Vs Ethereum



Bitcoin Vs Ethereum



Bitcoin

Bitcoin is a digital currency that can be transferred on a peer-to-peer (P2P) network without the need for any central authority.

It was invented by a person or group of people with the name Satoshi Nakamoto in 2008.

All the transactions are stored in an immutable distributed ledger.

- Bitcoin is created, stored, transacted, and distributed using a decentralized system known as Blockchain.
- A public ledger records all the transactions of the Bitcoin and copies are retained on all the servers around the world.
- It is not necessary to buy an entire bitcoin, one can buy only a fraction of it if that is all necessary.

Ethereum



Ethereum is a blockchain-based distributed platform.

The network currency of Ethereum is known as Ether (ETH).

Here also, the transactions are stored in an immutable distributed ledger.

- Ethereum is designed to be scalable, decentralized, and programmable.
- It provides a flexible platform to build applications using the solidity scripting language.
- Transactions are sent and received in user-created Ethereum accounts.
- It is a blockchain-based platform With the cryptocurrency Ether(ETH).

Bitcoin Vs Ethereum

- Bitcoin and Ethereum have many similarities but there are some long-term different visions and limitations that make them two different blockchain networks that have their pros and cons and are suitable for varying user requirements.



Bitcoin
(BTC)

vs



Ethereum
(ETH)

Difference

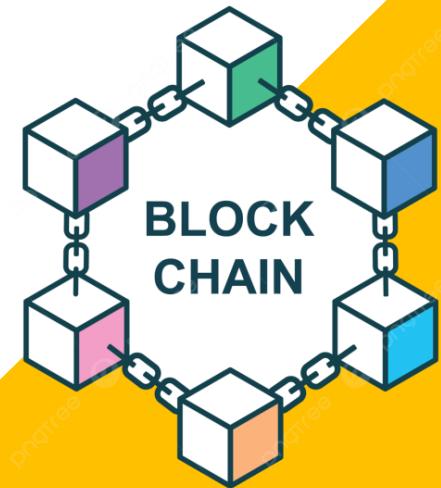
Basis	Bitcoin	Ethereum
Definition	Bitcoin (abbreviation: BTC; sign: ₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
History	The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.	Ethereum was conceived in 2013 by programmer Vitalik Buterin, and then went live on 30 July 2015.
Purpose	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.

Smart Contracts	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that a programming language would give them.	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.
Smart Contract Programming Language	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
Transactions	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.
Hash Algorithm	Bitcoin runs on the SHA-256 hash algorithm.	Ethereum runs on the Keccak-256 hash algorithm.
Consensus Mechanism	The Proof-of-Work (PoW) is the consensus mechanism used by the Bitcoin network.	The Proof-of-Stake is the consensus mechanism used by Ethereum.



	bitcoin	ethereum
concept	digital money	smart contracts
transaction	send from alice to bob	send from alice to bob if.. <ul style="list-style-type: none">• date = jan 1, 2018• bob's balance < 10 eth
market cap	~\$18 billion	~\$1 billion
founder	satoshi nakamoto (unknown)	vitalik buterin and team
release date	jan 2009	july 2015
release method	early mining	presale raised \$18M in bitcoin

Assignment



Unit Assignment

1. What do you understand by Ethereum?
2. Explain the difference between Bitcoin and Ethereum in blockchain.
3. Explain smart contracts in detail.
4. What is Ethereum structure? Explain with diagrams.
5. Explain core components of Ethereum blockchain operation.
6. What are the features of Ethereum? Explain each point.
7. Explain consensus model in Ethereum and their importance with evolution.
8. What do understand by incentive model in Ethereum blockchain? How does it work?

Thank you

Any
Queries

