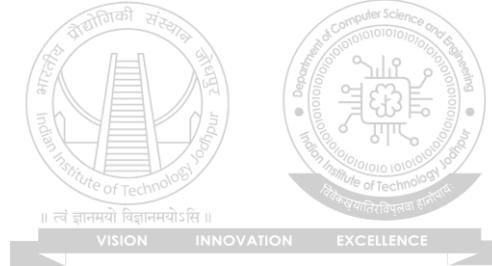


Problems and Solutions

Department of Computer Science and Engineering

Indian Institute of Technology, Jodhpur



What Are the Real-World Use Cases of Ethereum?

- **Answer:** There are many use cases of Ethereum. Some of them are as below.
- **Decentralized Finance:** One of the biggest use-cases is [decentralized finance](#) (De-Fi). It improves how the [financial sector](#) works and improves loans using smart contracts.
- **Digital Identity:** [Digital Identity](#) is another use-case where a person's identity is digitized, providing better usability for individuals as they do not have to carry documents and can be verified instantly through a connected network.
- **Health applications:** [Blockchain for healthcare](#) systems can utilize Ethereum based solutions to implement a decentralized network and improve things such as drug tracking, better patient management, and so on.
- **Supply Chain:** Ethereum is very useful in creating the [tokenization](#) of real-world assets. This makes it easy to trade items on the [Blockchain for supply chain](#) management solution.
- **Payments:** It also improves payments, especially cross-boundary transactions. Therefore, it's perfectly suited for any [blockchain in payment](#) solutions.

What Is Dapps?

- **Answer:** dApp stands for decentralized application. These applications are created to take advantage of blockchain technologies. dApps offer many benefits, including being decentralized and open source. It also follows protocols and incentivizes nodes that take part in the functioning of the dApp.
- Ethereum is a popular blockchain network for dApps as it offers the right ecosystem for developers to create real-world dApps.

What programming language is best for creating smart contracts and decentralized applications?

- **Solidity** is widely in use for writing smart contracts and decentralized applications (dApps) as the preferred programming language.
- (If you want to become a smart contract developer then Solidity is a must language to learn).

What Is the Programming Language Used to Write Smart Contracts and Dapps?

- Solidity is the main programming language that is used to create both dApps and smart contracts. However, smart contracts in Ethereum can also be written using any of the smart-contract languages (SCL). Some of the SCL examples include Vyper, Bamboo, Serpent, Ethereum bytecode, Pyramid, L4, and others.

What is the best way to get Ethers?

- There are two methods: by mining them or by exchanging them for other digital coins.

Considerations for Blockchain Adoption and Integration

- Considerations for Blockchain Adoption and Integration
- Some attributes of blockchain technology adding value to an organization as a technology-based system include decentralization, synchronization, traceable, immutability, security, scalability, auditability, and programmability. These attributes also mean that an organization must make special considerations during the implementation phase.

How is Blockchain distributed ledger different from a traditional ledger?

- A Blockchain distributed ledger is **highly transparent** as compared to a traditional ledger.
- Blockchain distributed ledgers are **irreversible**. Information registered on a distributed ledger cannot be modified whereas on a traditional ledger it is reversible.
- A distributed ledger is **more secure**. It **uses cryptography and every transaction is hashed and recorded** whereas in traditional ledger security can be **compromised**.
- In a distributed ledger, there is **no central authority**. It is a distributed system and the participants hold the authority to maintain the sanity of the network and are responsible for validating the transactions. Traditional ledgers are based on the concept of centralized control, which controls all transactions.
- In a distributed ledger, **identities are unknown and hidden** whereas in traditional ledger **identities of all participants have to be known before the transactions happen**.
- In a distributed ledger, **data modification or change cannot be done** but for a traditional ledger, it is possible.
- In a distributed ledger, **validation is done by the participants in the network while in a traditional ledger, validation is done by a centralized authority**.
- The copy of the ledger is **shared amongst participants in a distributed ledger while in a traditional ledger, a single copy is maintained in a centralized location**. It is not shared amongst the participants.

How is the hash (Block signature) generated?

- The process of generating a block signature involves:
- Passing transaction details through a one-way hash function i.e., SHA-256.
- Running the output value through a signature algorithm (like ECDSA) with the user's private key.
- Following these steps, the encrypted hash, along with other information (such as the hashing algorithm), is called the digital signature.

List down some of the extensively used cryptographic algorithms.

- Here are a few popular algorithms:
- SHA - 256
- RSA (Rivest-Shamir-Adleman)
- Triple DES
- Ethash
- Blowfish

What is a smart contract and list some of its applications?

- Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers
- Some of the applications are:
- **Transportations:** Shipment of goods can be easily tracked using smart contracts
- **Protecting copyrighted content:** Smart contracts can protect ownership rights such as music or books
- **Insurance:** Smart contracts can identify false claims and prevent forgeries
- **Employment contract:** Smart contracts can be helpful to facilitate wage payments

What is the Ethereum network and how many Ethereum networks are you familiar with?

- Ethereum is a blockchain-based distributed computing platform featuring smart contract functionality that enables users to create and deploy their decentralized applications
- There are three types of networks in Ethereum:
- **Live network (main network)** - Smart contracts are deployed on the main network
- **Test network** (like Ropsten, Kovan, Rinkeby) - Allow users to run their smart contracts with no fees before deploying it on the main network
- **Private network** - Are those which are not connected to the main network. They run within the premises of the organization but carry the features of an Ethereum network.

Where do nodes run a smart contract code?

- Nodes run smart contracts code on Ethereum Virtual Machine (EVM). It is a virtual machine designed to operate as a runtime environment for [Ethereum](#)-based smart contracts.
- EVM is operated in a sandboxed environment (isolated from the main network). This is a perfect testing environment.
- You can download the EVM, run your smart contract locally in an isolated manner and once you have tested and verified it, you can deploy it on the main network.

What is a Dapp and how is it different from a normal application?

- **Dapp:**
 - A Dapp is a decentralized application which is deployed using smart contract
 - A Dapp has its back-end code (smart contract) which runs on a decentralized peer-to-peer network
- **Process:**
 - Front-end
 - Smart contract (backend code)
 - Blockchain (P2P contract)
- **Normal application:**
 - Normal application has a back-end code which runs on a centralized server
 - It's a computer software application that is hosted on a central server
- **Process:**
 - Front-end
 - API
 - Database (runs on the server)

What is the difference between Bitcoin and Ethereum?

Criteria	Bitcoin	Ethereum
Concept	P2P currency	P2P currency and smart contract
Consensus mechanism	Proof of work	Proof of work/ Proof of stake
Hashing Algorithm	SHA-256	Ethash
Time is taken to mine a block	10 Minutes (approx.)	12-15 seconds
Reward	12.5 BTC	3 ETH
Transaction fee	Optional	A fee is calculated in <i>gas</i>
Value (8/21/18)	1 BTC = 6934.34 USD	1 ETH = 278.98 USD

THANK

YOU