Introduction to Blockchain Technologies

Unit 4

Distributed Ledgers for Business

Ethereum: Introduction – Ethereum Network – Components – Programing Languages; Hyperledger: Introduction – Reference Architecture – Fabric – Sawtooth Lake – Corda

Ethereum

1. **What**
    - A blockchain platform, similar to Bitcoin
    - Major difference: Ethereum is programmable
    - Ethereum can execute code- smart contracts- automatically when certain conditions are met.
    - Launched in 2015 by Vitalik Buterin
    - Meant to be a platform where developers can build and run applications that don't need a central authority

2. **Rationale behind the creation of Ethereum**
    - Create a decentralized world where users have control over their data and applications run on a blockchain rather than on centralized servers.
    - Ethereum was designed to be a platform for decentralized applications or dApps, that could do everything from managing financial transactions to creating new forms of digital ownership.

3. **How Ethereum Works**

    - Ethereum runs on its own blockchain, a decentralized ledger that records all transactions and smart contract executions.
    - Ethereum relies on a network of nodes- computers running the Ethereum software, to validate and record everything that happen on the network

    Smart Contracts

    - Ethereum has self-executing contracts with the terms of the agreement written directly into the code.

- Once the conditions are met, the contract automatically carries out the agreement with no human intervention.
- Smart contracts are the building blocks of decentralized applications, or dApps.

Ethereum Virtual Machine (EVM)

- Engine that drives the working of the Ethereum software across computers.
- It is a Turing-complete virtual machine that runs smart contracts that ensures they execute the same way on every node of the network.
- This helps developers write and deploy code such that it is consistent, reliable and secure.

4. Importance of Ethereum

Ethereum takes the idea of blockchain and turned it into a platform for innovation-serves as the foundation for decentralized finance, digital art and other applications.

a. Decentralized Finance (DeFi)
   - DeFi uses smart contracts to recreate traditional financial systems like lending, borrowing, and trading without the need for banks or other intermediaries.

b. Non-Fungible Tokens (NFTs)
   - NFTs are unique digital assets that represent ownership of a specific item or piece of content like art, music or virtual real estate.
   - Ethereum's smart contracts make it possible to buy, sell, and trade these assets in a decentralized, transparent way.

5. Upgrading to Ethereum 2.0
   - Aims to improve scalability, sustainability and security
   - Will shift from Proof of Work to Proof of Stake, which will reduce the network's energy consumption and increase its efficiency.

Ethereum Network

1. What
- A Decentralized, global infrastructure that supports the creation and execution of smart contracts and decentralized applications.
- It is not just a ledger of transactions, it is a world computer that anyone can use to build and run applications that operate without a central authority.

- The Ethereum network is being used to create digital art, launching new financial systems, other applications etc.
- The core of the Ethereum Network is the blockchain framework- but unlike Bitcoin, which primarily tracks the movement of its native currency, Ethereum's blockchain is designed to handle a wide range of complex operations.
- This is what makes Ethereum not just a currency, but a platform.

2. Working of the Ethereum Network

- Operates on a system of nodes running Ethereum software.
- Nodes validate transactions, execute smart contracts, and add new blocks to the blockchain.
- Relies on several key components beyond just data processing.

Smart Contracts and Decentralized Applications (dApps)

- Smart contracts are self-executing agreements with no intermediaries.
- They enable the creation of dApps on the Ethereum Network.
- Smart contracts power decentralized finance (DeFi) and non-fungible tokens (NFTs).
- dApps run on the blockchain, providing transparency, security, and censorship resistance.

Proof of Work (and the Shift to Proof of Stake)

- Currently uses Proof of Work (PoW), where miners solve puzzles to add blocks.
- PoW is energy-intensive, prompting a shift to Proof of Stake (PoS).
- Ethereum 2.0 will transition to PoS, where validators are chosen based on staked cryptocurrency.
- PoS will reduce energy consumption, increase scalability, and make Ethereum more sustainable.

The Ethereum Virtual Machine (EVM)

- The EVM is the engine of the Ethereum Network, processing smart contracts.
- It allows developers to write and deploy code in various programming languages.
- Ensures consistent execution of code across the network.
- Transforms Ethereum from a ledger into a decentralized world computer.

3. Power of the Ethereum Network

- Ethereum is a catalyst for innovation, not just infrastructure.
- It drives exciting developments in blockchain technology.
- The platform of choice for building decentralized systems.

Decentralized Finance (DeFi)

- DeFi uses smart contracts to replicate traditional financial services (e.g., lending, borrowing, trading).
- Eliminates the need for banks or intermediaries.
- Offers new financial opportunities, especially for those underserved by traditional banking.

Non-Fungible Tokens (NFTs)

- Ethereum is the birthplace of NFTs, unique digital assets representing ownership of specific items or content.
- NFTs have gained massive popularity among artists, creators, and collectors.
- Ethereum is the primary platform for minting and trading these digital goods.

4. **Scalability of Ethereum**
    - Scalability is a major challenge as the Ethereum Network grows.
    - High transaction volume sometimes causes network congestion.
    - **Ethereum 2.0** aims to improve capacity and speed.
    - Transition to **Proof of Stake (PoS)** for more efficient block validation.
    - Introduction of **sharding** to allow parallel processing of transactions.

Proof of Stake (PoS):

- In PoS, validators are selected to create new blocks based on the amount of cryptocurrency they "stake" as collateral.
- PoS consumes less energy than Proof of Work (PoW), improving the network's sustainability.
- Validators are rewarded for securing the network, and penalties are imposed for malicious behavior.

Sharding:

- Sharding splits the Ethereum network into smaller partitions (shards) to process transactions in parallel, increasing scalability.
- Each shard handles its own transactions and smart contracts, reducing the load on the entire network.
- It allows Ethereum to process many more transactions simultaneously, addressing scalability issues.

Components of Ethereum

a. The Ethereum Blockchain

- A decentralized, public ledger that does more than just track ownership (unlike Bitcoin's blockchain).
- Supports smart contracts and dApps, providing the foundation for Ethereum's ecosystem.
- Maintained by a network of nodes, each with a copy of the blockchain, ensuring security and transparency.

b. Ether (ETH)

- The native cryptocurrency of the Ethereum network.
- Used to power transactions, run smart contracts, and pay transaction fees (known as "gas").
- Demand for Ether increases as more people use the network for various decentralized applications.

c. Smart Contracts

- Self-executing contracts where the terms are written into code and executed without intermediaries.
- Once conditions are met, the contract automatically enforces itself, reducing the need for human involvement.
- Enables the automation of tasks in DeFi and NFTs, reducing costs and enhancing efficiency.

d. The Ethereum Virtual Machine (EVM)

- The EVM is the engine that runs smart contracts and dApps across the Ethereum network.
- It ensures that smart contracts execute consistently and securely, regardless of the programming language used.
- Makes Ethereum a decentralized, global computing platform.

e. Decentralized Applications (dApps)

- Applications that run on the Ethereum blockchain, free from centralized control.
- dApps are more secure, transparent, and resistant to censorship than traditional apps.
- Used in areas such as finance, social media, gaming, and decentralized organizations (DAOs).

f. Gas and Transaction Fees

- Gas is the fee paid in Ether to run operations like transactions or smart contracts.
- Simple transactions cost less gas, while complex operations (like running smart contracts) require more.
- Gas fees fluctuate depending on network demand and the complexity of the operation.

g. **Nodes and Mining**

- Nodes are the backbone of Ethereum, validating transactions and maintaining the blockchain.
- There are two types of nodes: full nodes, which store the entire blockchain, and light nodes, which store only essential data.
- Miners are responsible for processing transactions and securing the network through Proof of Work (soon transitioning to Proof of Stake with Ethereum 2.0).

Ethereum Programming Languages

a. **Solidity**:

- The most popular language for writing smart contracts on Ethereum.
- Similar to JavaScript, it's flexible, powerful, and relatively easy to learn.
- Compiles to Ethereum Virtual Machine (EVM) bytecode and is widely used for DeFi, NFTs, and dApps.

Why Solidity Matters:

- Includes important features like event logging, inheritance, and libraries designed for decentralized environments.
- Solidity's reliability and security are crucial for writing error-free, robust blockchain code.

b. **Vyper**:

- A simplified, stripped-down alternative to Solidity, focusing on security and readability.
- Avoids risky features like inheritance and function overloading to reduce audit complexity and errors.
- Well-suited for high-stakes financial contracts requiring bulletproof security.

Why Vyper Matters:

- Popular for developers prioritizing simplicity, clarity, and secure code.
- A compelling choice for users needing straightforward and safe smart contracts.

c. **Yul and Yul+**:

- Intermediate-level, low-level languages optimized for smart contract development.

- Yul is simpler and can be used as a target for Solidity and Vyper, while Yul+ adds more features for control.
- Best for developers focusing on performance and contract optimization.

  Why Yul and Yul+ Matter:

  - Provide granular control over the EVM for writing highly optimized code.
  - Ideal for developers looking to maximize performance in their contracts.

d. **LLL (Low-Level Lisp-like Language)**:

- Minimalist, assembly-like language offering maximum control over contract execution.
- Difficult to learn but provides unparalleled precision for developers comfortable with low-level programming.

  Why LLL Matters:

  - Allows for highly optimized, low-level code, perfect for those who need exact control over contract behavior.
  - Not widely used but extremely powerful in the right hands.

Hyperledger

1. **What**

- Hyperledger is a collaborative, open-source project, not a blockchain itself.
- Provides frameworks, tools, and libraries for enterprise-level blockchain development.
- Launched by the Linux Foundation in 2015 to support cross-industry blockchain technologies.

  Key Features:

  - Designed for private, permissioned networks, unlike public blockchains like Bitcoin and Ethereum.
  - Only authorized participants can interact with the network, making it ideal for businesses focused on privacy, compliance, and data control.
  - **Interoperability and Flexibility** – Has a large number of frameworks and tools to choose from, and business can tailor their blockchain solutions to their specific needs. Hyperledger is designed for interoperability, it can integrate with existing systems and other blockchain networks, making it a future proof solution.

2. Motivation behind Hyperledger

- Hyperledger aims to extend blockchain technology beyond cryptocurrencies to revolutionize business operations.
- Focuses on meeting business needs such as scalability, security, and interoperability.

For Collaboration and Flexibility:

- Hyperledger is a community-driven project offering customizable tools and frameworks for various industries.
- Designed to serve diverse sectors such as supply chain management, finance, healthcare, and government.
- Positioned to be the backbone of the new digital economy.

3. Key Components of Hyperledger

a. Hyperledger Fabric:

- Flagship framework of Hyperledger, designed for modular, plug-and-play components.
- Allows businesses to create private, permissioned blockchains with control over access and network actions.
- Powers enterprise blockchain solutions, from financial transactions to supply chain tracking.

b. Hyperledger Sawtooth:

- Flexible framework for building and running distributed ledgers with customizable consensus mechanisms.
- Separates the core system from the application layer, making it adaptable to various use cases.

c. Hyperledger Indy:

- Focuses on decentralized identity management, allowing businesses to create and manage secure, private, portable digital identities.
- Useful for industries requiring identity verification, like finance and healthcare.

d. Hyperledger Besu:

- Ethereum client designed for enterprise use, supporting both public and private networks.
- Offers flexibility to operate on Ethereum's mainnet or a private network, bridging public and enterprise blockchain solutions.

e. Hyperledger Caliper & Hyperledger Explorer:

- **Caliper**: A benchmarking tool to measure the performance of blockchain implementations.

    - **Explorer**: A web application for viewing, managing, and interacting with blockchain networks, helping enterprises optimize their blockchain solutions.

4. **Usage of Hyperledgers in Business**
    - IBM, Walmart
    - Tracking goods through supply chain, automating complex financial transactions, ensuring data integrity in healthcare.

Reference Architecture: Fabric, Sawtooth Lake, and Corda

1. **Hyperledger Fabric: The Swiss Army Knife**

- **Overview**: Hyperledger Fabric is a versatile and modular blockchain platform that provides flexibility and control, designed for businesses that want private, permissioned blockchains.

  Architecture Snapshot:

    - **Channels**: These are like private rooms where specific participants can conduct transactions without broadcasting the details to everyone, ensuring privacy.
    - **Smart Contracts (Chaincode)**: Smart contracts, known as chaincode in Fabric, are where the business logic resides. They can be written in popular programming languages like Go, Java, and JavaScript, making it easy for developers to build on the platform.
    - **Ordering Service**: Fabric's transaction coordinator. It ensures transactions are ordered and batched before they are added to the blockchain, keeping the ledger consistent and synchronized.
    - **Endorsement Policies**: These policies define who needs to approve or validate transactions before they are finalized. This ensures that no transaction gets added without the required approvals, enhancing security.

  Why Fabric Matters:

    - **Flexibility**: Fabric's modular architecture allows businesses to pick and choose components that fit their needs, ensuring scalability, security, and control.
    - **Enterprise Focus**: Perfect for businesses needing a robust, scalable platform to handle complex business processes, making it ideal for various industries like finance, healthcare, and supply chain management.

2. **Hyperledger Sawtooth Lake: The Agile Innovator**

- **Overview**: Sawtooth Lake is a highly flexible blockchain platform designed for innovation. It supports a variety of consensus algorithms and integrates smoothly with existing business systems.

Architecture Snapshot:

- **Consensus Mechanisms**: Sawtooth Lake allows flexibility in choosing from multiple consensus algorithms, including PoET (Proof of Elapsed Time), Raft, and PBFT (Practical Byzantine Fault Tolerance). This allows businesses to pick the best mechanism based on their needs (speed, security, fault tolerance).
- **Transaction Families**: Sawtooth handles business logic through modular **transaction families**, which define the rules for transactions. Businesses can create custom transaction families or use pre-existing ones, giving them control over how transactions are handled.
- **Validator Network**: Validators ensure the blockchain's integrity. Whether the network is public or private, businesses can configure validators based on their specific requirements.
- **Event System**: The event system allows applications to subscribe to blockchain events and receive real-time updates, making it ideal for applications that need to respond to changes quickly.

Why Sawtooth Lake Matters:

- **Flexibility**: Sawtooth Lake is ideal for businesses needing a blockchain platform that adapts to evolving needs. It is highly flexible, innovative, and designed for organizations that want control over consensus and transaction rules.
- **Innovation**: Sawtooth is perfect for organizations that value experimentation and quick adaptation.

3. Corda: The Finance Specialist

- **Overview**: Corda is a blockchain platform specifically designed for the financial industry, focusing on privacy, scalability, and ensuring transactions are legally enforceable. It was developed by R3, a consortium of over 200 financial institutions.

  Architecture Snapshot:

  - **State Objects**: The ledger in Corda is built from state objects, which represent the current state of assets or contracts. These objects are immutable, meaning once set, they can only be updated by creating a new version. This provides a clear, auditable transaction history.
  - **Notary Services**: Corda uses notary services to prevent double-spending and ensure transactions are unique. Notaries are trusted nodes that validate transactions, ensuring they aren’t duplicated on the network.
  - **Flows**: Flows automate the entire transaction process, from creation to validation and finalization. They are customizable, enabling businesses to streamline complex processes such as trade settlements and loan issuance.
  - **Legal Prose and Smart Contracts**: Corda integrates legal prose with smart contracts, ensuring that digital agreements are legally enforceable. This bridges the gap between blockchain and traditional legal frameworks, making Corda suitable for regulatory environments.

Why Corda Matters:

- Corda is ideal for the financial industry due to its focus on privacy, compliance, and legal enforceability.
- It is the platform of choice for banks and other financial institutions looking to use blockchain technology while adhering to legal standards and regulations.