UNIT IV

ETHEREUM AND SMART CONTRACTS

Basics of Ethereum

- The Bitcoin network solved the double-spend problem, making it possible to transact online with much greater certainty, but was fundamentally only designed to transact the crypto-currency bitcoin. It is not really a network architecture that supports diverse applications.
- Ethereum, by contrast, is designed to support more complex financial and programmable transactions. It too makes use of a digital token – called “ether” (ETH) – for processing transactions, but can also store and execute programs. Ethereum has grown to be the second largest digital token by market capitalization. More importantly, it has the largest community of developers.
- The main attraction of Ethereum is that it allows developers to create and deploy decentralized applications (Dapps) on its platform.
- Code that is programmed to execute using the Ethereum network is written and stored in the form of smart contracts. Ethereum is flexible enough that transactions can be permissioned or permissionless, and avoids some of the issues with miners by not paying a block creation reward, but just a transaction fee.

Basics of Ethereum (Contd.)

- The Ethereum platform forms the backbone for new applications by making sure they are free from censorship (if you pay to execute a transaction it will execute), have no downtime, and have no third-party interference.
- It is also the platform that has spurred the huge increase in Initial Coin Offerings (ICOs), since it is easy to launch a new digital token on Ethereum. Most of these tokens are meant to fund the development of Dapps.

What is Ethereum?

- Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called **smart contracts.**
- Smart contracts allow participants to transact with each other without a trusted central authority.
- Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data.
- Transactions are sent from and received by user-created Ethereum accounts.
- A sender must sign transactions and spend Ether, Ethereum's native cryptocurrency, as a cost of processing transactions on the network.

- On September 15th, 2022 06:42:42 UTC, at block 15537393, **The Merge** was completed, moving Ethereum from Proof of Work (PoW) to Proof of Stake (PoS). Amazon Managed Blockchain's Ethereum Mainnet nodes run on the Ethereum PoS network.
- The Merge upgrades Ethereum's consensus from PoW to PoS by merging Ethereum Mainnet with the Beacon Chain Proof of Stake system.
- This upgrade improved the sustainability of Ethereum by lowering energy consumption and was part of Ethereum foundation's ongoing upgrades to improve scalability, security, and sustainability.

Ethereum Smart Contract

- A smart contract is application code that resides at a specific address on the blockchain known as a **contract address.**
- Applications can call the smart contract functions, change their state, and initiate transactions.
- Smart contracts are written in programming languages such as Solidity and Vyper, and are compiled by the Ethereum Virtual Machine into bytecode and executed on the blockchain.

Ethereum Account

- There are two types of accounts in Ethereum: **Externally Owned Accounts (EOA) and Contract Accounts.**
- An EOA is controlled by a private key, has no associated code, and can send transactions.
- A contract account has an associated code that executes when it receives a transaction from an EOA. A contract account cannot initiate transactions on its own. Transactions must always originate from an EOA.

Ethereum Transaction

- A transaction in Ethereum is a signed data message sent from one Ethereum account to another.
- It contains the transaction sender and recipient information, the option to include the amount of Ether to be transferred, the smart contract bytecode, and the transaction fee the sender is willing to pay to the network validators to have the transaction included in the blockchain, known as gas price and limit.

Payment for transactions on Ethereum

- You can pay for transactions using Ether.
- Ether serves two purposes. First, it prevents bad actors from congesting the network with unnecessary transactions. Second, it acts as an incentive for users to contribute resources and validate transactions (mining).
- Each transaction in Ethereum constitutes a series of operations to occur on the network (i.e. a transfer of Ether from one account to another or a complex state-changing operation in a smart contract).
- Each of these operations have a cost, which is measured in gas, the fee-measure in Ethereum. Gas fees are paid in Ether, and are often measured in a smaller denomination called gwei. [1 ether = 1,000,000,000 gwei (10^9)].

Buying and storage of Ether

- Ether can be bought with fiat currency from a cryptocurrency exchange like Coinbase or Kraken.
- Ether is associated with your Ethereum account.
- To access your account and Ether, you must have your account address and the passphrase or the private key.

Signing a transaction

- Signing a transaction generates a signature on a transaction using the private key of the transaction sender's account.
- Transactions need to be signed before they are submitted to the network.

Virtual Machine

- A virtual machine (VM) is a software-based emulation of a physical computer that runs an operating system and applications just like a physical computer. Here are the key aspects of virtual machines:
- **Components of a Virtual Machine**

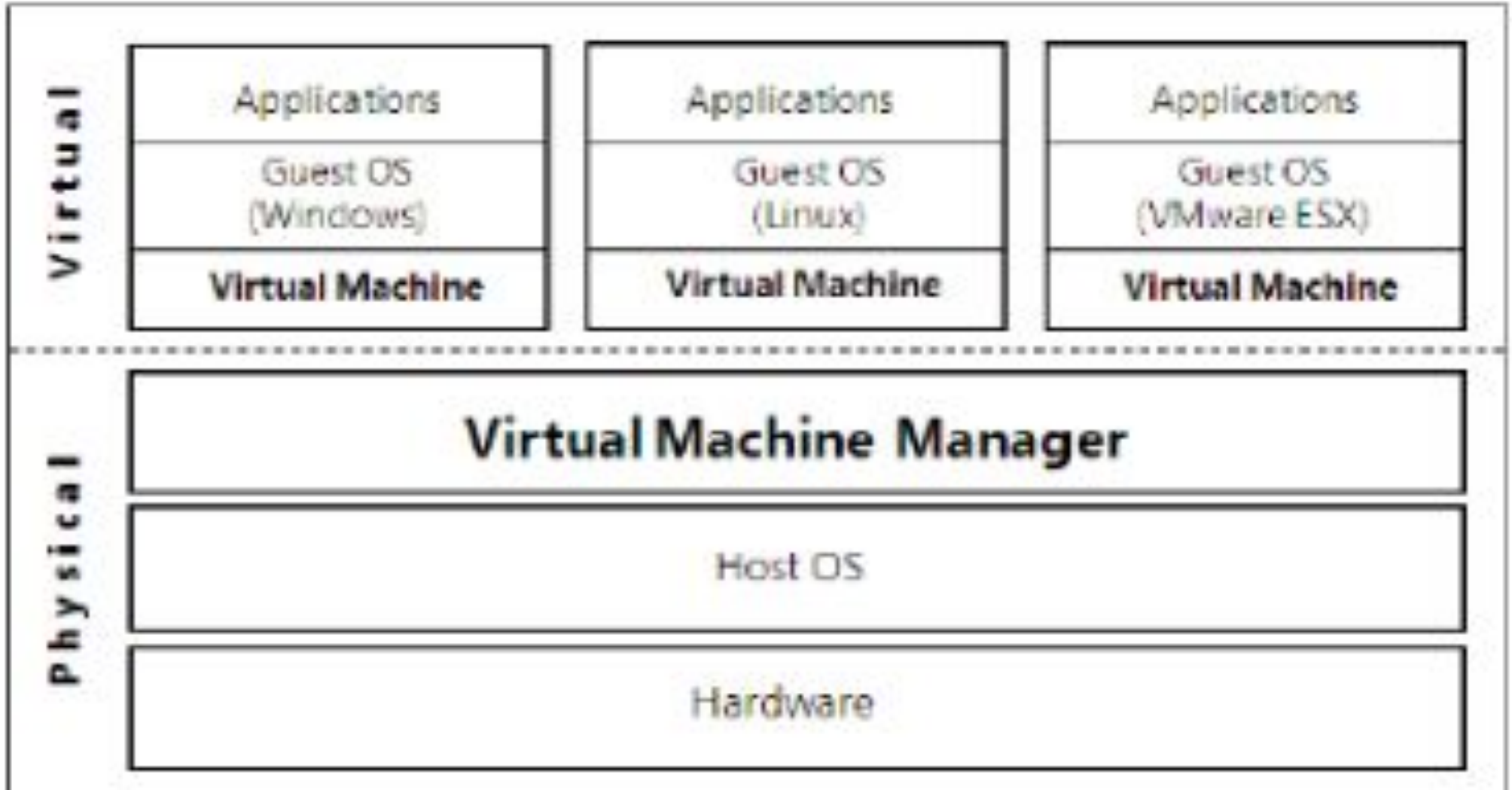
1. **Hypervisor:** The software layer that enables the creation and management of VMs.

2**. Virtual Hardware:** VMs simulate hardware such as CPUs, memory, storage, and network interfaces. These are allocated from the physical hardware of the host machine.

3. Guest Operating System: The OS running inside the VM. It can be different from the host OS, allowing multiple OSes to run on a single physical machine.

4. Virtual Disk: A file or set of files on the host system that emulates a physical hard drive for the VM.

Virtual Machine (Contd.)



Virtual Machine (Contd.)

- **Benefits of Virtual Machines**

1. **Isolation**: Each VM operates independently, isolating applications and services. This improves security and stability, as issues in one VM do not affect others.
2. **Resource Utilization**: VMs allow for better utilization of physical hardware by running multiple virtual machines on a single physical server.
3. **Scalability**: It is easier to scale resources up or down by adjusting the virtual hardware settings.
4. **Flexibility**: VMs can run different operating systems and applications on the same physical hardware, facilitating diverse workloads and testing environments.
5. **Backup and Recovery**: VMs can be easily cloned, snapshotted, and backed up, enhancing data protection and recovery processes.

Ethereum Virtual Machine (EVM)

- The Ethereum platform possesses its own programming language, called Solidity, which is similar to C++ or JavaScript.
- It is a “virtual” machine in that it doesn’t really exist except as a loose confederation of nodes on the Ethereum network.
- What is really clever about the EVM is that it enables the computers on the Ethereum network to function as a kind of global computing resource.
- The EVM is the powerhouse that executes smart contracts.
- Each participant in the network adds computing power to the network, and all decentralized apps (also known as Dapps) can purchase use of this power by spending ether.

Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is a crucial component of the Ethereum blockchain that enables the execution of smart contracts and decentralized applications (DApps). Here's an overview of its key aspects:

- Virtual Machine: The EVM is a virtual machine that runs on the Ethereum network, allowing developers to **deploy and execute smart contracts.** It provides a **runtime environment** for smart contracts, ensuring they run consistently across all nodes in the network.

- Turing Complete: The EVM is Turing complete, meaning it can execute any computational task given enough resources, allowing for complex and versatile applications.

- **Key Features**

1. Decentralization: The EVM operates on a decentralized network of nodes, ensuring that smart contracts are executed in a trustless and tamper-proof manner.

2. Deterministic: Smart contracts on the EVM are deterministic, meaning that they produce the same output from a given input across all nodes, ensuring consistency and reliability.

3. Bytecode Execution: Developers write smart contracts in high-level programming languages like Solidity, which are then compiled into EVM bytecode. This bytecode is what the EVM executes.

4. Gas: The EVM uses a concept called "gas" to measure computational work and prevent infinite loops or excessive resource usage. Gas is a unit of measure for the computational effort required to execute operations.

Ethereum Virtual Machine

- **Components**

1. Accounts:

- - **Externally Owned Accounts (EOAs):** Controlled by private keys, typically representing users.
- - **Contract Accounts:** Controlled by the code of the smart contract itself, executing functions when called upon.

2. Storage: Each smart contract has its own storage, a persistent state that can be accessed and modified by the contract code.

3. Memory: Temporary storage used during contract execution, which is cleared after the execution completes.

4. Stack: A last-in-first-out (LIFO) data structure used to hold intermediate values during contract execution.

Ethereum Virtual Machine

- **Functionality**

1. Smart Contract Execution: The EVM processes and executes smart contract instructions, ensuring all nodes achieve consensus on the contract's state and results.

2. Transaction Handling: The EVM validates and processes transactions, updating the state of accounts and contracts accordingly.

3. Gas Calculation: The EVM calculates the gas required for each operation, ensuring that transaction senders pay for computational resources consumed.

- **Use Cases**

1. Decentralized Finance (DeFi): Applications like lending platforms, decentralized exchanges, and stablecoins.

2. Non-Fungible Tokens (NFTs): Platforms for creating and trading unique digital assets.

3. Decentralized Applications (DApps): Various applications ranging from games to supply chain management.

- The Ethereum Virtual Machine is a foundational technology for the Ethereum blockchain, enabling decentralized computation through smart contracts. It provides a robust, secure, and decentralized environment for executing complex programs, fostering a wide range of innovative applications.

Ether and Gas

- Ether (ETH) and gas are fundamental concepts in the Ethereum network, but they serve different purposes.
- **Currency:** Ether is the native cryptocurrency of the Ethereum network. It functions similarly to Bitcoin in the Bitcoin network.

1. **Uses:**
    1. **Transactions:** It is used to transfer value between users.
    2. **Staking:** In Ethereum 2.0, Ether is used for staking, where users can lock up their ETH to help secure the network and earn rewards.
    3. **Store of Value:** It can be held as an investment or store of value.
2. **Symbol:** ETH
3. **Economic Role:** Ether acts as a medium of exchange and a store of value within the Ethereum ecosystem.

Ether and Gas (Contd.)

- **Gas**

1. **Purpose:** Gas is a unit of measure that represents the amount of computational effort required to execute operations, such as transactions and smart contract executions, on the Ethereum network.
2. **Measurement:** Gas is measured in units and determines the amount of work miners need to perform to include a transaction in a block.
3. **Cost:** The amount of gas required for a transaction depends on its complexity. More complex operations require more gas.

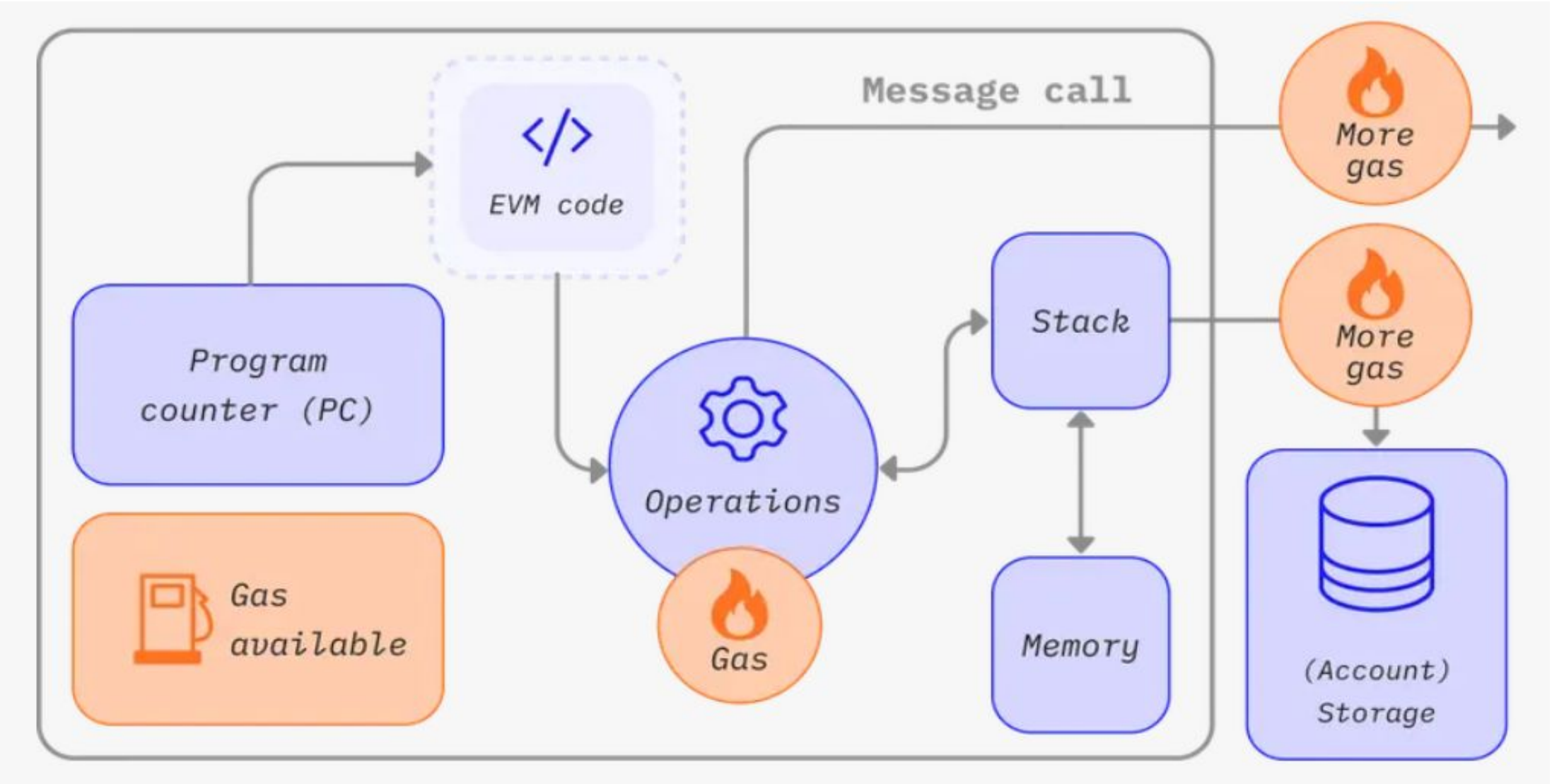
Ether and Gas (Contd.)

4. Price (Gas Price): Users specify the gas price they are willing to pay for each unit of gas, denominated in Ether. This is usually expressed in Gwei (1 Gwei = 10^(-9) ETH).

5. Function: Gas serves as a fee mechanism to incentivize miners to process transactions and to prevent abuse of network resources by making it costly to run expensive computations.

6. Limits:

1. **Gas Limit:** The maximum amount of gas a user is willing to spend on a transaction. If the gas runs out during execution, the transaction fails but the gas is consumed.
2. **Block Gas Limit:** The maximum amount of gas that all transactions in a block can consume. This limit is set by the network and ensures that blocks are processed efficiently.


Message call
EVM code
Program counter (PC)
Gas available
Operations
Gas
Stack
Memory
More gas
More gas
(Account) Storage

Ether

- Ethereum refers to the entire open-source platform for developing distributed applications, while “ether” is the actual digital token that is used to fuel the platform.
- Ethereum Foundation prefers to think of ether as being the “fuel” for running decentralized applications on the Ethereum network.
- The way the EVM is set up, network users have access to a global network of computers that is fast, efficient, and always available. However, running applications on the EVM is not free so ether can be used to transfer value to the computer owners on the network.

Ether (Contd.)

- You can think of ether as a tool for resource management of the computing power of the network. Just as your own computer has an activity monitor that allows you to toggle between applications and use CPUs effectively, a global decentralized computer also needs to manage who uses the computing power.
- Payment for computing power allows effective management of a scarce resource because there is very little incentive to spam the network or run an infinite loop of code if you are required to pay for all that computing. If you run out of fuel, your program stops!
- One can acquire ether by purchasing it on an exchange, by creating blocks for the Ethereum network, or by running and validating transactions on the Ethereum network.
- Since the movement away from Proof of Work to Proof of Stake, mining of ether has diverged greatly from mining bitcoin. The reward for creating a new block is capped at five ether coins.

Ether (Contd.)

- Gas is used by developers of Ethereum as the fuel for running their applications. As you already know, Ethereum is unique in that it is designed to host Dapps. Each of these programs varies considerably in terms of size and complexity. As a result, the amount that is charged to run these programs on the EVM must also vary. Costs are broken down by line of code and can be tiny fractions of one ether coin. Gas became a way to aid developers in accounting for the cost of running their programs as they were building.
- The basic idea was to decouple the price of running Ethereum transactions from the more volatile price of ether. In order to run your transaction on the EVM, you must specify how much you are willing to pay as the “gas limit” and you must actually have enough gas in your Ethereum wallet to afford to run the proposed transaction.

Smart Contract

- Ethereum is the most popular platform for developing, storing and executing smart contracts. Smart contracts can be thought of as computer programs that encode the rules for just about any kind of contract using programming languages such as Solidity, which has similarities to C and JavaScript, or Vyper, which looks more like Python.
- Solidity is considered to be a Turing-complete programming language, meaning it supports all of the programming structures of a full feature language like C.
- 1. Logic is encoded into smart contract program language
- 2. Nodes on the EVM compile, validate, store, and replicate the smart contract across the network
- 3. When the triggering event(s) occur, the contract is executed by the nodes on the network
- 4. Changes are made to the appropriate accounts on the network as a result of successfully executing the contract

Smart Contract (Contd.)

- Smart contracts are also key to expanding the functionality of the Internet of Things (IoT). Some of the attributes of smart contracts include:
- **Security** – smart contracts are encrypted and have a high degree of security
- **Redundancy** – copying a smart contract across all of the nodes on the network ensures redundancy (though lowers the efficiency of the network)
- **Accuracy** – contracts are validated by many nodes on the network
- **Autonomous** – there is no need for a third party to be involved in the execution of a contract, lessening the potential for bias or mistakes; additionally, smart contracts are a tool for automating business logic, and allowing machines to transact without intervention
- **Efficiency** – by eliminating middlemen, the cost of transactions is minimized
- **Transparency** – on a permissionless blockchain, all parties have access to the shared ledger; transactions can be audited.

On-chain versus Off-chain versus Side Chain

- These concepts have become especially important in discussions to resolve major issues and bugs in the platform. When developers submitted the proposal of the hard fork for The DAO to the Ethereum community (client developers and users) for comment and voting, this was an example of how governance issues were resolved in an “off-chain” manner. In other words, the solution was not built into the Ethereum protocols.
- As Vlad Zamfir, one of the key researchers at the Ethereum Foundation puts it, “‘On-chain governance’ refers to the idea that the blockchain nodes automatically upgrade when an on-chain governance process decides on an upgrade and that it’s time to install it. No hard forks required.”
- The deliberation process of hard-forks is part of off-chain governance, as the blockchain platform itself does not have protocols for moving through a decision. A key insight here is that off-chain governance necessitates the participation of node operators, as their decisions help define the outcome.

On-chain versus Off-chain versus Side Chain (Contd.)

- Newer blockchain platforms such as Dfinity are trying to improve on this by putting the rules for governance directly into their protocols so that they can avoid potentially fatal issues such as The DAO hack and the resulting hard fork.
- Dfinity's protocols allow for making direct changes to the ledger when there is a consensus among all of its coin holders. As these networks continue to grow, one of the biggest debates now in the blockchain community concerns scaling up the platforms to allow for higher processing volume and speed.
- One solution is to take some of the processing of transactions off-chain to lessen the burden on the main chain.
- If two banks, A and B, wanted to have thousands of Ethereum transactions between each other every day, it might help them to create a special sidechain.
- The sidechain would be much quicker and cheaper to run than it would be to have each transaction on the main Ethereum chain where a transaction fee would be incurred for each one. With a sidechain, all it takes is for the parties to use one transaction at the end of the day to settle their accounts on the main Ethereum chain.

On-chain

- The term "on-chain" refers to transactions, data, or activities that occur directly on a blockchain. Here are some key aspects of on-chain activities:
- **1. Transparency:** All on-chain transactions are recorded on the blockchain, which is a public ledger, and can be viewed by anyone. This ensures a high level of transparency.
- **2. Security:** Since transactions are verified by a network of nodes and recorded in a decentralized manner, they are secure and resistant to tampering.
- **3. Immutability:** Once data is recorded on-chain, it cannot be altered or deleted. This immutability is a core feature of blockchain technology.

On-chain (Contd.)

- **4. Decentralization:** On-chain activities are governed by the rules of the blockchain protocol and are not controlled by any single entity. This ensures a decentralized approach to data management and transaction processing.
- **5. Verification:** Transactions and activities on-chain are verified by the consensus mechanism of the blockchain (e.g., Proof of Work, Proof of Stake). This process ensures the integrity and validity of the transactions.
- **6. Smart Contracts:** On-chain operations can include the execution of smart contracts, which are self-executing contracts with the terms directly written into code. These can automate various processes and enforce agreements without intermediaries.
- Examples of on-chain activities include transferring cryptocurrencies, creating and executing smart contracts, and recording asset ownership or other data directly on the blockchain.

Off-chain

Off-chain transactions refer to transactions or activities that occur outside of the blockchain but can be later recorded on it. These transactions are typically used to enhance the efficiency and scalability of blockchain networks by reducing the load on the blockchain itself. Here are the key aspects of off-chain transactions:

1. **Speed and Efficiency:** Off-chain transactions can be processed more quickly and with lower costs since they don't require the immediate involvement of the entire blockchain network for each transaction.

2. Scalability: By handling transactions off-chain, blockchains can support a higher volume of transactions without congesting the network, thus enhancing overall scalability.

3. Privacy: Off-chain transactions can offer greater privacy since they are not immediately visible on the public blockchain. The details of these transactions can be kept confidential between the parties involved until they are settled on-chain.

Off-chain (Contd.)

4. Lower Fees: Since off-chain transactions do not require the same level of computational resources and network fees as on-chain transactions, they can be more cost-effective.

5. Flexibility: Off-chain mechanisms can allow for more complex transaction structures and interactions that might be more cumbersome or expensive to implement directly on-chain.

- **Use Cases**
- - **Micropayments:** Off-chain solutions are ideal for micropayments where on-chain fees would be prohibitively high.
- **- Private Agreements:** Businesses can conduct private transactions and only settle final balances on-chain.
- - **High-Frequency Trading:** Financial institutions can perform high-frequency trading without congesting the blockchain network.

Side-chain

- Sidechain transactions refer to activities that occur on a secondary blockchain (sidechain) which is interoperable with a main blockchain (mainchain). Sidechains are independent blockchains that are connected to the main blockchain through a two-way peg, allowing for the transfer of assets and data between the two chains. Here are key aspects of sidechain transactions:
- **1. Interoperability:** Sidechains are designed to work alongside the main blockchain. Assets or tokens can be moved from the mainchain to the sidechain and back, typically through a process involving locking and unlocking tokens.
- **2. Scalability:** By offloading transactions and computations from the mainchain to the sidechain, sidechains help alleviate congestion and enhance the scalability of the main blockchain.
- **3. Customization:** Sidechains can be tailored to specific use cases or requirements. They can have different rules, consensus mechanisms, and features from the mainchain, allowing for greater flexibility and experimentation.
- **4. Security:** While sidechains operate independently, their security is crucial. The assets transferred to a sidechain are usually secured by the sidechain's own consensus mechanism. The mainchain typically ensures security through mechanisms like the two-way peg and periodic audits.
- **5. Innovation:** Sidechains provide a sandbox for innovation, where new features and updates can be tested without affecting the mainchain. Successful features can later be integrated into the mainchain.

Side-chain (Contd.)

- How Sidechain Transactions Work
- **1. Two-Way Peg:** A mechanism that enables the transfer of assets between the mainchain and the sidechain. When assets are transferred to the sidechain, they are locked on the mainchain and an equivalent amount is minted or unlocked on the sidechain, and vice versa.
- **2. Validators:** Sidechains have their own set of validators or miners who are responsible for maintaining the network, validating transactions, and securing the blockchain.
- **3. Smart Contracts:** Sidechains can utilize smart contracts to manage the locking and unlocking of assets, ensuring that the total supply of tokens remains consistent between the chains.
- **Use Cases**
- - **High-Throughput Applications:** Applications requiring high transaction throughput, such as gaming or microtransactions, can be handled on sidechains.
- **- Confidential Transactions:** Sidechains can offer enhanced privacy features, making them suitable for confidential transactions.
- **- Experimentation:** Developers can test new features, consensus algorithms, or blockchain configurations on sidechains without risking the stability of the mainchain.

Mining Ethereum

- While there are many similarities between mining on the Ethereum network and mining on the Bitcoin network, it might be useful to consider how they differ.
- it takes about ten minutes on average to create a new block on the Bitcoin network, whereas on Ethereum, it takes about fifteen seconds to add a block.
- Ethereum miners are awarded 3 ETH plus the transaction fees included with the block for each block they create. Keep in mind that a transaction on Ethereum could include processing the program code stored on the network for supporting a smart contract.
- Mining ether is also designed to be ASIC-resistant so that small, individual miners can compete with the big mining firms using cheaper GPU mining rigs. This is accomplished by using the ethash hashing algorithm, which is designed specifically to be solved by GPU machines, as opposed to the SHA-256 algorithm used by Bitcoin.
- Just as with bitcoin, as the price of ether rises, more miners compete to create new blocks and the associated hash rate increases. To keep the block creation time at fifteen seconds, the network can adjust the difficulty of the hashing algorithm to make it harder.
- Assuming that one has access to cheaper electricity, it may be worthwhile to purchase a GPU machine and install the full Ethereum network protocols that are needed to become a miner. With Ethereum, it may not be as much about making a fortune as it is with the mining of bitcoin.