Giovanni Paul-Sodipo

EKOLANCE SOLIDITY COURSE: Week 1
Assignment

1. What are Layer-1 & Layer-2 blockchains?

Layer-1 blockchains are the foundation of the blockchain architecture. Layer-1 blockchains validate and execute transactions without the assistance of another network, and cryptocurrencies are used to reimburse transaction fees in decentralized systems.

Layer-2 refers to solutions designed to help an application scale by processing transactions outside of the Ethereum Mainnet (layer 1) while maintaining the same security and decentralization as the mainnet. Layer 2 solutions boost throughput (transaction speed) while lowering gas costs.

Basically, Layer-1 is here to improve the blockchain architecture, while layer-2 is here to build third-party networks on top of the main blockchain.

2. Does Solana have a layer two blockchain?

No, Solana lacks a layer two blockchain. It employs a layer one blockchain and is generally regarded as a third-generation blockchain.

3. What are ZK rollups?

ZK-rollups are "hybrid scaling solutions," or off-chain protocols that operate independently but rely on Ethereum for security. It performs transactions, computations, and data storage off-chain while holding assets in an on-chain smart contract.

4. What is the Blockchain Trilemma?

In 2017, Ethereum co-founder Vitalik Buterin coined the phrase "Blockchain trilemma," outlining the trade-offs required to achieve "scalability".The Blockchain Trilemma refers to the widely held belief that decentralized networks can only provide two of three benefits in terms of decentralization, security, and scalability at any given time. In this article, we will look at the current challenges of providing all three elements at the same time.

5. What is Ethereum Merge?

A major event the crypto industry has long been awaiting finally happened: Ethereum's "Merge" which proponents say could boost crypto prices in the long run and significantly change the future of cryptocurrency.The Merge is an upgrade to the Ethereum blockchain, which powers innovations in the crypto ecosystem like non-fungible tokens (NFTs).

The Merge is an upgrade to the Ethereum blockchain, which powers innovations in the crypto ecosystem like non-fungible tokens (NFTs).

The upgrade transitioned Ethereum to the proof-of-stake model, which is a more energy-efficient and environmentally-friendly system. It entails nodes being selected via an algorithm that has a preference for nodes that hold more of a network's currency.

6. What is a Blockchain?

A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called blocks that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks.

Each block on the chain contains several transactions, and whenever a new transaction occurs on the Blockchain, each participant's record of that transaction is added to the ledger.

7. What is the difference between Bitcoin, Ethereum, Polkadot, Solana, Cardano and Binance smart chains?

Bitcoin: Bitcoin is primarily designed to be an alternative to traditional currencies and hence a medium of exchange and store of value. It uses BTC as its cryptocurrency abbreviated name.

Ethereum: Ethereum proposed to use blockchain technology not only for maintaining a decentralized payment network but also for storing computer code that can be used to power tamper-proof decentralized financial contracts and applications.Ethereukm is represented by the abbreviation "ETH".

Polkadot: The main blockchain runs on a relay chain, which allows for lightning-fast transaction processing. This process is extremely fast, resulting in lower transaction fees and a lower carbon footprint than other Proof-of-Stake protocols.It can be referred natively in markets as "POLKADOT" in markets.

Solana: Solana is a decentralized blockchain built to enable scalable, user-friendly apps for the world. It is termed as "SOL".Solana provides much faster transactions at a reduced cost when compared to Ethereum and Polygon.

Cardano: Cardano is a blockchain and smart contract platform whose native token is called Ada. The Cardano platform runs on the Ouroboros consensus protocol. Ouroboros, created by Cardano in its foundation phase, is the first PoS protocol that was proved to be secure.

Binance smart Chain: "BNB" Smart Chain is a high-performance and cheap to run blockchain with an emphasis on smart contract programmability. BSC is a new smart contract platform launched by Binance based on the Go Ethereum (Geth) client, making it compatible with blockchain apps developed for the Ethereum network.

Additional differences;
- Block size differences
- Ethereum 2.0 is updating to keep its leading position
- They have different algorithm
- They were built with different programming languages

8. What is a Consensus Algorithm?

A consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. These algorithms are designed to achieve reliability in a network involving multiple users or nodes.

9. State any four type of Consensus Algorithms.

- Proof of Work

The PoW algorithm is one of the oldest types if not the oldest of consensus algorithms. First introduced in 1993 and reintroduced in 2008 by Bitcoin founder Satoshi Nakamoto.The central idea of PoW is to have nodes solve complex mathematical puzzles and make as many guesses as possible in the fastest possible time.

In cryptocurrency blockchains based on the PoW algorithm, miners or validators also known as participant nodes must prove that the work they've done and submitted gives them the right to add new transactions to the blockchain. They must solve a complex mathematical problem by finding a cryptographic hash of a particular block.This is done by taking data from a block header as an input, and continuously running this data through a cryptographic hash function.

- Proof of Stake

Proof of Stake (PoS) is considered an alternative to PoW. Unlike PoW, PoS requires little specialized hardware or software resources to mine cryptocurrencies since it doesn't involve solving complex computational problems. Rather, crypto validators lock up or stake some of their coins in a wallet. They then validate blocks if they discover a block that can be added to the blockchain.

Validators get a reward -- or their stake increases -- proportionate to their bets based on the blocks added to the blockchain. Since the algorithm is incentive-based, it consumes less computational energy than PoW. Despite this advantage, the PoS algorithm has a serious drawback. The mining capacity of a validator depends on the number of tokens they have, so a miner who starts with more coins gets more control over the consensus mechanism. Additionally, a few miners can purchase many coins, further diluting the mechanism and reducing the system's decentralization property.

- Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is considered a more efficient and democratic version of PoS. This algorithm is based on a voting system in which delegates or witnesses vote for their favorite validators to achieve consensus during the generation and validation of blocks. Besides validating transactions, delegates also help maintain the integrity, reliability and transparency of the blockchain network.

The voting power of each delegate is proportional to the number of coins held. They receive rewards for their work with transaction fees, which are shared with their respective electors.

The DPoS algorithm's voting system, and therefore the consensus mechanism, depends on the reputation of the delegates. It's a more scalable mechanism than PoW or PoS since it can process more transactions per second and provide faster confirmation times.

- Proof of Burn

Proof of Burn (PoB) is being tested as a viable and sustainable alternative to PoW and PoS algorithms. PoB is like PoW, but it consumes much less computational energy. This is because its block validation process on the blockchain doesn't require computational resources or hardware. Instead, miners "burn" or invest coins in the blockchain to achieve consensus.

Coins are sent to an address from where they can't be retrieved, rendering them inaccessible and useless. This demonstrates the miners' commitment to the network and gives them the right to mine new coins and validate new transactions on the network. The more coins a miner burns, the more mining power they have, which increases their chances of becoming the next block validator.

Filename: Dauda Lawal.docx
Directory:
                   /Users/user/Library/Containers/com.microsoft.Word/Data/Docu
      ments
Template: Normal.dotm
Title:
Subject:
Author: Microsoft Office User
Keywords:
Comments:
Creation Date: 13/10/2022 09:08:00
Change Number: 3
Last Saved On: 13/10/2022 13:18:00
Last Saved By: Microsoft Office User
Total Editing Time: 51 Minutes
Last Printed On: 13/10/2022 13:19:00
As of Last Complete Printing
      Number of Pages: 3
      Number of Words: 1,307
      Number of Characters: 7,297 (approx.)