MODULE 15

Nayeer Naushad

21052338

**Blockchain:** A decentralized database technology that maintains a continually growing set of transactions and smart contracts hardened against tampering and revision using cryptography

**Block:** A growing list of records in a blockchain

**Transaction:** An exchange, usually of currency, in a blockchain

**Ledger:** A digital record of transactions

**Immutable:** The ability of a blockchain to remain unchanged

**Trust:** The dispersed confidence in accuracy among blockchain users

**Transparency:** Clear and open accounting of transactions

**Amazon Athena**

Athena is an interactive query service that makes it easy to analyze data in Amazon Simple Storage Service (Amazon S3) using standard structures query language (SQL)

Athena is serverless, so there is no infrastructure to manage, and users pay only for the queries that they run. Users can quickly query your data without having to set up and manage any servers or data warehouses. Point to the data in Amazon S3, define the scheme, and start querying using the built-in query editor. Athena lets users tap into all of their data in S3 without the need to set up complex processes to extract, transform, and load (ETL) the data. Athena is easy to use; there’s no need for complex ETL jobs to prepare data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

Athena is out-of-the-box integrated with AWS Glue Data Catalog, letting users create a unified metadata repository across various services, crawl data sources to discover schemas, populate the Data Catalog with new and modified table and partition definitions, and maintain schema versioning. Users can also use AWS Glue fully manages ETL capabilities to transform data or convert it into columnar formats to optimize cost and improve performance.

With Athena, users pay only for the queries that they run. Users can save from 30 percent to 90 percent on per-query costs and get better performance by compressing, partitioning, and converting data into columnar formats. Athena queries data directly in Amazon S3. There are no additional storage charges beyond S3. Athena uses Presto with ANSI SQL supports and works with a variety of standard data formats, including CSV, JavaScript Object Notation (JSON), Apache ORC, Apache Avro, and Apache Parquet. Athena is ideal for quick, one-time querying, but it can also handle complex analysis, including large joins, window functions, and arrays. Athena is highly available and runs queries using compute resources across multiple facilities and multiple devices in each facility.Athena uses Amazon S3 as its underlying data store, making data highly available and durable. With Athena, users don’t have to worry about having enough compute resources to get fast, interactive query performance. Athena automatically runs queries in parallel, so most results come back within seconds.

**Amazon Macie**

Macie is a security service that used machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property and provides dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects risk to protect data stored in Amazon S3, with support for additional AWS data stores coming soon. Macie makes it easy for security administrations to have management visibility into data storage environments, beginning with S3, with additional AWS data stores coming soon.

‘

Macie uses machine learning to automate the process of discovering, classifying, and protecting data stored in AWS.This helps you better understand where sensitive information is stored and how its being accessed, including user authentication and access patterns. Macie can send all findings to Amazon CloudWatch Event. This lets users build custom remediation and alert management for existing security ticketing systems.

**Blockchain and Amazon Managed Blockchain**

Blockchain is a way to manage an open distributed ledger of transactions. A ledger is a type of database in which transactions are only appended, never changed, making it immutable and trusted because there is no way to alter entries. A transaction is the record of some event taking place where ownership or possession is being transferred. The primary objective of a blockchain is to eliminate a central authority or middleman in order to speed things up.

Blockchain is a growing list of records, like a databse - called blocks - that are linked using cryptography. Each block contains information about the block before it, a timestamp, and transaction data. Blockchain began with the development of cryptocurrency and has no branched out into new products and services.

Blockchain makes it possible to build applications whre multiple parties can run transactions without the need for a trusted central authority. Managed Blockchain is a fully managed service that lets usres set up and manage a scalable blockchain network with a few clicks. Managed Blockchain eliminates the overhead required to create the network and automatically scales to meet the demands of thousands of applications running millions of transactions. After the network is up and running, Managed Blockchain makes it easy to manage and maintain your blockchain network. It manages certificates and lets users easily invite new members to join the network.

Managed Blockchain is a service that assists in choosing and provisioning other AWS services together with non-AWS services such as Ethereum in order to implement a blockchain. By asking a series of structured questions, Managed Blockchain guides the process of choosing the services needed to implement one of several types of blockchain.

With Managed Blockchain, users can quickly create blockchain networks that span multiple AWS accounts, letting a group of members run transactions and share data without a central authority. Unlike self-hosting a blockchain infrastructure, Managed Blockchain eliminates the need for manually provisioning hardware, configuring software, and setting up networking and security components. With the Managed Blockchain voting application programming interface (API), network participants can vote to add or remove members. After a new member is added, Managed Blockchain lets that member launch and configure multiple blockchain peer nodes to process transaction requests and store a copy of the ledger. Managed Blockchain also monitors the network and automatically replaces poorly performing nodes.

Managed Blockchain supports two popular blockchain frameworks: Hyperledger Fabric and Ethereum. Hyperledger Fabric is well suited for applications that require stringent privacy and permission controls with a known set of members; for example, a financial application where certain trade-related data is only shared with select banks. Ethereum is well suited for highly distributed blockchain networks where transparency of data for all members is important; for example, a customer loyalty blockchain network that lets any retailer in the network independently verify a user's activity across all members to redeem benefits. Alternatively, Ethereum can be used for joining a public Ethereum blockchain network. Ethereum and Hyperledger Fabric are products that are produced by companies outside AWS.

Managed Blockchain can easily scale your blockchain network as the usage of applications on the network grows over time. When a network member requires additional capacity for creating and validating transactions, the member can quickly add a new peer node using Managed Blockchain APIs. Managed Blockchain provides a selection of instance types that comprise varying combinations of central processing unit (CPU) and memory to give the flexibility to choose the appropriate mix of resources for the workload. Additionally, Managed Blockchain secures the network’s certificates with AWS Key Management Service (AWS KMS) technology, eliminating the need for users to set up their own secure key storage.

Blockchain technologies are often used to solve two types of customer needs. In the first case, multiple parties work with a centralized, trusted authority to maintain a complete and verifiable record of transactions. An example is a retail customer looking to connect their suppliers with a centralized ledger that maintains a transparent and verifiable history of information related to the movement of a product through its supply chain.