COLOMBIA POTENCIA DE LA VIDA

TIC

Algoritmos de consenso **básico para blockchain**

Lección 3- Módulo 2 - Unidad 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Desarrollo de la sesión:

En la exploración inicial de esta sesión sobre algoritmos de consenso en blockchain, es esencial comprender la función central del consenso en la integridad de los datos en redes descentralizadas. El consenso garantiza que todos los nodos de la red estén de acuerdo sobre el estado del libro mayor compartido, evitando así la posibilidad de doble gasto y garantizando la coherencia de la información almacenada en la cadena de bloques.

Una de las formas más comunes de alcanzar el consenso en blockchain es mediante la Prueba de Trabajo (Proof of Work - PoW). En PoW, los participantes compiten entre sí para resolver problemas criptográficos complejos y validar transacciones en la red. Este proceso requiere una gran cantidad de energía y potencia computacional, pero proporciona una seguridad robusta al garantizar que los datos en la cadena de bloques sean inmutables y resistentes a la manipulación.

Otro enfoque popular es la Prueba de Participación (Proof of Stake - PoS), que asigna la capacidad de validar bloques según la cantidad de criptomonedas que un participante está dispuesto a apostar. PoS es conocido por ser más eficiente energéticamente que PoW y promueve la participación activa de los titulares de criptomonedas en la seguridad y gobernanza de la red.

Además, existen variantes como la Prueba de Autoridad (Proof of Authority - PoA), que se basa en una lista de nodos de confianza para validar transacciones. PoA prioriza la velocidad de transacción y la eficiencia en entornos de blockchain más controlados y privados, lo que lo hace adecuado para casos de uso específicos donde la velocidad es crucial y la descentralización no es una prioridad.

Es importante comprender las implicaciones y trade-offs de cada algoritmo de consenso, ya que cada uno tiene sus propias ventajas y desventajas en términos de seguridad, escalabilidad y descentralización. La elección del algoritmo de consenso adecuado depende del contexto específico de la aplicación y los requisitos del proyecto de blockchain.

En la práctica, los proyectos de blockchain implementan estos algoritmos de consenso de manera diferente según sus necesidades y objetivos de diseño. Algunos pueden optar por PoW para garantizar una mayor seguridad, mientras que otros pueden elegir PoS para mejorar la eficiencia y reducir el consumo de energía. La diversidad de enfoques refleja la naturaleza adaptable y flexible de la tecnología blockchain.

Los algoritmos de consenso también están en constante evolución, con investigaciones y desarrollos continuos para mejorar su eficiencia y seguridad. Es crucial estar al tanto de las últimas innovaciones en este campo para garantizar que las redes blockchain sigan siendo seguras, escalables y descentralizadas en un mundo digital en constante cambio.

Los algoritmos de consenso son mecanismos fundamentales en las redes blockchain que permiten a los participantes llegar a un acuerdo sobre el estado del libro de contabilidad distribuido sin necesidad de una autoridad central. Estos algoritmos son esenciales para garantizar la seguridad, integridad y descentralización de la red. A continuación, se describen algunos de los algoritmos de consenso más comunes:

Prueba de Trabajo (Proof of Work - PoW):
PoW es el algoritmo de consenso original utilizado en Bitcoin. En este sistema, los nodos de la red (llamados "mineros") compiten para resolver problemas criptográficos complejos. El primer minero en resolver el problema y encontrar un hash válido para el bloque propuesto tiene el derecho de agregar el bloque a la cadena y recibir una recompensa en criptomonedas. PoW es conocido por su seguridad, pero también consume una gran cantidad de energía.

Prueba de Participación (Proof of Stake - PoS):
En PoS, la probabilidad de que un nodo mine un bloque y reciba recompensas está determinada por la cantidad de criptomonedas que posee y está dispuesto a bloquear como "participación". Esto significa que cuanto más grande sea la participación de un nodo, más probabilidades tendrá de ser seleccionado para validar transacciones y agregar bloques a la cadena. PoS se considera más eficiente energéticamente que PoW, pero algunos críticos argumentan que puede conducir a la centralización.

Prueba de Autoridad (Proof of Authority - PoA):
PoA es un algoritmo de consenso en el que un conjunto limitado de nodos (llamados "autoridades") tienen el derecho exclusivo de crear nuevos bloques y validar transacciones. Estas autoridades son seleccionadas por la comunidad en función de su reputación y credibilidad. PoA es altamente eficiente y escalable, pero sacrifica la descentralización en favor de la velocidad y la seguridad.

Prueba de Espacio y Tiempo (Proof of Space-Time - PoST):
PoST es un algoritmo de consenso emergente que combina la capacidad de almacenamiento con la prueba de tiempo para validar transacciones. Los nodos compiten demostrando que han dedicado una cantidad significativa de espacio de almacenamiento y tiempo para participar en la red. PoST busca ser más eficiente energéticamente que PoW al utilizar recursos de almacenamiento subutilizados.

Prueba de Historia (Proof of History - PoH):
Propuesto por Solana, PoH es un algoritmo de consenso que establece un orden temporal de las transacciones utilizando un registro criptográfico secuencial. Esta información de tiempo es utilizada por otros algoritmos de consenso, como PoS, para lograr un consenso más rápido y escalable.

Algoritmo de Consenso	Descripción	Ventajas	Desventajas
Prueba de Trabajo	Los mineros compiten para resolver problemas criptográficos complejos. El primero en encontrar un hash válido para el bloque propuesto agrega el bloque a la cadena.	Alta seguridad, descentralización.	Consumo de energía, escalabilidad limitada.
Prueba de Participación	La probabilidad de minar un bloque está determinada por la cantidad de criptomonedas que posee el nodo y está dispuesto a bloquear como "participación".	Eficiencia energética, menor consumo de recursos.	Posible centralización si se acumula demasiada participación.
Prueba de Autoridad	Un conjunto limitado de nodos (autoridades) tienen el derecho exclusivo de crear nuevos bloques y validar transacciones.	Eficiencia, velocidad de transacción.	Centralización, dependencia de las autoridades.
Prueba de Espacio-Tiempo	Los nodos compiten demostrando que han dedicado una cantidad significativa de espacio de almacenamiento y tiempo para participar en la red.	Utilización eficiente de recursos de almacenamiento.	Requiere tiempo y espacio de almacenamiento significativos.
Prueba de Historia	Establece un orden temporal de las transacciones utilizando un registro criptográfico secuencial. Esta información de tiempo es utilizada por otros algoritmos de consenso.	Consenso rápido y escalable.	Dependencia de un único registro de tiempo, riesgo de manipulación de datos.

+ info

La tabla anterior resume las características principales de cada algoritmo de consenso utilizado en las redes blockchain. Cada algoritmo tiene sus propias ventajas y desventajas, y la elección del algoritmo adecuado depende de los requisitos específicos y los objetivos de la red en cuestión. La seguridad, la eficiencia energética, la escalabilidad y el grado de descentralización son consideraciones clave a tener en cuenta al seleccionar un algoritmo de consenso.

Ejercicio 2: Prueba de Participación (Proof of Stake)

En este escenario, se considera un sistema blockchain que utiliza el algoritmo de Prueba de Participación. En este caso, la probabilidad de forjar un nuevo bloque está determinada por la cantidad de criptomonedas que un validador posee y está dispuesto a apostar. Dado un conjunto de validadores y sus respectivas cantidades de criptomonedas, se solicita determinar la probabilidad de que cada uno sea seleccionado para forjar el próximo bloque.

+ solución

Solución:

```
def proof_of_stake(validators):
    total_coins = sum(validators.values())
    probabilities = {validator: coins / total_coins for
validator, coins in validators.items()}
    return probabilities

# Ejemplo de uso:
validators = {"Validator1": 100, "Validator2": 200,
"Validator3": 150}
probabilities = proof_of_stake(validators)
print("Probabilidades de selección para cada validador:",
probabilities)
```

Prueba de Trabajo (Proof of Work):

El primer código aborda el algoritmo de Prueba de Trabajo (Proof of Work), utilizado en muchas blockchains, incluida Bitcoin. Este algoritmo requiere que los mineros realicen un trabajo computacionalmente costoso para validar y agregar nuevos bloques a la cadena. El objetivo principal es encontrar un nonce (número arbitrario utilizado solo una vez) que, al combinarse con los datos del bloque, produzca un hash que cumpla con ciertos criterios, como tener un número mínimo de ceros al principio.

El código comienza definiendo una función llamada proof_of_work que toma dos parámetros: los datos del bloque y la dificultad deseada para la Prueba de Trabajo. Luego, inicia un bucle while que iterará hasta que se encuentre un nonce válido. En cada iteración, se calcula el hash del bloque concatenando los datos del bloque con el nonce y luego se verifica si el hash cumple con los requisitos de dificultad establecidos. Si el hash cumple con los requisitos, el nonce se devuelve como resultado.

Prueba de Participación (Proof of Stake):

El segundo código se centra en el algoritmo de Prueba de Participación (Proof of Stake), utilizado en algunas blockchains como Ethereum 2.0. En este algoritmo, la probabilidad de forjar un nuevo bloque está determinada por la cantidad de criptomonedas que un validador posee y está dispuesto a apostar en la red. En lugar de realizar cálculos intensivos de energía como en Prueba de Trabajo, Prueba de Participación se basa en el concepto de "apuesta" de criptomonedas.

El código define una función llamada proof_of_stake que toma un diccionario de validadores como entrada, donde cada validador está asociado con la cantidad de criptomonedas que posee. La función calcula la probabilidad de que cada validador sea seleccionado para forjar el próximo bloque en función de la cantidad de criptomonedas que posee en comparación con el total de criptomonedas apostadas en la red.