Algoritmo de Consenso

Vera Catashunga, Alejandro Vidal

Programación Concurrente y Distribuida

November 28, 2021

Tabla de contenidos

Introducción

Todos los días vemos como surgen nuevas tecnologías de blockchain en nuestro medio. No importa cuanto tratamos de captar de la última tecnología, ella siempre tiene algo nuevo que ofrecer. ¿Alguna vez te has preguntado cuál es la raíz de todas estas tecnologías de blockchain? Bueno, los algoritmos de consenso son la raíz principal de esta tecnología revolucionaria. Los algoritmos de consenso son lo que hace que todas estas secuencias de consenso de blockchain sean diferentes una de las otras. La red blockchain cuenta con millones y millones de personas en el mismo espacio. Entonces, ¿por qué no interfieren unas con otras o existen mutuamente?
La respuesta está en la arquitectura de la red blockchain. La arquitectura esta diseñada de forma inteligente y los algoritmos de consenso son el núcleo de esta arquitectura.

Algoritmo de Consenso

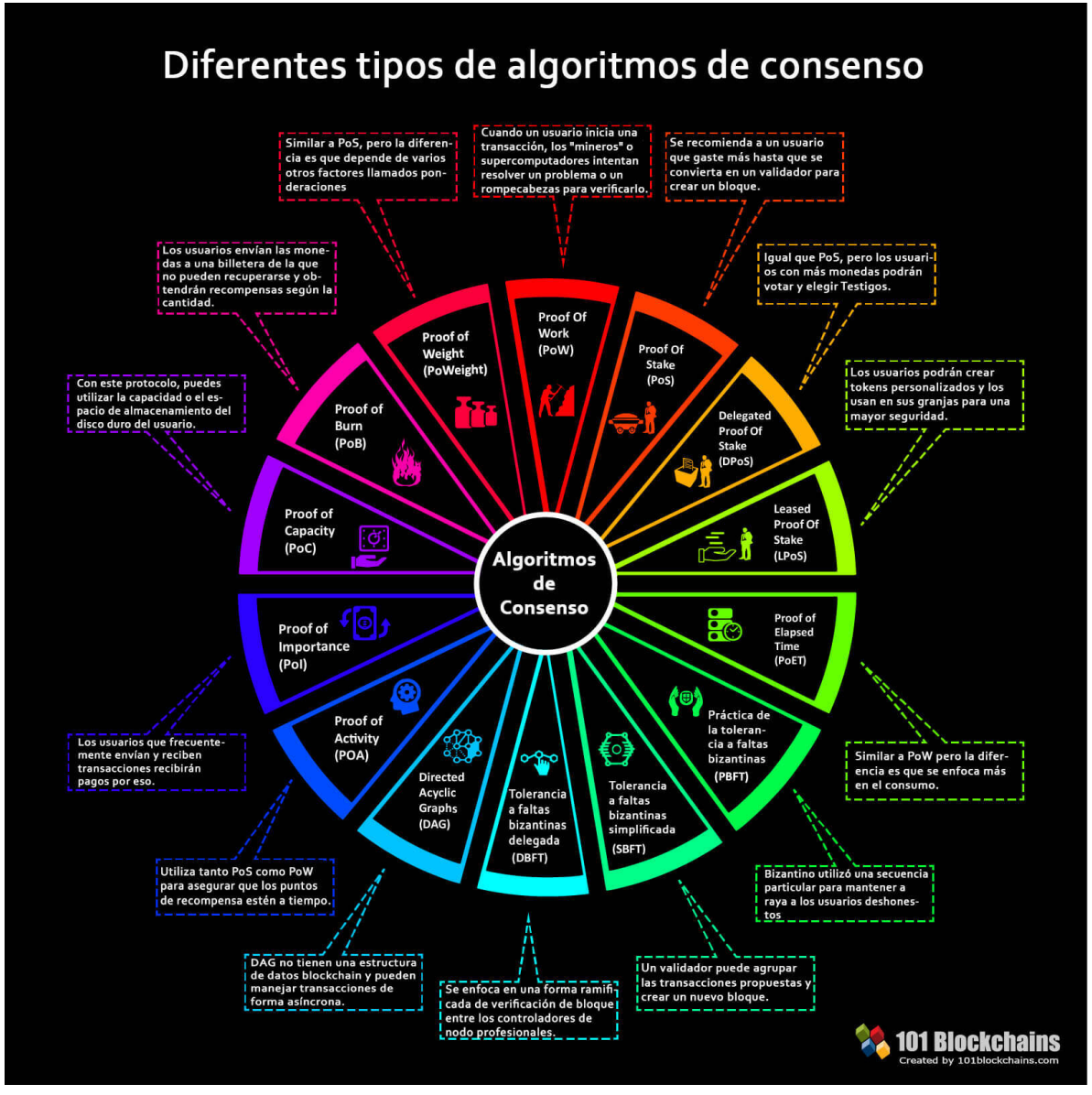
Son procesos de toma de decisiones para un grupo, donde cada individuo dentro del grupo construye y apoya la decisión que funcione mejor para ellos. Es una forma de resolución donde los miembros deben apoyar la decisión mayoritaria, les guste o no.

En términos simples, es solo un método para tomar decisiones dentro de un grupo. Los algoritmos de consenso no solo están de acuerdo con la mayoría de los votos, sino que también están de acuerdo con aquel que los beneficie a todos. Así que, siempre es una victoria para la red.

Estos modelos de consenso de blockchain consisten en algunos objetivos particulares, tales como:

- Llegar a un acuerdo
- Colaborar
- Cooperar
- Igualdad de derechos
- Participación
- Actividad

Diferentes tipos de algoritmos de consenso



El problema con la tolerancia a faltas bizantinas

La tolerancia a faltas bizantinas es un evento particular de fallas. Se le llama problema de los generales bizantinos. La mejor forma de experimentar esa situación es con un sistema informático distribuido. Muchas veces puede haber un mal funcionamiento de los sistemas de consenso.

Estos componentes son los responsables de la información conflictiva. Los sistemas de consenso solo pueden funcionar con éxito si todos los elementos trabajan en armonía. Sin embargo, incluso si uno de los componentes en de este sistema funciona mal, todo el sistema podría fallar.

Los componentes defectuosos siempre causan inconsistencia en el sistema de tolerancia a faltas bizantinas, y es por eso que no es ideal utilizar estos sistemas de consenso para una red descentralizada.

¿Por qué necesitamos algoritmos de consenso?

El problema principal con Bizantino es el poder llegar a un acuerdo. Si se produce un solo fallo, los nodos no podrán llegar a un acuerdo o tendrán un valor de dificultad mayor.

Por otro lado, los algoritmos de consenso no se enfrentan a este tipo de problema. Su objetivo principal es el de alcanzar una meta específica por cualquier medio.

Por eso, cuando podría haber resultados contradictorios en un sistema distribuido; es mejor usar algoritmos de consenso para una mejor salida.

Blockchain: El esqueleto de la organización de datos de la red descentralizada

- Es una nueva forma de organizar la base de datos.
- Puede almacenar todo lo que cambia según la red.
- Todos los datos se ordena en un bloque como materia.

Sin embargo, no veras ninguna descentralización en el mismo blockchain. Esto se debe a que blockchain no proporciona el entorno descentralizado. Es por eso que necesitamos algoritmos de consenso para asegurarnos de que el sistema esté completamente descentralizado.

Por lo tanto, la tecnología blockchain solo permitirá crear una base de datos con estructura diferente, pero no llevará a cabo el proceso de descentralización. Es por esto que blockchain se considera el esqueleto de toda la red descentralizada.

Algoritmos de consenso: El alma de la red

El método es bastante simple en realidad. Estos modelos de consenso de blockchain son solo la forma en la que se llega a un acuerdo. Sin embargo, no puede haber ningún sistema descentralizado sin algoritmos de consenso comunes.

Ni siquiera importará si los nodos confían entre sí o no. Tendrán que ir por ciertos principios y llegar a un acuerdo colectivo. Para hacerlo, tendrán que revisar todos los algoritmos de consenso.

Hasta ahora no hemos encontrado ningún algoritmo específico de blockchain que funcione para cada tecnología de blockchain.

Tipos de algoritmos de consenso

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake(DPoS)
- Proof of Elapsed Time (PoET)
- Práctica de tolerancia a faltas bizantinas
- Tolerancia a faltas bizantinas
- Grafo de acíclico dirigido
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

Proof of Work (POW)

Reconocida por Bitcoin, basado 100% en hardware, donde se compite por resolver algoritmos matemáticos para registrar transacciones dentro de un blockchain.

Fue implementado por primera vez en Bitcoin, pero el concepto en sí existe desde hace cierto tiempo. Los validadores (mineros) someten a hash los datos que desean añadir, hasta que logran producir un solución concreta.

Proof of Stake (POS)

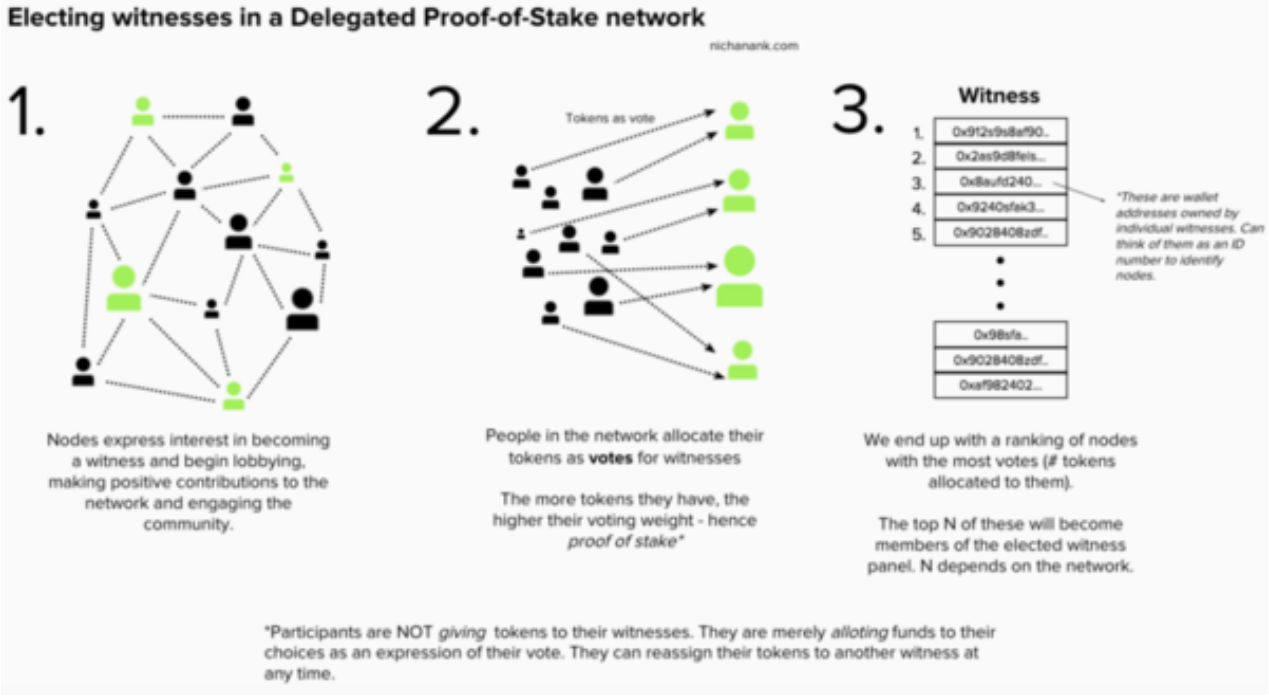
No existe un concepto de mineros, hardware especializado o consumo masivo de energía. En lugar de eso tenemos validadores que deben invertir cierta cantidad de criptomonedas, todo lo que necesitas es una PC normal.

No presentas un recurso externo, sino uno interno: la criptomoneda. Las reglas difieren con cada protocolo, pero generalmente hay una cantidad mínima de fondos que debes tener para ser elegible para el staking.

Comparación entre POW y POS

Delegated Proof of Stake(DPOS)

Los algoritmos de consenso son procesos de toma de decisiones para un grupo, cada individuo dentro del grupo construye y apoya la decisión que funciona mejor para ellos. Es una forma de resolución donde los miembros deben apoyar la decisión mayoritaria.



Proof of Elapsed Time (PoET)

Utiliza la computación confiable para definir aleatoriamente el tiempo de espera para construcción de bloques. La forma en que el protocolo elige al nodo que agregará el próximo bloque requiere menos energía que en POW.

Byzantine Fault Tolerance

Es propio de blockchain privado, una decisión de consenso determinada sobre las bases de las decisiones enviadas por todos, se decide sobre una base de votación.

Proof-of-Activity

El proceso de minería comienza igual que el algoritmo PoW. Los mineros resuelven un problema para obtener una recompensa. En PoW, los mineros extraen bloques que tienen una transacción completa. En Proof-of-Activity, los mineros extraen solo la plantilla de los bloques (información del encabezado, dirección de recompensa para los mineros).

Luego, el sistema se pasa a la PoS. La información del encabezado dentro de un bloque apunta a un inversionista aleatorio, los cuales validan los bloques pre-minados.

Mientras más guarda un validador, más aumentan las posibilidades de que aprueben un bloque. Solo después de la validación, ese bloque particular entra en la blockchain. La red paga a los mineros y validadores la parte justa de las tarifas transaccionales. De este modo, el sistema actúa contra la "tragedia de los comunes" y crea una mejor solución para la validación de bloques.

Proof-of-Importance

El concepto es un desarrollo del Proof-of-Stake. Aunque, NEM introdujo una nueva idea: la recolección o la adquisición. El mecanismo de recolección determina si un nodo es elegible para ser agregado a la cadena de bloques o no. Cuanto más coseche en un nodo, más posibilidades tendrá de agregarse a la cadena. A cambio de la recolección, el nodo recibe las tarifas de transacción que el validador cobra como recompensa. Para poder recolectar, debes tener al menos 10,000 XEM en tu cuenta.

Esto resuelve el mayor problema de la Proof-of-Stake. En PoS, el más rico obtiene más dinero en comparación con los validadores que tienen menos dinero. Por ejemplo, si posees el 20% de las criptomonedas, puedes minar el 20% de los bloques en la red de blockchain. Esto hace que los algoritmos de consenso favorezcan a los ricos.

Proof-of-Capacity

El ejemplo de consenso Proof-of-Capacity es una actualización del famoso protocolo de consenso blockchain Proof-of-Work . La característica esencial de esta es el “plotting”.

Esta misma naturaleza hace que el sistema sea más rápido el PoW. La Proof-of-Capacity puede crear un bloque en solo cuatro minutos, mientras que la Proof-of-Work toma diez minutos para hacer lo mismo. Además, trata de abordar el problema de hash del sistema de PoW. Cuantas más soluciones o planes tenga en su computadora, mayores serán sus posibilidades de ganar la batalla minera.

Proof-of-Burn

Para salvaguardar las criptomoneda de PoW, una parte de las monedas serán quemadas. El proceso ocurre cuando los mineros envían unas pocas monedas a una "Eater Address". Las Eater Address no pueden gastar estas monedas en ningún propósito. Un registro realiza un seguimiento de las monedas quemadas haciéndolas realmente imposibles de usar. El usuario que quemó las monedas también recibirá una recompensa.

Sí, la quema es una pérdida. Pero el daño es temporal ya que el proceso protegerá las monedas a largo plazo de los piratas informáticos y de sus ataques cibernéticos. Por otra parte, el proceso de quemarlas aumenta las apuestas de las monedas alternativas. Tal escenario aumenta la posibilidad de que un usuario extraiga el siguiente bloque mientras aumenta sus recompensas en el futuro. Así que, la quema podría ser usada como un privilegio minero.

Proof-of-Weight

Esta es una gran actualización del algoritmo Proof-of-Stake. En el Proof-of-Stake, mientras más fichas tengas, más posibilidades tendrás de conseguir más, lo que hace que el sistema sea un poco parcial. El Proof-of-Weight intenta resolver la naturaleza tan parcial de los PoS. Las criptomonedas como Algorand, Filecoin y Chia implementan el PoWeight. Considera algunos otros factores además de poseer más monedas como en PoS.

Estos factores se identifican como los "Factores ponderados". Por ejemplo, Filecoin considera la cantidad de datos de IPFS que tienes y evalúa ese factor. Algunos de los otros factores incluyen, pero no se limitan, a la Proof-of-Spacetime y la Proof-of-Reputation.

Las ventajas fundamentales de este sistema incluyen personalización y escalabilidad. Aunque incentivar podría ser un gran desafío para este algoritmo de consenso.

Conclusiones

- Los algoritmos de consenso hacen que la naturaleza de las redes blockchain sean tan versátiles. No hay un solo algoritmo de consenso blockchain que pueda afirmar que es perfecto, pero esa es la belleza de la tecnología que poseemos; el cambio constante para mejorar.
- Si estos algoritmos de consenso no estuvieran allí, tendríamos que depender de la Proof-of-Work. Te guste o no, el PoW amenaza la descentralización y la naturaleza distribuida de las blockchains.
- Proof of Work sigue siendo la oferta dominante, es la alternativa más confiable y más segura. Dicho esto, hay una enorme cantidad de investigación y desarrollo en reemplazos para PoW.
- Toda la idea de la tecnología blockchain es la descentralización y la lucha contra la monarquía. Ya es hora de que la gente común detenga el sistema corrupto y defectuoso.

Referencias

- https://www.youtube.com/watch?v=qd2edK9pw68
- https://www.youtube.com/watch?v=z4R0TRLRaEc&t=86s
- https://www.youtube.com/watch?v=gJaQ1n0D_SI
- https://101blockchains.com/es/algoritmos-de-consenso-blockchain/