Solana: Un nuevo paradigma en las tecnologías Blockchain

1st Jhonier Jiménez
Facultad de Ingeniería
Universidad de Antioquia
Medellín, Colombia
jhonier.jimenez@udea.edu.co

***Abstract*—Desde la publicación del whitepaper de Satoshi Nakamoto en 2008, el cual llevó a la aparición de Bitcoin en el año 2009, las tecnologías blockchain han llegado para cuestionar nuestro entendimiento del mundo financiero. Sin embargo, estas tecnologías presentan problemas inherentes a su naturaleza, que han limitado su expansión e implementación en las industrias. Esta investigación explora los principales problemas del ecosistema blockchain y cómo Solana se presenta a sí misma como una solución; principalmente al problema de escalabilidad y al uso excesivo de recursos. Se examinarán los factores que han contribuido a su creciente popularidad; a través de un recorrido por los fundamentos de Solana, analizando en detalle su arquitectura y el funcionamiento de su protocolo de consenso Proof of History que aparece como un nuevo paradigma en el mundo Blockchain.**

***Pálabras clave*—blockchain, escalabilidad, proof of history, styling, insert**

1. Introducción

Introducidas en 2009 junto con Bitcoin, las tecnologías blockchain ofrecen una metodología diferente para registrar y verificar transacciones. A diferencia de los sistemas centralizados tradicionales, las tecnologías blockchain utilizan un sistema distribuido, donde la información se almacena públicamente en una red de computadoras, eliminando así la necesidad de una autoridad única. Este enfoque descentralizado fomenta la confianza y la inmutabilidad, dado que los datos no son fácilmente manipulables después de haber sido agregados a la cadena de bloques.

Pero a pesar de su potencial y la revolución que han generado en el mundo financiero; las limitaciones inherentes al ecosistema Blockchain -conocidas como el "Trilema de Blockchain"- han obstaculizado la adopción generalizada en diversas industrias. Y a medida que crece la demanda de soluciones blockchain, la necesidad de soluciones innovadoras que aborden estos desafíos se vuelve cada vez más crítica.

Así mismo, las últimas décadas han traído consigo nuevos desafíos para la humanidad; entre ellos, uno de los más importantes es el cambio climático. Y es en este sentido que ya se escuchan voces cuestionando el uso de las tecnologías Blockchain, principalmente Bitcoin, por su alto consumo energético a través de millones de computadoras en la red buscando completar procesos de minado de transacciones para obtener beneficios en esta criptomoneda.

2. El trilema Blockchain

Este concepto fue introducido inicialmente por Vitalik Buterin, cofundador de Ethereum. Y lo describe como la dificultad de lograr simultáneamente los tres pilares fundamentales de las redes Blockchain: Seguridad, Descentralización y Escalabilidad [4]. La regla del trilema establece entonces que, sólo dos de estos objetivos pueden alcanzarse simultáneamente. Por lo tanto, el trilema representa los desafíos no resueltos actuales de la tecnología blockchain en cuanto a su usabilidad y adopción generalizada. Particularmente, la escalabilidad limitada reduce la facilidad de uso y el potencial de una plataforma blockchain para soportar una base de usuarios en crecimiento [3].

A. Descentralización

La descentralización es un principio fundamental en las tecnologías blockchain, que se refiere a la capacidad de distribuir la red entre numerosos nodos; en lugar de depender de un solo punto de autoridad, como ocurre en muchos sistemas centralizados; permitiendo así que la red funcione de manera distribuida y democrática. Esta característica esencial impide entonces que una única entidad ejerza un control excesivo o tenga una influencia dominante sobre el sistema. [3]

B. Escalabilidad

La escalabilidad en el mundo blockchain se refiere a la capacidad de un sistema para manejar un mayor volumen de transacciones sin sacrificar su rendimiento. En otras palabras, un blockchain escalable puede procesar más transacciones por segundo (TPS) manteniendo tiempos de espera razonables y costos bajos. La escalabilidad es un desafío importante para las blockchains, al igual que para otras tecnologías como las bases de datos. [2]

Cuando una red blockchain se congestiona por un alto número de transacciones, se presentan problemas que afectan la confianza de usuarios e inversionistas:

- Transacciones lentas: La red no puede procesar todas las transacciones de inmediato, generando tiempos de espera prolongados.
- Aumento de tarifas: Los mineros priorizan las transacciones con comisiones más altas, lo que incrementa significativamente el costo para confirmar una transacción en un tiempo aceptable.

C. Seguridad

La seguridad en el contexto Blockchain es un concepto muy amplio, pero de manera general una red Blockchain segura debe mínimamente contener los siguientes elementos:

1) Consistencia: En las tecnologías Blockchain, la consistencia se refiere a que todos los nodos de la red tengan una copia idéntica del libro mayor al mismo tiempo. Existen dos modelos de consistencia:

- Consistencia eventual: Las actualizaciones de datos se propagan eventualmente a todos los nodos, pero puede haber un retraso. Es posible leer datos desactualizados durante este tiempo.
- Consistencia fuerte: Todos los nodos tienen el mismo libro mayor en todo momento. Las operaciones de lectura/escritura deben esperar a que se confirme la actualización antes de continuar. Este modelo es más lento pero más seguro.

2) Resistencia a la manipulación: Una red Blockchain es resistente a la manipulación de los datos de sus transacciones por dos razones:

- Firma digital: Cada transacción está firmada por el usuario que la envía, lo que permite verificar su autenticidad.
- Funciones hash criptográficas: Los bloques del Blockchain están encadenados mediante hash criptográficos. Cualquier intento de modificar un bloque se detectará fácilmente debido a la inconsistencia con los bloques anteriores y posteriores.

3) Resistencia a ataques DDoS: Gracias a su naturaleza descentralizada, las redes Blockchain deben ser resistentes a ataques DDoS que intenten sobrecargar la red e interrumpir el servicio. Un atacante necesitaría controlar una gran parte de la red para tener éxito, lo cual es cada vez más difícil a medida que la red crece.

4) Resistencia al double spending: El gasto doble es un ataque específico de las monedas digitales donde se gasta la misma moneda dos veces. Las redes Blockchain normalmente evitan esto mediante la implementación de:

- Registro de transacciones: Todas las transacciones se registran en el Blockchain, lo que permite verificar públicamente si una moneda ya se ha gastado.
- Firma digital: Cada transacción está firmada por el usuario que la envía, evitando la falsificación.

5) Resistencia a ataques del 51%: Un ataque del 51% ocurre cuando un minero o grupo de mineros maliciosos controlan más del 50% de la potencia de cómputo de la red. Esto teóricamente les permitiría realizar acciones como gastar dos veces sus monedas o revertir transacciones legítimas.

6) Pseudonimato: Las direcciones en las redes Blockchain deben ser seudónimas, y funcionar como un alias que no revele la identidad real del usuario, aunque sí permitir cierto rastreo si se analiza la actividad en la red.

En la realidad, el trilema de seguridad, escalabilidad y descentralización en las tecnologías blockchain, se encuentra materializado incluso en las redes más importantes como Bitcoin y Ethereum:

> "Por ejemplo, las blockchains públicas sin permisos como Bitcoin permiten que cualquiera participe activamente y mantenga la red. Por lo tanto, están razonablemente descentralizadas debido a la gran cantidad de diferentes participantes y, gracias al uso del mecanismo de consenso Proof of Work, también son seguras contra ataques maliciosos como la Falla Bizantina (Nakamoto, 2008). Sin embargo, sufren limitaciones de escalabilidad, lo que se traduce en tiempos de transacción más largos y tarifas más altas durante períodos de alta demanda (Zhou et al., 2020).
>
> Por el contrario, las blockchains privadas con permisos, como Hyperledger Fabric, solo permiten que se unan participantes seleccionados y restringen aún más la capacidad de mantener la red. Esto reduce la descentralización de la red y también la seguridad mediante el uso de mecanismos de consenso menos robustos como Proof of Authority, que son vulnerables a ataques maliciosos y, en algunos casos, ni siquiera son resistentes a la indisponibilidad de participantes individuales de la red, también conocido como Crash Fault Tolerant (Ekparinya et al., 2019). Esto reduce la complejidad de agregar nuevas transacciones al libro mayor, lo que da como resultado un mayor rendimiento de transacciones y una menor latencia de red para una mejor escalabilidad (Guggenberger et al., 2022).
>
> Estos ejemplos ilustran la tensión que enfrentan las soluciones blockchain actuales y que actualmente se pueden alcanzar dos de las tres dimensiones, pero no las tres al mismo tiempo." [3]

3. Implementación de Soluciones

Es claro entonces que las redes blockchain son muy diferentes a las entidades de confianza centralizadas tradicionales y han sido una alternativa a los sistemas financieros existentes; Al ofrecer un sistema peer-to-peer y una gestión descentralizada de transacciones que son escritas en bloques inmutables y transparentes para todos los nodos. Pero los problemas presentados afectan directamente la confianza de los usuarios y las compañías que invierten sus recursos y esfuerzos en las tecnologías Blockchain.

Particularmente, y a medida que se ha incrementado su popularidad y su valor comercial, el problema de la escalabilidad ha tomado gran importancia en estas redes. Y es que, cuando un gran número de usuarios intentan realizar transacciones simultáneamente, la red se satura, provocando retrasos y aumentando los costos como lo hemos visto en plataformas como Bitcoin y Ethereum.. Y ante esta situación, los mineros empiezan a seleccionar las transacciones que ofrecen una tarifa más alta. Como consecuencia, las tarifas que se deben pagar a los mineros para confirmar la transacción aumentan considerablemente. A veces se puede requerir una tarifa 100

veces mayor que el promedio para tener las transacciones confirmadas según las expectativas del usuario en términos de tiempos de espera.[2]

En este contexto, se han propuesto muchas soluciones, como bases de datos centralizadas y computación en la nube para gestionar grandes volúmenes de información. Así como la aparición constante de nuevas redes basadas en Blockchain que resultan de estudios realizados por empresas y equipos de investigación que buscan crear soluciones capaces de manejar situaciones de alta afluencia de usuarios. Algunas de las estrategias más implementadas son:

- Aumento del tamaño de bloque: Esta estrategia busca incrementar la capacidad de la red permitiendo almacenar más transacciones por bloque. Si bien es una solución simple, tiene sus desventajas. Aumentar excesivamente el tamaño de los bloques puede dificultar la participación de nodos con menor capacidad computacional en la red, afectando su descentralización.
- Compresión de bloque: En lugar de aumentar el tamaño del bloque, se explora la posibilidad de comprimir la información contenida en él. Mediante técnicas de criptografía y codificación eficientes, se puede almacenar la misma cantidad de transacciones en un espacio menor. Esto permitiría mantener la participación de nodos con recursos limitados.
- Sharding (Fragmentación): Esta técnica divide la red blockchain en múltiples sub-redes o "shards". Cada shard procesa un conjunto independiente de transacciones, aumentando la capacidad de procesamiento general de la red. Los usuarios interactúan con el shard correspondiente a su transacción, mejorando la eficiencia.
- Mejora de los algoritmos de consenso: Los algoritmos de consenso son el mecanismo por el cual la red blockchain valida las transacciones y asegura su inmutabilidad. Algunos algoritmos, como Proof of Work (PoW), utilizados en Bitcoin, son computacionalmente costosos y lentos. Algunas investigaciones se han centrado en desarrollar algoritmos de consenso más eficientes, que permitan procesar transacciones con mayor rapidez sin comprometer la seguridad.

Pero como se ha presentado, si bien estas soluciones mejoran la escalabilidad del sistema, también sacrifican otras dos propiedades fundamentales de la cadena de bloques: su descentralización y seguridad. Al optar por soluciones que priorizan la escalabilidad, es posible que se debilite la descentralización al centralizar ciertas funciones o al aumentar el riesgo de ataques debido a la reducción de medidas de seguridad.

4. Solana

En su whitepaper "A new architecture for a high performance blockchain", Anatoly Yakovenko presenta oficialmente a Solana en el año 2017. Y desde su aparición, se ha consolidado como uno de los sistemas blockchain más grandes de la actualidad. Esta afirmación se sustenta en métricas clave como la cantidad de direcciones activas, el volumen diario de transacciones y la multimillonaria capitalización de mercado de su token nativo, SOL.

Más que solo una mejora a las redes blockchain existentes, Solana propone un nuevo paradigma con el que busca solucionar el problema de la escalabilidad sin comprometer la seguridad o la descentralización. Esto a través de un mecanismo denominado como "Proof of History" en combinación del ya bien conocido Proof of Stake el cual es ampliamente utilizado en las redes blockchain como Ethereum. En palabras de Anatoly Yakovenko:

> "El blockchain es una implementación de una máquina de estado replicada tolerante a fallos. Las cadenas de bloques públicas disponibles actualmente no dependen del tiempo, o asumen débilmente la capacidad de los participantes para mantener la hora. Cada nodo en la red usualmente confía en su propio reloj local sin conocimiento de los relojes de ningún otro participante en la red. La falta de una fuente confiable de tiempo significa que cuando se usa la marca de tiempo (timestamp) de un mensaje para aceptar o rechazar un mensaje, no hay garantía de que todos los demás participantes en la red tomarán exactamente la misma decisión. El PoH (Proof of History) presentado aquí está diseñado para crear un registro con paso de tiempo verificable, es decir, la duración entre eventos y el orden de los mensajes. Se anticipa que cada nodo en la red podrá confiar en el paso del tiempo registrado en el libro mayor sin necesidad de confianza."

5. La importancia de la medición del tiempo

Como podemos notar entonces, desde Bitcoin hasta las redes Blockchain más recientes, una de las grandes preguntas que se deben hacer todas las implementaciones de esta tecnología es: ¿Qué hora es en realidad?.

Para las redes blockchain, el tiempo es crucial por varias razones:

1) Inmutabilidad: Como característica fundamental del Blockchain, es necesario garantizar la inmutabilidad de los datos que se almacenan en la red; y para lograr esto se hace necesario tener un registro preciso del tiempo en que se agregó cada bloque a la cadena. Previniendo así la manipulación de los datos y manteniendo la integridad del historial de transacciones.

2) Orden de las transacciones: Las redes Blockchain procesan las transacciones en un orden específico, y este orden es crucial para evitar el doble gasto y garantizar la validez de las transacciones. El tiempo se utiliza para determinar el orden en que se reciben las transacciones y para garantizar que se procesen en la misma secuencia por todos los nodos de la red.

3) Sincronización de la red: Los nodos de una red blockchain deben estar sincronizados entre sí para mantener un registro coherente de la cadena de bloques. El tiempo en este sentido se utiliza para garantizar que todos los nodos estén de acuerdo en la hora en que se agregaron los bloques a la cadena

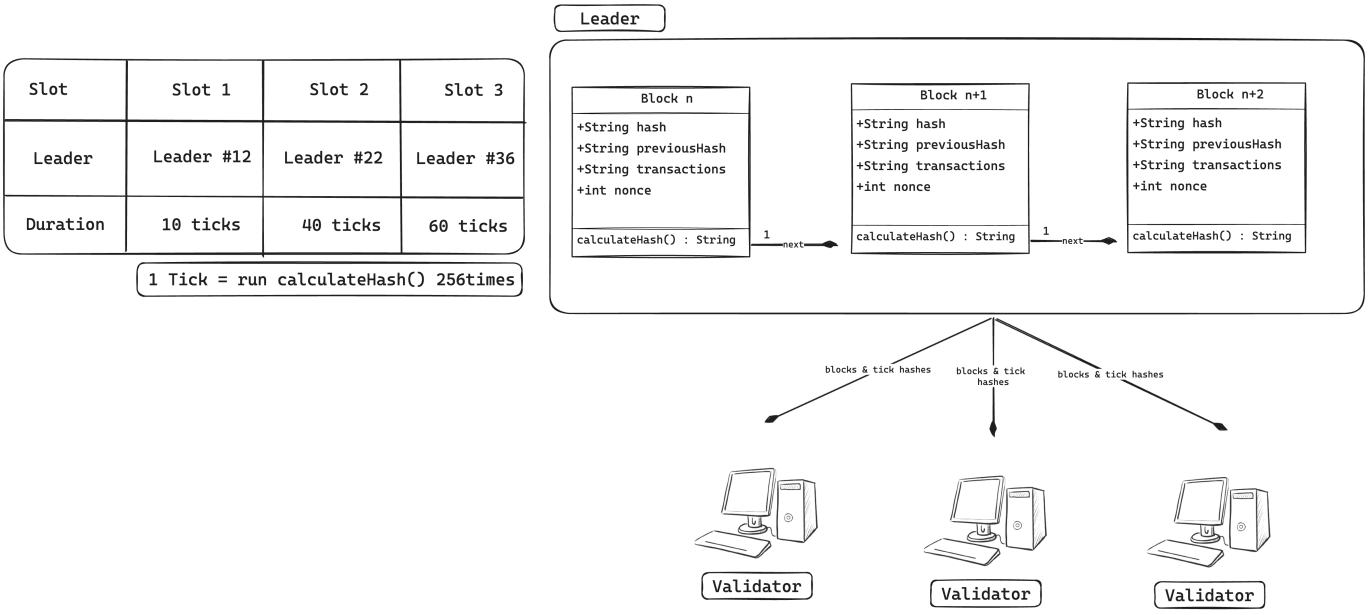

Fig. 1. Arquitectura Leader-Validator de Solana

y en el orden de las transacciones. Evitando así bifurcaciones en la red y manteniendo la integridad de la cadena de bloques.

4) Smart Contracts: Los smart contracts pueden utilizar el tiempo para desencadenar eventos, como la liberación de fondos o la ejecución de acciones, en función de un horario o de condiciones específicas.

6. Dificultades para determinar el tiempo

Desde su diseño, las redes como Bitcoin preservan el orden de los eventos; Sin embargo, la precisión en términos de tiempo de dichos eventos es cuestionable, a pesar de que cada bloque tiene un timestamp asociado. En la práctica, los timestamps de Bitcoin pueden diferir de la hora real mantenida por los nodos participantes de la red, y en teoría, podrían diferir radicalmente de la hora real fuera de la red Bitcoin dado que cada nodo que procesa transacciones en esta red descentralizada tiene su propio reloj interno en el que se basa para funcionar. Con miles de nodos en todo el mundo, puede haber ligeras discrepancias entre los relojes de los sistemas locales. Esto se vuelve problemático cuando la red descentralizada necesita llegar a un consenso sobre qué transacciones han tenido lugar y, más específicamente, el orden temporal en el que ocurrieron.

Por lo que, de manera efectiva, estos protocolos no permiten determinar la hora exacta con precisión [12], lo que desencadena ciertos problemas al momento de leer los timestamps:

1) Brechas: Una brecha ocurre principalmente por tiempo de espera agotado ó timeout, que puede deberse a una congestión en la red o a problemas de conexión del propio dispositivo. Lo que resulta en una diferencia de tiempo entre dos bloques consecutivos.

2) Bifurcaciones en la Cadena de Bloques: Una bifurcación ocurre cuando dos bloques diferentes son minados sobre el mismo bloque anterior. En este caso, existen dos versiones distintas de la blockchain. Inicialmente, la red no está segura de cuál de los bloques será incluido en la cadena final y, por lo tanto, debe determinar qué cadena será aceptada y continuada. Dado que, los pares solo aceptan uno de los bloques y lo incluyen en la blockchain, mientras que el otro bloque es descartado.Este fenómeno genera una incertidumbre temporal hasta que se resuelva cuál cadena prevalecerá.

3) Timestamp Reset: Tradicionalmente, se supone que el timestamp de un bloque representa el momento en que el minero recibe el bloque anterior. Sin embargo, esta suposición no siempre es válida. Algunos mineros pueden optar por ”reiniciar” el timestamp durante el proceso de minería, ajustándolo a la hora actual.

Si bien dentro de las redes como Bitcoin existen herramientas para dar solución a estos problemas en la medición del tiempo, como mecanismos de consenso, selección de la cadena más larga y un tercero “confiable”. La implementación de las mismas afecta el rendimiento de la red, el costo computacional y todos los costos asociados a la minería.

La medición del tiempo en Solana

La red de Solana utiliza un sistema de unidades de tiempo para coordinar su funcionamiento. Estas unidades nos permiten entender el tiempo en el que se procesan las transacciones y cómo se avanza en el estado del blockchain:

4) Hash: Solana se basa en la suposición de que cada participante de la red puede generar alrededor de 2.000.000 de hashes por segundo. Esta cifra se eligió tomando como referencia la potencia de procesamiento de un hardware específico (Intel Xeon e5-2520 v4).

5) Tick/Slot: Un tick es una unidad fundamental que representa 12.500 hashes. Funciona como una marca de tiempo

dentro del registro distribuido de Solana. En base a la tasa de hash asumida, un tick ocurre aproximadamente cada 400 milisegundos (ms). Este periodo también define la ventana temporal en la que se espera que el validador líder cree un nuevo bloque. Durante este tiempo, el líder debe recopilar y procesar las transacciones para incluirlas en el bloque.

6) Época (Epoch): Siguiendo la misma lógica de la tasa de hash, una época en Solana dura aproximadamente dos días. Se define como un conjunto de 432.000 slots. Las épocas son útiles para tareas de creación de bloques y mantenimiento de la red que se programan para ocurrir a intervalos regulares.

Proof of History

El concepto de Proof-of-History o PoH introduce una nueva forma de medir el tiempo dentro de una red blockchain descentralizada. En lugar de confiar en una fuente de tiempo centralizada, susceptible a fallos o manipulaciones, Proof of History utiliza el tiempo que toma la creación de una cadena de hash para crear un registro cronológico inviolable. Imaginemos esta cadena como una fila de dominós perfectamente alineados. Cada dominó representa un bloque en la cadena y su cara frontal contiene el resultado de aplicar una función hash especial al bloque anterior. Esta función, similar a una huella digital, genera una salida única a partir de cualquier entrada de datos. Lo crucial es que la función hash es unidireccional, es decir, no hay forma de recuperar los datos originales a partir del resultado (el hash).

La clave de PoH reside entonces en la limitación de la velocidad de cálculo de esta función para la creación de una cadena de hashes. El hardware más potente sólo puede generar hashes a un ritmo determinado; lo cual establece un límite superior global para la tasa de creación de la cadena hash.

En otras palabras, sin importar las capacidades computacionales para generar por ejemplo, una cadena de 100 hashes, no es posible hacer la distribución de esta tarea en diferentes hilos, dado que cada hash depende del resultado anterior para poder ser generado. Lo que obliga entonces al líder a "esperar" su turno para crear el bloque mientras genera la cadena de hashes que luego serán verificados; creando así un sistema global para la medición del tiempo dentro de la red.

En ese sentido, y dado que la generación de la cadena de hashes se lleva a cabo mediante una sola máquina y un sólo hilo; tenemos como consecuencia también que la velocidad del sistema aumentará de acuerdo con la Ley de Moore, la cual establece que la capacidad de procesamiento de los microchips se duplica aproximadamente cada dos años. En otras palabras, a medida que el hardware de computación se vuelva más rápido, el rendimiento del sistema de Solana también mejorará de manera proporcional [2].

Esta cadena de hash se usa entonces como un reloj global para cada validador en la red. Cada nodo puede estimar cuándo le toca producir bloques según el calendario preestablecido. Además, los líderes pueden demostrar a otros que ha transcurrido el tiempo suficiente para la creación de un bloque, proporcionando una parte (o la totalidad) de la cadena hash correspondiente.

Proof of History ofrece varias ventajas sobre los métodos tradicionales de consenso basados en el Proof of Work En primer lugar, elimina la necesidad de una carrera computacional que consume mucha energía, como ocurre con Proof of Work. Y en segundo lugar, hace frente a los problemas que se presentan en la red cuando no se establece el tiempo dentro de la misma.

Arquitectura de Solana

En la práctica, Solana no solo utiliza el Proof of History, sino que combina este con el uso del Proof of Stake para la selección de un líder entre los validadores en la red.(Fig. 1.)

Validator

Un validador es un nodo que participa activamente en la red Solana y que adicionalmente tiene un papel especial en la misma. Se les puede considerar la columna vertebral de Solana, ya que son responsables de:

7) Reenvío de transacciones: Los validadores actúan como intermediarios entre los usuarios y el líder actual (el nodo encargado de producir el siguiente bloque). Al recibir una transacción de un usuario, el validador la reenvía al líder para su procesamiento.

8) Validación de bloques: Una vez que el líder crea un bloque, los validadores lo verifican para garantizar su validez. Esto implica comprobar que las transacciones incluidas en el bloque sean legítimas así como la integridad del propio bloque.

9) Validación de la cadena de Hashes: Los nodos encargados de la validación también son responsables de verificar los hashes generados en los ticks del líder, para de esta manera asegurar que el líder generó los bloques en el momento correspondiente.

10) Voto sobre bloques: Cada validador tiene poder de voto proporcional a la cantidad de tokens SOL que tiene (staking). Utilizan este poder de voto para aprobar o rechazar los bloques propuestos por el líder. Un voto mayoritario (¿ 2/3 del stake total) sobre un bloque específico lo finaliza, lo que significa que se considera permanente y no se puede revertir.

Este sistema garantiza que los validadores tengan un gran interés en actuar con honestidad, ya que un comportamiento malicioso podría resultar en la pérdida de su poder de voto y, por lo tanto, de sus potenciales recompensas como validadores de la red.

En ese sentido entonces, en la red de Solana, un bloque se considera finalizado cuando cumple alguna de las siguientes condiciones:

- Supermayoría: cuando un bloque recibe el voto de una supermayoría (más del 66% del staking total) en un intervalo determinado.
- Bloque "viejo": Si un bloque ha recibido más de 32 votos a favor en un tiempo determinado (lo que se traduce en un tiempo de bloqueo excesivamente largo), se considera finalizado y no puede ser revertido.

Leader

La red de Solana opera en ciclos temporales llamados ”épocas”. Al inicio de cada época, entre los validadores, se define un calendario de líderes que asigna a cada uno de ellos un conjunto de ”slots” (espacios para bloques) en los que tendrá la responsabilidad de producir bloques.

Esta selección de líderes no es aleatoria. Para garantizar la seguridad y descentralización de la red, se utiliza un sistema basado en el Proof of Stake de cada validador. La apuesta representa la cantidad de tokens SOL que el validador bloquea en la red para participar en la validación. De esta forma se crea un índice ponderado, donde cada validador ocupa una posición. El peso de su posición en el índice está determinado por el tamaño de su stake. Cuanto mayor sea, mayor será su peso y, por tanto, su probabilidad de ser seleccionado como líder para un slot determinado.

Sin embargo, y para evitar la centralización del poder, Solana implementa también un sistema de equilibrio en la distribución del stake entre los validadores. De esta forma, se garantiza que el poder de validación esté repartido de manera justa y que la red mantenga su descentralización y resistencia a manipulaciones.

Al asignar slots de manera probabilística basada en la participación, y el equilibrio, se fomenta una distribución equitativa de la producción de bloques entre los validadores, lo que ayuda a prevenir centralizaciones.

Paralelización de la validación

Tal como se ha descrito, no es posible para un leader hacer una paralelización al crear la cadena de hashes, debido a que cada nuevo hash depende del anterior. En Solana, los Verificadores utilizan la paralelización para verificar que el Líder haya actuado honestamente. De hecho, el Proof of History puede ser verificado por una computadora de múltiples núcleos en un tiempo significativamente menor al tiempo requerido por el Líder para generarla, al llevar segmentos de la cadena de hashes a cada núcleo. Asegurando así la escalabilidad de la red y mejorando el rendimiento de todo el sistema.

Tiempos de minado y costos

Solana tiene un tiempo de creación de bloques de 410 milisegundos, lo que representa una enorme mejora en el rendimiento si lo comparamos con Ethereum y sus 10 segundos para la creación de un mismo bloque, ó Bitcoin con sus 10 minutos. Así mismo, Anatoly Yakovenko afirma que su red es capaz de alcanzar un rendimiento de 710,000 transacciones por segundo, lo cual es alrededor de 30 veces las 23,666 transacciones que puede manejar Visa.

Como consecuencia, las tasas que se deben pagar a los mineros para completar una transacción en un tiempo determinado se ven altamente incrementadas, llegando en algunos casos a ser 100 veces más de su valor promedio regular como ya ha sucedido en la historia de Bitcoin o Ethereum.

Comunidad de desarrollo y el medioambiente

Otros factores con los que podemos explicar la popularidad de Solana en los últimos años son tales que, a diferencia de redes Blockchain como Ethereum; los smart contracts de Solana pueden ser escritos en cualquier lenguaje de programación que pueda ser compilado y llevado a bytecode utilizando la Low Level Virtual Machine. Lo que hace más fácil la adaptación de la red por parte de la comunidad de desarrolladores.

Así mismo, los problemas medioambientales y de costos generados por la minería en redes blockchain como Bitcoin y su pérdida de trabajo computacional inherente a su Proof of Work, generan interés por parte de la comunidad Blockchain en general.

Conclusión

El enfoque utilizado por Solana para la escalabilidad sin poner en riesgo la seguridad y la descentralización del sistema, no solo se basa en el mejoramiento del hardware, sino también en una arquitectura de software diseñada específicamente para maximizar el rendimiento. Su combinación de Proof of History y Proof of Stake para lograr un consenso rápido y eficiente, le permite procesar un gran número de transacciones por segundo con tiempos de espera cortos y tarifas bajas. Esto la diferencia de otras redes blockchain como Bitcoin y Ethereum, que sufren de congestión y altos costos de transacción.

References

[1] Anatoly Yakovenko. Solana: A new architecture for a high performance blockchain v0. 8.13. Whitepaper (October 2018).

[2] Giuseppe Antonio Pierro; Roberto Tonelli; Can Solana be the Solution to the Blockchain Scalability Problem?. (2022)

[3] Principato, Marc; Babel, Matthias; Guggenberger, Tobias; Kropp, Julius; and Mertel, Simon, ”Towards Solving the Blockchain Trilemma: An Exploration of Zero-Knowledge Proofs”. (2023)

[4] Vitalik. Buterin. The Limits to Blockchain Scalability. (2021)

[5] J Sliwinski; Q Kniep; R Wattenhofer; F Schaich. Halting the Solana Blockchain with Epsilon Stake

[6] Rui Zhang; Rui Xue. Security and Privacy on Blockchain

[7] Javad Zarrin; Phang Hao Wen; Lakshmi Babu Saheer; Bahram Zarrin. Blockchain for decentralization of internet: prospects, trends, and challenges

[8] Ozili PK. Decentralized finance research and developments around the world.

[9] Saurabh Singh; A. S. Sanwar Hosen; B. Yoonlockchain. Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network

[10] P. Szalachowski, ”(Short Paper) Towards More Reliable Bitcoin Timestamps,”. (2018)

[11] E. Regnath, N. Shivaraman, S. Shreejith, A. Easwaran and S. Steinhorst, Blockchain, what time is it? Trustless Datetime Synchronization for IoT. (2020)