NKN: una red descentralizada escalable autodesarrollada y autoincentivada

NKN Lab
www.nkn.org
(Fecha: 13 de marzo de 2018 Versión: 1.0)

NKN (New Kind of Network) es una nueva generación de infraestructura de red blockchain altamente escalable, autodesarrollada y autoincentivada. NKN aborda la descentralización de la red y la autoevolución mediante la introducción de la metodología Cellular Automata (CA) [1, 2] tanto para el dinamismo como para la eficiencia. NKN recompensa la conectividad de la red y la capacidad de transmisión de datos con una prueba de trabajo nueva y útil. NKN se centra en la descentralización de los recursos de red, de forma similar a Bitcoin [3] y Ethereum [4], que descentralizan la potencia, y también similar a IPFS [5] y Filecoin [6], que descentralizan el almacenamiento. Todos ellos, forman los tres pilares de la infraestructura de Internet para los sistemas blockchain de próxima generación. Finalmente, NKN permite que la red sea más descentralizada, eficiente, ecualizada, robusta y segura, lo que augura un Internet más seguro y abierto.

CONTENIDO

1. Desafíos 2
- 1.1. Limitaciones de las redes P2P 2
- 1.2. Utilización de recursos 2
- 1.3. Neutralidad de red y fragmentación 2

2. Visión 2
- 2.1. Objetivos de NKN 2
- 2.2. El tercer pilar: creación de redes 3
- 2.3. Componentes elementales 3
- 2.4. Kit de herramientas de redes para un desarrollo DApp rápido y sin dolor 4

3. Fundamentos tecnológicos 4
- 3.1. Autómatas celulares 4
- 3.2. Reglas como fórmulas 5

4. Nuevo tipo de red 5
- 4.1. Red descentralizada de próxima generación 5
- 4.2. Una prueba útil de trabajo 6
- 4.3. Topología de red y enrutamiento 6
  - 4.3.1. Dinámica 7
  - 4.3.2. Autoorganización 7
  - 4.3.3. Auto-Evolución 8
- 4.4. Descentralización eficiente 8

5. Consenso accionado por autómatas celulares 8
- 5.1. Consenso de la corriente principal 8
- 5.2. Consenso accionado por autómatas celulares 9
  - 5.2.1. Problema de escalabilidad de BFT y PBFT 9
  - 5.2.2. Consenso en los autómatas celulares descrito por Ising Model 9
  - 5.2.3. Ising Model 9
  - 5.2.4. Enlace entre los autómatas celulares y el modelo Ising 10
  - 5.2.5. Autómatas cel. de voto mayoritario como algo. de consenso 10
  - 5.2.6. Vecinos aleatorizados 10
  - 5.2.7. Simulaciones del Algoritmo de consenso de CA 11
  - 5.2.8. Extensión a redes asincrónicas y no confiables 11
- 5.3. Prueba del relevo 11
- 5.4. Posibles ataques 12

6. Conclusiones 13

Referencias 14

1. DESAFÍOS

Después de años de transmutación, Internet está en peligro de perder su visión y espíritu originales. Por ejemplo, se neutraliza la neutralidad de red [7]; el espectro y el ancho de banda no se utilizan de manera eficiente; la información está fragmentada y puede ser censurada; la protección de la privacidad es limitada. Estos indican que la red necesita una reforma.

Las soluciones existentes no son adecuadas para los sistemas blockchain de próxima generación debido a las siguientes razones:

- Utilizar un enfoque centralizado para mejorar la eficiencia.
- Sacrificar la escalabilidad de la red para acelerar el consenso.
- Limite la tasa de participación de nodos o exija autorización para aumentar la "seguridad".
- Use motivaciones puramente financieras o terceros de confianza para resolver problemas que deben ser resueltos por las matemáticas y la tecnología.

1.1. Limitaciones de las redes P2P

Las redes peer-to-peer (P2P) actualmente enfrentan varios desafíos importantes, que son las oportunidades para NKN. La primera topología de red estática es vulnerable a ataques defectuosos y maliciosos. En segundo lugar, no existe un esquema económico autoincentivado para la conectividad de red y la transmisión de datos. Finalmente, la escalabilidad de la red es ampliamente sacrificada para mejorar la controlabilidad. Todo esto debe ser resuelto por el NKN como se muestra en la Fig. 1.

Fig. 1. Comparación de características entre soluciones ya existentes y las que ofrece NKN.

1.1. Utilización de recursos

Una Internet altamente confiable, segura y diversa es esencial para todos. Sin embargo, existe una enorme ineficiencia en la red actual al proporcionar conectividad global y transmisión de información. Es hora de reconstruir la red que queremos, no solo parchear la red que tenemos. Un sistema de igual a igual totalmente descentralizado y anónimo ofrece un gran potencial en términos de una mayor eficiencia, sostenibilidad y seguridad para la industria y la sociedad.

1.2. Neutralidad de red y fragmentación

Cuando la Comisión Federal de Comunicaciones (FCC) apruebe una medida para eliminar las reglas de neutralidad de la red para fines de 2017 [7], una demanda de poner fin a nuestra dependencia de grandes monopolios de telecomunicaciones y construir Internet descentralizada, asequible y de propiedad local en - La infraestructura se vuelve más fuerte. El entorno de acceso a Internet no restringido y privado se está volviendo insostenible bajo un flujo interminable de ataques y bloqueo, lo que lleva a una propagación de información selectiva y tendenciosa. Sin un esquema de participación incentivador adecuado, es casi imposible mantener un canal de propagación de información constante y seguro.

Además, Internet se ha fragmentado debido a varias razones. Esto no solo agrava la separación, sino que también impacta negativamente en la innovación de la ciencia, la tecnología y la economía.

2. VISIÓN

NKN tiene la intención de revolucionar toda la tecnología de redes y los negocios. NKN quiere ser el Uber o Airbnb del negocio de servicios de comunicación de un billón de dólares, pero sin una entidad central. NKN aspira a liberar los bits y construir la Internet que siempre quisimos.

2.1. Objetivos de NKN

NKN establece los siguientes objetivos:

- Cualquier nodo puede conectarse a esta red completamente abierta desde cualquier lugar
- Promover el intercambio de redes
- Asegurar la neutralidad de la red de las innovaciones de la capa de red
- Siempre mantener la red abierta y escalable
- Realizar un enrutamiento eficiente y dinámico
- ‘Tokenizar’ la conectividad de red y los activos de transmisión de datos e incentivar los nodos participantes.

- Diseñar y construir la próxima generación de red blockchain.

2.2. El tercer pilar: trabajo en red

'Blockchainizando' el tercer y probablemente el último pilar de la infraestructura de Internet, NKN revolucionará el ecosistema blockchain innovando en la capa de red, después de Bitcoin [3] y Ethereum [4] potencia de cómputo 'blockchainizada', así como IPFS [5] y Filecoin [6] almacenamiento 'blockchainizado'. La blockchain de próxima generación basadas en NKN son capaces de soportar un nuevo tipo de aplicaciones descentralizadas (DApp) que tienen una capacidad de transmisión y conectividad mucho más poderosa. La visión de NKN no solo es revolucionar las capas de red descentralizadas, sino también desarrollar tecnologías centrales para la cadena de bloques de próxima generación.

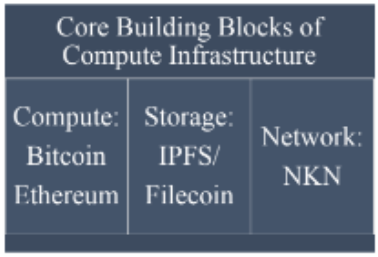

Fig. 2. NKN como el tercer pilar de Internet blockchainized infraestructura.

2.3. Componentes elementales

NKN se basa en varias innovaciones elementales, componentes que son diferentes a las soluciones existentes, como se muestra en la Fig. 3.

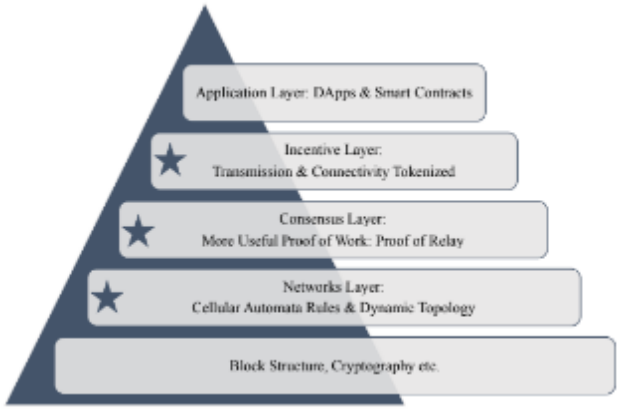

Fig. 3. Componentes elementales de NKN.

1. Bloqueando los bloques básicos restantes de la infraestructura informática: NKN introduce el concepto de esquema descentralizado de transmisión de datos (DDTN) y utiliza blockchain verdaderamente descentralizado para proporcionar conectividad de red y capacidad de transmisión de datos mediante el uso de nodos de retransmisión independientes masivos para resolver el problema de precipitación de datos redundantes en la red.

2. Automated Cellta powered DDTN: NKN introduce la idea de usar Cellular Automata para reconstruir la capa de red. Las características intrínsecas de los autómatas celulares, como la descentralización, la equivalencia entre iguales y la concurrencia, nos permiten construir una red blockchain verdaderamente descentralizada.

3. Consenso impulsado por autómatas celulares: NKN logra consenso de manera eficiente con alta tolerancia a fallas en sistemas distribuidos a gran escala basados en Cellular Automata, que es esencial para sistemas descentralizados sin terceros confiables.

4. Prueba de relevo, una prueba de trabajo útil: NKN propone Prueba de relevo (PoR), un mecanismo que alienta a los participantes a contribuir a la red Blockchain compartiendo su conectividad y ancho de banda para obtener recompensas, mejorando la conectividad de la red y la capacidad de transmisión de datos. PoR es una prueba de trabajo útil (PoW).

5. Tokenización de conectividad de red y capacidad de transmisión de datos: NKN tokeniza la conectividad de la red y la capacidad de transmisión de datos animando a los participantes a compartir su conectividad y ancho de banda a cambio de tokens. Los recursos de la red inactiva se pueden utilizar mejor a través de dicho mecanismo de intercambio. NKN mejora la utilización de los recursos de red y la eficacia de la transmisión de datos. Consulte nuestro documento sobre el modelo de economía para más detalles [8].

6. Conjunto de herramientas de redes para un desarrollo de DApp rápido e indoloro: con NKN, los desarrolladores DApp ahora tienen un nuevo conjunto de herramientas de redes para desarrollar aplicaciones verdaderamente descentralizadas de forma rápida y fácil. Los desarrolladores de DApp pueden enfocarse completamente en la creatividad, la innovación, la interfaz de usuario / experiencia del usuario y la lógica empresarial. Este conjunto de herramientas de redes es totalmente complementario al conjunto de herramientas de otros proyectos de blockchain que trabajan en identidad, aprendizaje automático, pago, almacenamiento, etc.

NKN utiliza metodologías de Cellular Automata para lograr una descentralización completa. Todos los nodos son iguales, verdaderamente de igual a igual, y cada uno es capaz de enviar, recibir y transmitir datos. Cellular Automata hace posible tener reglas locales simples que pueden generar una topología de superposición de red global altamente dinámica y altamente escalable que es independiente de la infraestructura física y lógica subyacente. La simplicidad y la ubicación de las reglas hacen posible una implementación rentable en todos los tipos de dispositivos de red, desde Internet of Things (IoT), teléfonos inteligentes hasta routers. A pesar de su aparente simplicidad, el enrutamiento habilitado de Cellular Automata puede ser altamente aleatorio e impredecible, proporcionando así seguridad y privacidad superiores. Los nodos de NKN se recompensan por proporcionar conectividad y potencia de transmisión, lo que resulta en un mercado completamente competitivo optimizado para maximizar la capacidad total de la red.

Para las redes existentes, NKN aumentará la utilización de la conectividad y la capacidad de transmisión de datos al compartir el ancho de banda no utilizado de los nodos participantes. Cada vez más nodos nuevos se unirán a la red para ganar recompensas, lo que permitirá rápidamente iniciar y expandir la red de NKN. Los nodos existentes están incentivados para actualizar y aumentar la capacidad de transmisión de datos. Todo lo anterior impulsará aún más la capacidad general de la red, así como también mejorará la topología dinámica ya que la red tiene muchos más grados de libertad al elegir la ruta. Además, NKN propone una prueba de trabajo nueva y más útil. A diferencia del cálculo de hash tradicional tipo Prueba de trabajo que no proporciona ninguna utilidad adicional, NKN presenta prueba de relé basado en muchas actividades útiles que incluyen permanecer en línea durante un período prolongado, expandir la cantidad de conexión entre pares, proporcionar alta velocidad y baja latencia, etc. el algoritmo de consenso está diseñado desde cero para mejorar la eficiencia y la equidad, a la vez que converge determinista y globalmente en base al conocimiento local. Además, NKN pretende promover el uso compartido de redes y la propiedad de la red por parte de sus usuarios. El modelo económico y el modelo de gobernanza de NKN reflejarán esto en el diseño y en la implementación. Estas innovaciones tecnológicas y de modelo económico se complementan entre sí y juntas amplificarán el poder de la red de NKN.

2.4. Kit de herramientas de redes para el desarrollo de DApps rápidamente y sin complicaciones

Con NKN, los desarrolladores de DApp ahora tienen un nuevo conjunto de herramientas de red para desarrollar aplicaciones realmente descentralizadas de forma rápida y sin complicaciones. Los desarrolladores de DApp pueden enfocarse completamente en las ideas y la innovación, la IU (interfaz de usuario) / UX (experiencia del usuario) y la lógica de negocios que hacen que sus productos sean exitosos para los usuarios finales. Ya no necesitan vadear la selva salvaje de blockchain, la criptografía, el mecanismo de consenso, la identidad y la seguridad antes incluso de escribir una línea de código para sus usuarios.

Por ejemplo, en el desarrollo de aplicaciones tradicionales con ofertas centralizadas SaaS (software como servicio), uno puede alojar aplicaciones en plataformas de computación en la nube, almacenar datos en almacenamiento en la nube, usar servicios web para mensajes de texto, llamadas telefónicas y pagos. En el mundo descentralizado de las cadenas de bloques, ya es concebible construir un nuevo tipo de Facebook utilizando Ethereum/NEO para la computación, IPFS para el almacenamiento y NKN para la creación de redes. La belleza de este nuevo paradigma es que los usuarios poseerán personalmente su identidad y datos, y pueden ser tanto consumidores como proveedores en todo el sistema también. Además de eso, en cada capa hay un mecanismo autoincentivado incorporado para maximizar el efecto de red y arrancar a toda la comunidad.

NKN será uno de los tres elementos fundamentales y desempeñará un papel fundamental en este paradigma descentralizado.

3. FUNDACIONES TECNOLOGICAS

En este documento técnico, tomamos elementos selectivos del NKS (New Kind of Science) como inspiración. NKN utiliza reglas microscópicas basadas en Cellular Automata para definir la topología de red, lograr comportamientos de autoevaluación y explorar el consenso impulsado por los autómatas celulares, que es fundamentalmente diferente de la capa de red blockchain existente.

Como una herramienta poderosa para estudiar sistemas complejos, Cellular Autómata está estrechamente vinculado a categorías filosóficas como simple y compleja, micro y macro, local y global, finita e infinita, discreta y continua, etc.

3.1. Cellular Automata

Fig. 4. Propiedades de los autómatas celulares.

Cellular Automata (CA) es una máquina de estado con una colección de nodos, cada uno cambiando su estado siguiendo una regla local que solo depende de sus vecinos. Cada nodo solo tiene unos pocos nodos vecinos. Propagando a través de interacciones locales, los estados locales eventualmente afectarán el comportamiento global de CA. La apertura deseada de la red está determinada por la homogeneidad de los autómatas celulares, donde todos los nodos son idénticos, formando una red P2P (peer-to-peer) totalmente descentralizada. Cada nodo de la red de NKN se actualiza constantemente en función de su estado actual y de los estados de los vecinos. Los vecinos de cada nodo también cambian dinámicamente de modo que la topología de red también es dinámica sin cambiar su infraestructura subyacente y sus protocolos. NKN utiliza CA para lograr una topología eficiente, descentralizada y dinámica de modo que la información y los datos se puedan transmitir de manera eficiente y dinámica sin conectividad centralizada.

3.2. Reglas como fórmulas

La fórmula de programación de Cellular Automata se denomina "regla local", que es una regla indispensable para la red de próxima generación de NKN y tiene una influencia importante en la topología de red [2, 10-13]. La elección adecuada de las reglas locales conduce a los autómatas celulares con comportamientos complejos pero autoorganizados en el límite entre la estabilidad y el caos. Las reglas son esenciales porque son fórmulas para programar los autómatas celulares y las redes de autómatas. Las características estáticas de un autómata celular son un sistema dinámico discreto definido como

$$CA = (S, N, K, f) \quad (1)$$

El número finito de nodos interactúa en una red regular. S representa estados de nodos, donde cada nodo tiene un estado local. El estado de todos los nodos determina el estado global. N denota la cantidad de nodos en la red. K describe el conjunto vecino, es decir, qué nodos vecinos se tienen en cuenta en las transiciones de estados locales. f denota una función de transición de estado, que tiene un impacto dramático en la evolución global del sistema.
Las características dinámicas de un autómata celular se ilustran en la figura 5. La evolución dinámica comienza desde un estado inicial. Los nodos cambian sus estados según sus estados actuales y los estados de sus nodos vecinos. El estado global está completamente determinado por los estados locales de todos los nodos y evoluciona en consecuencia. Los enfoques de caracterización de autómatas celulares utilizan topología estática y completamente conectada.

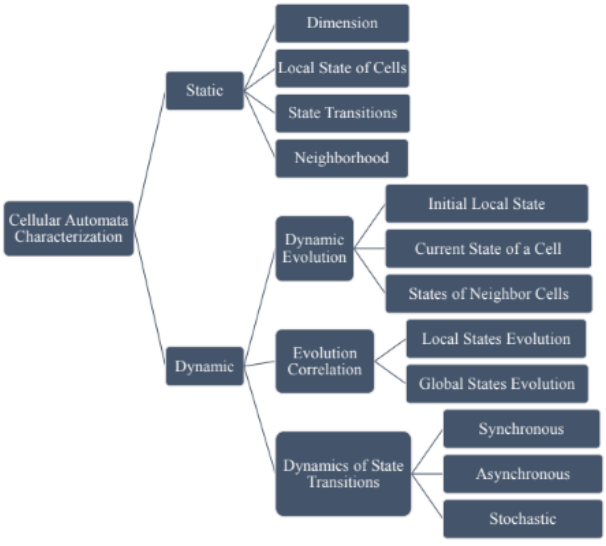

Fig. 5. Características de los autómatas celulares.

El equipo de NKN cree que los sistemas basados en CA o CA son más naturales y orgánicos que los enfoques actuales que utilizan topología estática y completamente conectada. Los sistemas complejos con una estructura tan simple están más cerca de los sistemas naturales, lo que permite la autoevolución.

4. NUEVO TIPO DE RED

NKN es la próxima generación de infraestructura de red entre pares basada en la tecnología blockchain respaldada por la teoría de Cellular Automata, que apunta a revolucionar Internet con una verdadera descentralización y un mecanismo de incentivo token nativo.

4.1. Red descentralizada de próxima generación

Como los líderes actuales en blockchain, Bitcoin y Ethereum tokenizan el poder computacional a través de la Prueba de trabajo (PoW). IPFS [5], Filecoin [6], Sia [14] y Storj [15], por otro lado, tokenizan el almacenamiento. Sin embargo, pocos sistemas bloquean la conectividad de red y la potencia de transmisión de datos, el tercer elemento esencial en Internet. NKN está diseñado para simbolizar la conectividad de red y la capacidad de transmisión de datos como un PoW útil. NKN resuelve el problema de "eficiencia" de blockchain igualando todos los nodos en la red. Cada nodo sigue una regla de Cellular Autómata y actualiza su estado en función de las reglas locales. Propuesto por Von Neumann en la década de 1940, Cellular Automaton (CA) es un término genérico para un tipo de modelo, una máquina de estados caracterizada por tiempo discreto, espacio e interacción [16, 17]. Es un sistema discreto que evoluciona localmente de acuerdo con reglas específicas y se ha demostrado que es capaz de emular la evolución de sistemas complejos.

Cellular Autómata tiene las características de descentralización, igualdad de pares y concurrencia. Por primera vez, NKN propuso Cellular Automata como el elemento fundamental de la capa de red para blockchain, a fin de garantizar que toda la capa de red pueda beneficiarse de ella. Las fórmulas de actualización en los autómatas celulares se denominan "reglas locales", que se consideran el factor crítico que controla la transición del autómata celular entre la estabilidad y el caos [2]. Como parte indispensable de NKN, las reglas son uno de los principales factores que afectan la topología de la red. NKN introdujo el concepto de Red de Transmisión de Datos Descentralizada (DDTN). DDTN combina múltiples nodos de retransmisión independientes y autoorganizados para proporcionar a los clientes conectividad y capacidad de transmisión de datos. Esta coordinación es descentralizada y no requiere la confianza de las partes involucradas. La operación segura de NKN se logra a través de un mecanismo de consenso que coordina y valida las operaciones realizadas por cada nodo. DDTN proporciona una variedad de estrategias para aplicaciones descentralizadas (DApp).
A diferencia de la conectividad de red centralizada y la transmisión de datos, existen múltiples rutas eficientes entre los nodos en DDTN, que se pueden utilizar para mejorar la capacidad de transmisión de datos. Los tokens nativos pueden incentivar el uso compartido de los recursos de red y, a la larga, minimizar el desperdicio de conectividad y ancho de banda. Tal propiedad se denomina "autoincentivada".

4.2. Una prueba útil de trabajo

Como la criptomoneda pionera, Bitcoin [3] es generada por la minería, un mecanismo de prueba de trabajo que incentiva a los mineros a verificar las transacciones resolviendo problemas difíciles de hash. La desventaja de la minería de Bitcoin es que la minería eficiente requiere hardware especializado y costoso y consume mucha energía. De acuerdo con Digiconomist, la tasa de consumo de energía de Bitcoin es cercana a 50 TWh / año a mediados de febrero de 2018 y sigue aumentando, mientras que el número está cerca de 14 TWh / año para Ethereum. La electricidad consumida por estas dos criptomonedas combinadas ha superado el consumo de electricidad de muchos países.

Una forma de probar el trabajo evitando el desperdicio de recursos es muy deseado. NKN propone una alternativa al PoW actual al proporcionar una infraestructura de red más descentralizada, dinámicamente evolutiva, autoorganizable y autónoma y diseñando un conjunto completamente nuevo de mecanismos de consenso. La novela PoW no genera un desperdicio de recursos. En cambio, es un mecanismo de intercambio punto a punto a nivel de blockchain. Los participantes reciben recompensas al aportar más recursos de red de los que consumen. NKN usa el mecanismo de prueba de relé para garantizar la conectividad de la red y la capacidad de transmisión de datos.

4.3. Topología de red y enrutamiento

Cellular Automata on Networks (CAoN) es una extensión natural de Cellular Automata [10, 11, 18] que es capaz de modelar redes con conexiones vecinas no geométricas. Es poderoso cuando se modelan redes cuya topología está evolucionando según las reglas locales. Como el objetivo es construir un sistema blockchain descentralizado con topología dinámica, CAoN es un modelo natural para el sistema.

Consideramos una red P2P dinámica con N nodos. Las conexiones de red en el tiempo t pueden describirse mediante una matriz de adyacencia N × N A (t) que evoluciona con el tiempo. Las conexiones entre nodos se pueden agregar, eliminar o modificar en cada paso de tiempo. Si la dinámica de A es Markovian, el proceso de actualización se puede escribir como

$$A\,(t + 1) = f\,[A\,(t)], \qquad (2)$$

donde *f* es la regla de actualización de topología de red. Para mantener la regla de actualización local, *f* debe elegirse de modo que solo se use información de los vecinos de cada nodo al actualizar sus conexiones. La regla de actualización anterior no contiene estados de nodos, por lo que la evolución de la topología es independiente del estado de cualquier nodo. Una regla de actualización de Markovian más general debería tener en cuenta tanto la topología de la red como los estados de los nodos de modo que

$$\begin{aligned} A(t + 1) &= f[A(t),S(t)] \\ S(t + 1) &= g[A(t + 1),S(t)] \end{aligned} \qquad (3)$$

donde $S(t)$ es un vector que representa los estados de todos los nodos en la red en el tiempo t, f es la regla de actualización de topología, y g es la regla de actualización de estado. Del mismo modo, f y g deben elegirse de modo que solo se utilice la información de los vecinos actuales al actualizar. El estado podría contener información histórica. Un estado de ejemplo en el sistema blockchain es todos los bloques que un nodo almacena localmente. Tenga en cuenta que, aunque describimos el sistema formalmente utilizando el estado global S y la conectividad global A, cada nodo solo necesita saber y almacenar su estado local S_i y sus vecinos $\{j|A_{ij} = 0\}$.

Considere una CAoN en un sistema blockchain donde se generan bloques. Cada vez que se recibe un bloque, el nodo actualiza su estado y envía el bloque a los vecinos con firma digital. Los vecinos decidirán si reenviar el mensaje según sus estados, como si recibió el bloque, si el bloque es válido o si entra en conflicto con otro bloque en estado, afectando de hecho la topología de toda la red sin cambiar la capa física o el protocolo subyacente.

Como un ejemplo para ilustrar cómo modelamos la red, uno puede considerar una Automatización de Red general que permite un número arbitrario de vecinos. Para simplificar, se adopta un enfoque minimalista para emular la expansión de cadena de bloques y la retransmisión de datos a partir de un pequeño conjunto de reglas microscópicas. Inicialmente (en el tiempo cero) la red es una estructura cúbica 3D con 8 nodos, cada uno tiene 3 vecinos, como se muestra en la Fig. 6.

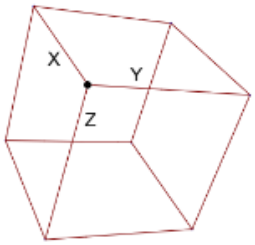

Fig. 6. Un ejemplo de Autómatas de red con forma de 8 nodos, una red cúbica en el espacio 3D en el estado inicial.

A partir de la red simple de la figura 6, el sistema se amplía mediante la adición de nodos siguiendo varias reglas de actualización. La topología resultante puede ser dramáticamente diferente cuando se usan reglas diferentes, como se muestra en la Fig. 7.

NKN unirá la evolución de la red y las funciones blockchain utilizando modelos de red similares con reglas microscópicas. Las simples reglas locales hacen que la replicación sea sencilla, simplificando y acelerando las implementaciones del sistema.

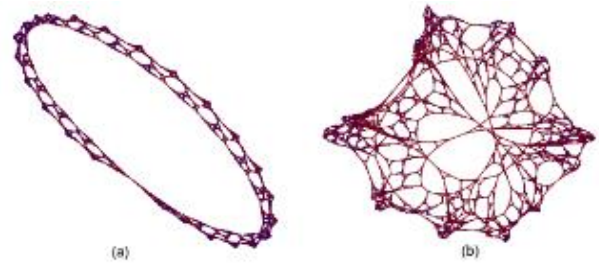

Fig. 7. Algunos ejemplos de topologías de red blockchain complejas con varios conjuntos de reglas simples (a) topología de anillo, regla 1655146, paso de tiempo 1573; (b) topología pseudoaleatoria, regla 1655185, paso de tiempo 1573.

4.3.1. Dinámica

Las dinámicas en CAoN son puramente locales: cada nodo evalúa la transición de estado independientemente de otros nodos y cambia su estado en consecuencia [19]. El estado del nodo puede ser impulsado por la interacción entre nodos o información externa, como se muestra en la figura 8.

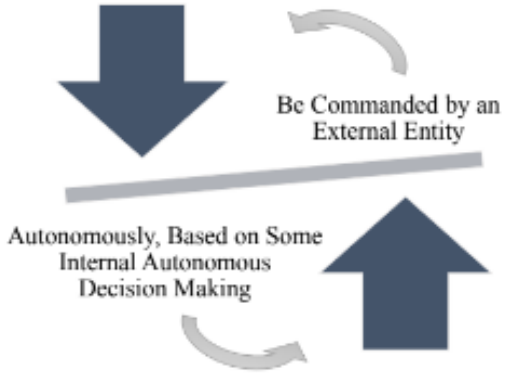

Fig. 8. Posibles condiciones para que un nodo cambie su estado en CAoN.

Las reglas son cruciales para la topología resultante en CAoN. La topología de red sería muy diferente dados los pequeños cambios en las reglas de actualización, como se muestra en la figura 9.

Aunque en la descripción matemática se usó el paso de tiempo discreto por conveniencia, CAoN no requiere que los nodos tengan tiempo global o tiempo discreto. En cambio, cada nodo realiza la actualización de forma asincrónica [19]. Esta es una descripción más general y realista de las redes de blockchain reales.

4.3.2. Autoorganización

La dinámica global de los autómatas celulares se puede clasificar en 4 tipos [2]: constante, periódica, caótica y compleja. Nuestro enfoque está en el tipo complejo (Clase 4), también conocido como el borde del caos, donde todos los patrones iniciales evolucionan en estructuras que interactúan de maneras complejas, con

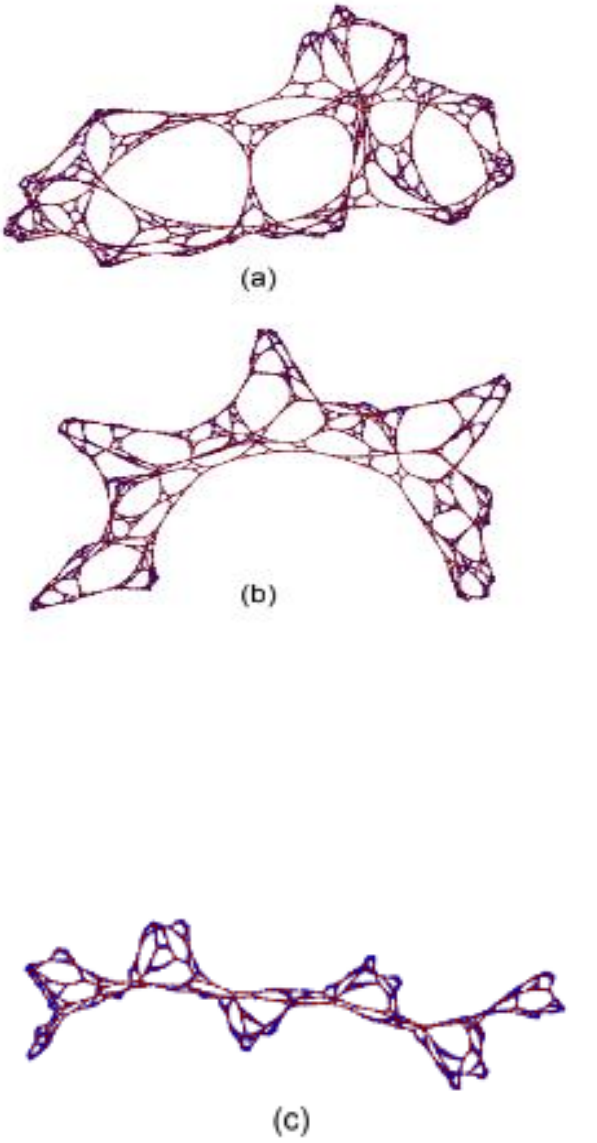

Fig. 9. Dinámica de la topología de red mediante la reescritura de reglas del Cellular Automata al mismo tiempo paso índice, (a) rule 1655163, paso de tiempo 1573; (b) regla 1655175, paso de tiempo 1573; (do) regla 1655176, paso de tiempo 1573.

la formación de estructuras locales que pueden sobrevivir por largos períodos de tiempo. Wolfram especula que, aunque no todos los autómatas celulares de clase 4 son capaces de computación universal, muchos de ellos son completos. Esta visión ha sido probada con éxito por las Reglas 110 [2, 20] y el Juego de la vida de Conway [21]. Las estructuras complejas, autorreorganizadas y dinámicas emergen espontáneamente en CA de Clase 4, proporcionándonos un candidato ideal para la base de sistemas descentralizados.

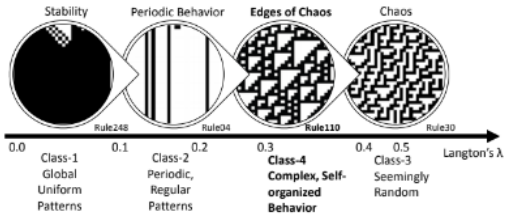

Fig. 10. Las 4 clases de comportamientos de Wolfram versus el parámetro λ de Langton en 1D Cellular Automata.

Una medida cuantitativa de la regla que puede explicar y predecir el tipo de comportamiento de la CA es el parámetro λ de Langton definido por la fracción de las entradas de la tabla de reglas que da como resultado el estado activo. A medida que λ aumenta desde 0, el sistema pasará de estado estable a estado periódico, luego a estado complejo y finalmente a estado de caos, como se muestra en la Fig. 10. En la clásica CA 1D con la interacción de vecino más próximo, el comportamiento de Clase 4 emerge λ es alrededor de 0.3. El parámetro λ de Langton nos proporciona una guía teórica sobre cómo encontrar las reglas de actualización deseadas, que es esencial para los sistemas de alta dimensión.

4.3.3. Auto-Evolución

CAoN es inherentemente autodesarrollado debido a su dinámica local simple pero poderosa. La regla de actualización esencialmente establece la dirección de la evolución, y el sistema evoluciona continuamente hacia la dirección, independientemente de los estados iniciales o cómo se agregan los nodos a la red. La Fig. 11 muestra un ejemplo de la autoevolución en CAoN.

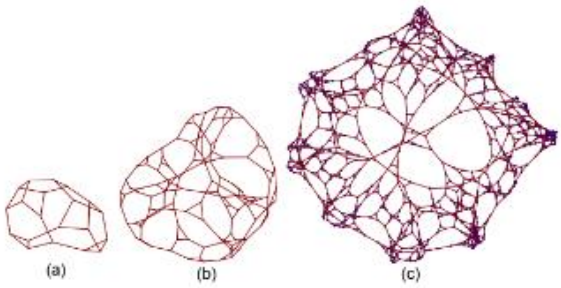

Fig. 11. Autoevolución de un modelo 3D CAoN en la regla 1655185 en varios índices de paso de tiempo (a) 100; (b) 1000; (c) 10000.

4.4. Descentralización eficiente

Debido a la naturaleza dinámica de NKN, la topología de red entre nodos se actualiza constantemente. El mecanismo de actualización adecuado es fundamental para lograr la descentralización de la topología resultante. Si, por ejemplo, el mecanismo de actualización se elige de modo que un nodo recién unido tenga más posibilidades de elegir un nodo con más vecinos para ser su vecino, y la probabilidad de elegir un nodo sea proporcional al grado de ese nodo, entonces la red resultante estará libre de escalas: la distribución de grados sigue una forma de ley de poder. Tales redes tienen concentradores centralizados definidos por nodos en gran medida. Aunque los hubs podrían potencialmente aumentar la eficiencia, hacen que la red sea menos robusta, ya que la falla de los hubs tendrá un impacto mucho mayor que la falla de otros nodos.

Uno de los objetivos de NKN es diseñar y construir redes descentralizadas que a la vez sean eficientes en la transmisión de información. Esto debe hacerse utilizando un mecanismo de actualización de topología adecuado que considere tanto el algoritmo como el incentivo. En el lado del algoritmo, los vecinos deberían ser muestreados y elegidos al azar; en el lado de los incentivos, la recompensa por la transmisión de datos debería ser sublineal (crece más lento que la función lineal) por lo que se desaconsejan los centros. La red aleatoria dispersa es una posible topología que podría generarse a partir de dicho mecanismo. Está descentralizado y, por lo tanto, es robusto para la falla de cualquier nodo, al tiempo que sigue siendo eficiente en el enrutamiento debido a su pequeño diámetro de red.

5. CONSENSO ALIMENTADO DE CELLULAR AUTOMATA

Los nodos en blockchain son iguales debido a la naturaleza descentralizada de blockchain. La inherente falta de confianza en los sistemas de blockchain es particularmente notable porque cualquier nodo puede enviar información a cualquier nodo en la cadena de bloques. Los compañeros deben evaluar la información y llegar a un acuerdo sobre sus acciones para que blockchain funcione correctamente.

NKN está diseñado para ser una infraestructura de cadena de bloques futurista que requiere baja latencia, gran ancho de banda, escalabilidad extremadamente alta y bajo costo para alcanzar el consenso. Estas propiedades son cruciales para futuros DApps. Por lo tanto, NKN necesita nuevos algoritmos de consenso que puedan satisfacer tales requisitos elevados.

5.1. Consenso general

Actualmente hay varios enfoques para llegar a un consenso en blockchain: algoritmo de tolerancia a fallas bizantinas (BFT) [24], algoritmo de tolerancia a fallas bizantino práctico (PBFT) [25], algoritmo de prueba de trabajo (PoW) [3], algoritmo de Proof-of-Stake (PoS) [26, 27] y algoritmo de Proof-of-Stake delegada (DPoS) [28].

1. Práctico Tolerante a fallas bizantinas (PBFT): La tolerancia a fallas bizantina es un modelo que Leslie Lamport propuso en 1982 para explicar el tema del consenso. Discute el consenso bajo el escenario donde algunos nodos podrían ser malvados (el mensaje puede estar falsificado) y ofrece la peor garantía de caso [24]. En la tolerancia a fallas bizantina, deje que el número total de nodos sea N y el número de nodos defectuosos sea F, si $N \geq 3F + 1$, entonces el problema puede ser resuelto por el algoritmo de tolerancia a fallas bizantinas (BFT). Lamport demostró que hay un algoritmo válido tal que cuando la fracción de nodos defectuosos no supera un tercio, los nodos buenos siempre podrían alcanzar el consenso sin importar qué mensajes envíen los nodos defectuosos. Practical Byzantine Fault Tolerant (PBFT), propuesto por primera vez por Castro y Liskov en 1999, fue el primer algoritmo de BFT ampliamente utilizado en la práctica [25]. El PBFT es mucho más eficiente y funciona de manera asincrónica, mientras que todavía puede tolerar la misma cantidad de nodos defectuosos que BFT, lo que lo hace más práctico de usar en sistemas reales.

2. Proof-of-Work (PoW): la red de blockchain de Bitcoin introdujo un algoritmo de Prueba de trabajo (PoW) innovador [3]. El algoritmo limita el número de propuestas al aumentar el costo de las mismas y relajar la necesidad de una confirmación final de conformidad al acordar que todos aceptarán la cadena más larga conocida. De esta manera, cualquiera que intente con el vandalismo pagará

un gran costo económico. Ese es, para pagar más de la mitad de la potencia de cálculo del sistema. Más tarde, varios algoritmos de la serie "PoX" se proponen siguiendo este pensamiento, utilizando sanciones económicas para restringir los spoilers. PoW es el consenso utilizado por Bitcoin y también es el más antiguo utilizado en el sistema blockchain. En resumen, PoW significa cuánto trabajo paga un minero y cuánto gana. El trabajo aquí es la potencia de cálculo y el tiempo que proporciona un minero contribuir al sistema blockchain. El proceso de proporcionar tales servicios es "minería". En PoW, el mecanismo para asignar recompensas es que los ingresos mineros son proporcionales a la potencia de cálculo. Cuanto más poderosa sea la máquina minera utilizada, más recompensas esperadas obtendrán los mineros.

3. Proof-of-Stake (PoS): Inicialmente, la Prueba de Estaca reduce la dificultad de calcular hash de acuerdo con la cantidad de tokens retenidos. PoS es similar al financiamiento activos financieros en el banco, que distribuyen el rendimiento financiero proporcional a la cantidad de activos que posee la participación en un período determinado. De manera similar, en PoS, el sistema blockchain asigna "intereses" de acuerdo con la cantidad de tokens de las partes interesadas y el tiempo de espera [26, 27]. En Delegated Proof of Stake (DPoS), no todas las partes interesadas pueden crear bloque. En cambio, los nodos votan por los fideicomisarios que los representan para el parlamento y crear bloques. Los usuarios que deseen convertirse en consejeros deben pasar por una prueba comunitaria para ganarse la confianza de esta [28].

5.2. Consenso impulsado por autómatas celulares

5.2.1. Problema de escalabilidad de BFT y PBFT

Es desafiante obtener consenso en grandes sistemas distribuidos usando algoritmos BFT y PBFT. En el algoritmo BFT, el número total de mensajes que se enviarán al sistema es O (N!) [24], por lo que no es práctico. El algoritmo PBFT redujo el conteo total de mensajes a O (N2) [25], que es manejable pero no escalable cuando N es grande. Además, tanto BFT como PBFT requieren que cada nodo tenga una lista de todos los otros nodos en la red, lo cual es difícil para la red dinámica.

5.2.2. Consenso en los autómatas celulares descrito por el modelo Ising

Cellular Automata (CA) es, naturalmente, un gran sistema distribuido con solo conexiones locales. El comportamiento asintótico del sistema está controlado por su regla de actualización. Es posible lograr un consenso global garantizado en CA utilizando un algoritmo de paso de mensajes basado únicamente en vecinos locales dispersos para un conjunto de reglas de actualización.

Usando el marco matemático desarrollado originalmente para el modelo Ising [29] en física, encontramos y probamos que una clase de reglas de CA garantizará alcanzar consenso en la mayoría de las iteraciones de O (N) usando solo estados de vecinos dispersos por un mapa exacto de CA a cero temperatura. Algunos estudios investigaron la tolerancia a fallas de los autómatas celulares y cómo aumentar la robustez en sistemas basados en autómatas celulares [30-32]. Además, demostramos que el resultado es robusto para los nodos defectuosos aleatorios y maliciosos y calculamos el umbral cuando no se puede lograr el consenso deseado.

5.2.3. Modelo Ising

El modelo Ising es un modelo de sistemas de espín con interacción por pares en el campo magnético externo [29]. El hamiltoniano (energía) del sistema sin campo magnético externo se puede escribir así:

$$H(s) = -\sum J_{ij} s_i s_j, \qquad (4)$$

donde $s_i = \pm 1$ es el giro del nodo *i*, y J_{ij} es la interacción entre el nodo *i* y el nodo *j*. Consideramos el caso donde Jij solo puede ser 1 (interacción ferromagnética) o 0 (sin interacción). La probabilidad de que el sistema se encuentre en estado en equilibrio sigue la distribución de Boltzmann

$$p(s) = \frac{1}{Z} e^{-\beta H(s)} = \frac{1}{Z} e^{\beta \sum_{i,j} J_{ij} s_i s_j}, \qquad (5)$$

Ising modelo en celosía ha sido ampliamente estudiado [29, 33]. Para el modelo de Ising en un enrejado dimensional D con interacción de vecino más cercano, se produce una transición de fase a temperatura crítica finita Tc excepto para D = 1 donde la temperatura crítica Tc = 0. Cuando T <Tc, el sistema colapsa en uno de los dos estados donde los nodos tienen un giro preferido (magnetización espontánea), mientras que el sistema no tiene un giro preferido cuando T> Tc.

Por ejemplo, para una cuadrícula cuadrada 2D con la interacción de un vecino más cercano, se puede obtener la solución exacta del modelo de Ising. La temperatura crítica es

$$T_c = \frac{2}{\ln(1+\sqrt{2})} \approx 2.27, \qquad (6)$$

y la magnetización espontánea es

$$\langle s \rangle = \pm \left[1 - (\sinh 2\beta)^{-4}\right]^{\frac{1}{8}}. \qquad (7)$$

Todos los giros serán los mismos (ya sea 1 o -1) cuando T → 0.

Si el sistema de interés distribuido se puede describir matemáticamente mediante un modelo de Ising, se garantiza que el sistema alcanzará el consenso (todos los nodos tienen los mismos estados) cuando la temperatura es cero. La temperatura finita desempeña el papel de falla al agregar aleatoriedad a la transición de estado, y la temperatura crítica finita conduce a la solidez de dicha falla.

5.2.4. Enlace entre los autómatas celulares y el modelo Ising

Cellular Automata (CA) está estrechamente relacionado con Ising Model. Una CA se caracteriza por su regla de actualización

$$p(s^{t+1}|s^t) = \prod_i p(s_i^{t+1}|s^t) \qquad (8)$$

eso representa la probabilidad de que el sistema se transfiera al estado st + 1 en el tiempo t + 1 dado el estado del sistema s t en el tiempo t. La probabilidad de transferencia es condicional independiente porque cada nodo en CA actualiza su estado únicamente dependiendo del estado del sistema anterior. Para CA determinista, la probabilidad de transferencia p (st + 1 | st) es una función delta. Si se puede definir un hamiltoniano de la forma H (s) = -Pi tal que;

$$p(s_i^{t+1}|s^t) \propto e^{-\beta H(s_i^{t+1}|s^t)} = e^{\beta \sum_j J_{ij} s_i^{t+1} s_j^t}, \qquad (9)$$

La probabilidad de transferencia se vuelve

$$p(s^{t+1}|s^t) \propto e^{\beta \sum_{i,j} J_{ij} s_i^{t+1} s_j^t}. \qquad (10)$$

La probabilidad de transferencia de St ahora es proporcional a la distribución de Boltzmann

$$p(S^{t+1}|S^t) = p(s^{t+1}|s^t) \propto e^{\beta \sum_{i,j} J_{ij} s_i^{t+1} s_j^t} = e^{-\beta H(S^{t+1})}, \qquad (11)$$

Por lo tanto, la CA se asigna a un modelo de Ising con el estado *S*. La distribución estacionaria de *S* sigue la distribución de Boltzmann

$$p(S) = \frac{1}{Z} e^{-\beta H(S)}, \qquad (12)$$

mientras que la distribución estacionaria de *s* está dada por

$$p(s) = \frac{1}{Z} \sum_{s^*} e^{\beta \sum_{i,j} J_{ij} s_i s_j^*} \qquad (13)$$

La CA determinista puede correlacionarse con el modelo de Ising a temperatura cero, donde $T \to 0$, $\beta \to \infty$, $p(S)$ y $p(s)$ no son cero solo en el estado (s) con la energía más baja. En el caso de J_{ij} = 1 o 0 que nos interesa, solo dos estados (s_i = 1, ∀*i* o s_i = -1, ∀i) se permiten a temperatura cero.

5.2.5. Automatización Celular de Voto de Mayoría como un Algoritmo de Consenso

La mayoría de los autómatas celulares de voto (MVCA) es un autómata celular que utiliza la mayoría de los votos como regla de actualización. Se puede formalizar como

$$s_i^{t+1} = \text{sign}\left(\sum_j J_{ij} s_j^t\right), \qquad (14)$$

donde Jij = 1 si el nodo i y j están conectados, de lo contrario
0. signo (x) = 1 si x> 0, o -1 si x <0. signo (0) = 1 o -1 con igual probabilidad. La definición de signo (0) no tiene ningún impacto si cada nodo tiene un número impar (k) de conexiones, lo cual es cierto para los autómatas celulares D dimensionales con las conexiones de vecinos más cercanos y la auto conexión. Solo k impar se considera por implicidad.

El hamiltoniano se puede definir como H = -Pi, j Jij sisj. Se puede verificar que la regla de voto mayoritario cumpla la condición de mapeo con temperatura cero ($\beta \to \infty$). De acuerdo con la sección anterior, cuando MVCA alcanza el equilibrio, todos los nodos tendrán el mismo estado que depende de la condición inicial.

Para mostrar que MVCA convergerá a su equilibrio, usaremos la ecuación derivada en la sección anterior que es distinta de cero solo cuando H (St + 1) se minimiza. A partir de la definición de H (S) obtenemos que igual es posible solo cuando st + 1 = s, ya que st + 1 está determinado exclusivamente por st cuando cada nodo tiene un número impar de conexiones. Específicamente, para s = st-1 tenemos H (St + 1) ≤ H (St), donde igual solo se cumple cuando st + 1 = st-1, es decir, sistema en equilibrio o dos oscilaciones de estado. El último se puede evitar cuando J es dinámico, por lo que lo ignoramos por el momento. SoH (St + 1) <H (St) antes de que MVCA alcance su equilibrio. Por otro lado, observamos que H (S) solo puede ser enteros que cambian en el paso de 2 y -kN ≤ H (S) ≤ kN, donde N es el número total de nodos en el sistema y k es la cantidad de conexiones que tiene cada nodo. Por lo tanto, MVCA garantiza converger al estado de consenso en la mayoría de las iteraciones kN para cualquier estado inicial. De forma similar, si el estado inicial tiene m valores "incorrectos", se requieren como máximo km de iteraciones para corregir esos valores "incorrectos".

Aunque en la derivación anterior utilizamos CA como modelo, no asumimos la conectividad local. De hecho, los resultados son válidos para cualquier topología de red con matriz de conectividad simétrica J.

5.2.6. Vecinos aleatorizados

Los autómatas celulares y el modelo de Ising son sistemas basados en celosía con una fuerza de interacción que depende principalmente de la distancia euclidiana. Este tipo de modelos son matemáticamente más fáciles de resolver, mientras que no es práctico implementarlos en sistemas distribuidos, especialmente cuando los nodos son dinámicos, poco confiables e incontrolables. Aquí proponemos que la red aleatoria debería ser una mejor topología para el consenso en el sistema distribuido con nodos dinámicos. El algoritmo de consenso que propusimos funciona en redes aleatorias sin ninguna modificación, de modo que cada nodo no necesita mantener una conectividad específica. Cabe mencionar que la red aleatoria discutida aquí es puramente una red superpuesta, independientemente de cómo los nodos estén físicamente conectados. En un sistema distribuido donde el nodo no tiene una lista de otros nodos, uno puede

usar algoritmos como el muestreo por pares para lograr conectividad aleatoria.

Un parámetro crítico que controla la velocidad de propagación de la información y, por lo tanto, el consenso puede ser el diámetro de la red que se define como la distancia más corta entre los dos nodos más distantes de la red. Para una red aleatoria donde cada nodo tiene k vecinos yk es O (logN), el diámetro de la red es como máximo O (logN) [12], mucho más pequeño que un sistema basado en red. Esto es esperado ya que una red aleatoria podría tener conexiones de largo alcance, lo que no es posible en sistemas de celosía. Como resultado, las redes aleatorias convergen más rápidamente a los estados de consenso. También se muestra que el aumento k conduce a un diámetro más pequeño [12], como uno puede esperar.

Wolfram Class 4 Cellular Automata es ideal para construir la red aleatorizada para un rendimiento de consenso superior. En Class 4 CA, la conectividad es efectivamente impredecible, autoorganizada y autodesarrollada.

5.2.7. Simulaciones del algoritmo de consenso de CA

Para mostrar el rendimiento de nuestro algoritmo de consenso, lo aplicamos a una red simulada con N = 1, 000, 000 nodos. Cada nodo tiene k vecinos seleccionados al azar de la red. En cada iteración, su estado se actualiza en función de los estados de sus k vecinos más su propio estado utilizando la regla MVCA como se propuso anteriormente. Los vecinos son unidireccionales, por lo que no se garantiza que J sea simétrico. Inicialmente (iteración 0), el estado de cada nodo se elige independientemente para que sea 1 o -1 con alguna probabilidad. La simulación se ejecuta para varias iteraciones con diferentes k, como se muestra en la figura 12. Se puede ver que el MVCA converge al estado de consenso global en solo unos pocos pasos, incluso con k = 10, mucho más rápido que el límite superior teórico kN. Tenga en cuenta que se alcanzará el consenso incluso cuando el estado inicial contiene el mismo número de nodos 1 y -1. Una mayor k conduce a una convergencia más rápida.

Se debe mencionar que cuando N es grande, la topología de la red aleatoria estará más cerca de su caso típico, ya que la probabilidad de tener una conectividad específica disminuye exponencialmente a medida que N aumenta. Por lo tanto, uno debe mirar el tiempo medio de convergencia en lugar del peor caso cuando (y solo cuando) N es grande, como en nuestras simulaciones.

Simulamos aún más el escenario donde una fracción de nodos son maliciosos. En este caso, los nodos correctos tienen el estado inicial 1, mientras que los nodos maliciosos tienen el estado inicial -1 y no actualizan sus estados independientemente de los estados de sus vecinos. El objetivo de los nodos correctos es llegar a un consenso sobre el estado 1, mientras que los nodos maliciosos intentan llegar a un consenso sobre el estado -1. De los resultados (Fig. 13) se puede ver que hay una transición entre el colapso al estado incorrecto (-1) y el mantenimiento de la mayoría de los nodos correctos en el estado correcto (1). Para N = 1, 000, 000 yk = 10, la fracción crítica de los nodos maliciosos es de alrededor del 30%, lo cual es significativo considerando el tamaño de N. La fracción crítica también depende de k, como se muestra en la Fig. 13. Más grande k tiene dos efectos: se pueden tolerar nodos más maliciosos y los nodos correctos se verán afectados por nodos maliciosos. Los resultados en la Fig. 12 y la Fig. 13 combinados muestran el límite superior y el límite inferior de la dinámica de red con estados iniciales defectuosos: el primero simula el caso en que los nodos con estado inicial incorrecto no son maliciosos, mientras que el segundo simula el caso donde los nodos con un estado inicial incorrecto son todos maliciosos y desean que el resto de la red acuerde el estado incorrecto. Las dinámicas de red caen entre estas dos curvas con los mismos estados iniciales, independientemente de los nodos defectuosos de estrategia (los que tienen un estado inicial defectuoso).

5.2.8. Extensión a redes asincrónicas y no confiables

Una ventaja del uso del modelo Ising para describir el sistema es la extensión natural a los canales de comunicación ruidosos y poco confiables. El parámetro de temperatura en el modelo Ising controla la cantidad de ruido en el sistema, y en nuestro caso es la aleatoriedad en la regla de actualización. A temperatura cero, la regla de actualización es determinista, mientras que la regla se vuelve más aleatoria cuando la temperatura aumenta, y eventualmente se vuelve puramente aleatoria cuando la temperatura va al infinito. Al incluir un estado predeterminado, la falla probabilística de la entrega del mensaje se puede modelar mediante la temperatura finita en el modelo de Ising. Por lo tanto, aún se puede llegar a un consenso siempre que el ruido esté por debajo del umbral, como se discutió anteriormente. El umbral se puede calcular numéricamente teniendo en cuenta las estadísticas de conectividad de red. La actualización de estado asíncrono también se puede modelar mediante dicho ruido cuando se agrega el tiempo de espera de comunicación, por lo que es práctico para la implementación.

5.3. Prueba de retransmisión

El consenso en NKN está impulsado por Prueba de Retransmisión (PoR), una prueba de trabajo útil (PoW) donde las recompensas esperadas que obtiene un nodo dependen de su conectividad de red y poder de transmisión de datos. Nodo demuestra su carga de trabajo de retransmisión agregando firma digital al reenviar datos, que luego es aceptado por el sistema a través del algoritmo de consenso.

El PoR no es un desperdicio de recursos, ya que el trabajo realizado en PoR beneficia a toda la red al proporcionar más potencia de transmisión. La "minería" se redefine como contribución a la capa de transmisión de datos, y la única

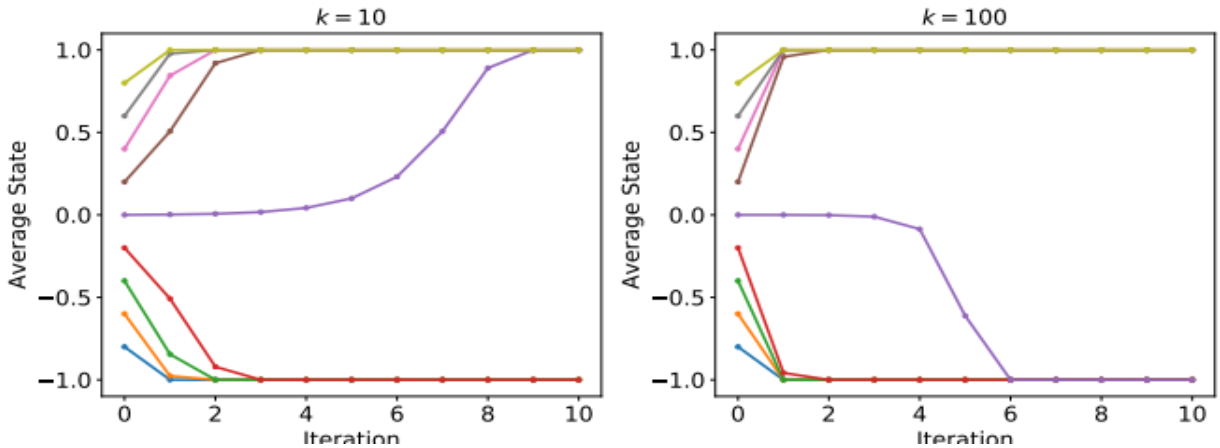

Fig. 12. El estado promedio del sistema converge a 1 o -1, ambos representan el consenso global. MVCA converge al estado de consenso que es el estado de la mayoría de los nodos en solo unos pocos pasos, incluso con solo 10 nodos vecinos en una red de nodos de 1,000,000. Aumentar la cantidad de vecinos acelera la convergencia. Tenga en cuenta que cuando exactamente la mitad de los nodos están en un estado mientras que la otra mitad en el otro estado, el estado convergente podría ser uno.

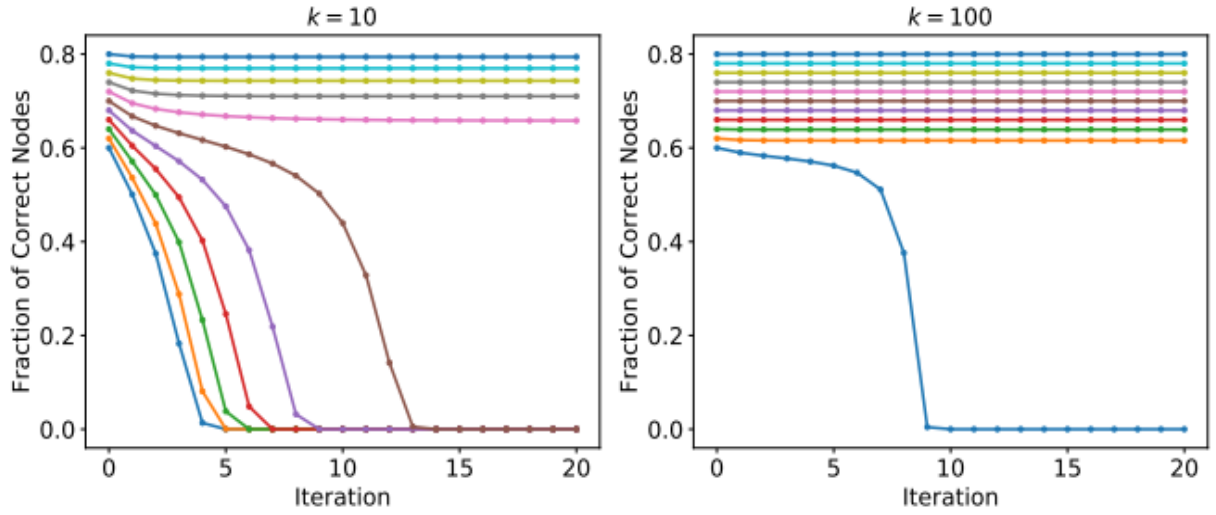

Fig. 13. Fracción de nodos correctos (estado 1) bajo el ataque de nodos maliciosos (estado -1) que no actualiza sus estados. Hay una transición entre si el sistema se colapsará al estado incorrecto cuando cambia la fracción inicial de nodos maliciosos.

forma de obtener más recompensas es proporcionar más potencia de transmisión. La competencia entre nodos en la red eventualmente conducirá al sistema hacia la dirección de baja latencia, alta red de transmisión de datos de ancho de banda. PoR se usa tanto para la extracción de tokens como para la verificación de transacciones. Por un lado, el token se recompensará con nodos para la transmisión de datos; por otro lado, la recompensa esperada para la verificación de la transacción también puede depender de PoR, ya sea mediante elección o ajuste de dificultad.

Para los algoritmos detallados y el modelo económico, consulte nuestro documento técnico amarillo separado [34] y el modelo económico Paperon [8].

5.4. Posibles ataques

Dado que NKN está diseñado teniendo en cuenta la prevención de ataques, es necesario revisar los tipos de ataques relacionados. Ataque el análisis y la mitigación serán uno de los aspectos importantes del desarrollo y el trabajo futuro de NKN, y se incluirán en el documento técnico amarillo [34].

1. Ataque de doble gasto: ataque de doble gasto se refiere al caso en el que el mismo token se gasta más de una vez. En los sistemas clásicos de blockchain, los nodos evitan el ataque de doble gasto por consenso para confirmar la secuencia de transacción.

2. Ataques de Sybil: el ataque de Sybil se refiere al caso en que el nodo malicioso pretende ser usuarios múltiples. Los mineros malintencionados pueden fingir que entregan más copias y se les paga. El reenvío físico se realiza creando múltiples identidades de Sybil, pero solo transmitiendo datos una vez.

3. Ataques de denegación de servicio (DoS): un ataque céntrico de recursos fuera de línea se conoce como ataque de denegación de servicio (DoS). Por ejemplo, un atacante puede querer apuntar a una cuenta específica e impedir que el titular de la cuenta publique transacciones.

4. Ataques de calidad de servicio (QoS): algunos atacantes quieren ralentizar el rendimiento del sistema, lo que puede reducir la cantidad de conexiones de red.
velocidad de transferencia de información y datos.

5. Ataque de eclipse: el atacante controla la red de comunicación P2P y manipula los vecinos de un nodo para que solo se comunique con los nodos maliciosos. La vulnerabilidad de la red al ataque de eclipses depende del algoritmo de muestreo entre pares, y se puede reducir eligiendo cuidadosamente los vecinos.

6. Ataques egoístas a la minería: en una estrategia minera egoísta, los mineros egoístas mantienen dos blockchains, uno público y otro privado. Inicialmente, el blockchain privado es el mismo que el blockchain público. El atacante siempre extrae en la cadena privada, a menos que la cadena pública atrape la longitud de la cadena privada, en cuyo caso el atacante publica la cadena privada para obtener recompensas. El ataque esencialmente reduce el umbral del 51% de ataque, ya que puede ser más eficiente para otros mineros a los míos. la cadena privada que la cadena pública. Sin embargo, como ataque económico, un ataque minero egoísta debe anunciarse con anticipación para atraer a los mineros.

7. Ataques de fraude: los mineros malintencionados pueden reclamar grandes cantidades de datos para ser transmitidos, pero pueden generar datos a demanda de manera eficiente mediante el uso de applets. Si el applet es más pequeño que la cantidad real de datos de retransmisión aumenta la probabilidad de que los mineros malintencionados reciban bonificaciones por bloque.

6. CONCLUSIONES

Este documento técnico presenta un camino claro y cohesivo hacia la construcción del sistema NKN. Consideramos que este trabajo es un punto de partida para futuras investigaciones sobre
conectividad de red descentralizada y transmisión de datos. El trabajo futuro incluye, entre otros, enrutamiento impulsado por CellularAutomata, consenso basado en Cellular-Automata, prueba de relé, etc. NKN tiene varias ventajas en comparación con las plataformas actuales.

Primero, NKN es una plataforma de red ideal para desarrollar aplicaciones descentralizadas. Los desarrolladores de DApp pueden centrarse completamente en las ideas creativas y las innovaciones que hacen que sus productos sean exitosos para los usuarios finales, así como también en la lógica empresarial. Ya no necesitan preocuparse por los detalles de la infraestructura de red. En segundo lugar, el modelo de incentivos de NKN alienta a más personas a unirse a la red para compartir y mejorar la conectividad de la red y la transmisión de datos, cambiando toda la estructura de la red y creando un gran mercado. NKN apunta al negocio de las telecomunicaciones de un billón de dólares y apunta a proporcionar una mejor conectividad para todos incentivando el intercambio de recursos de red no utilizados, expandiendo y revolucionando la red de intercambio.

Compare con los sistemas actuales, la plataforma NKN Blockchain es más adecuada para la transmisión de datos y la conectividad de igual a igual. Mientras tanto, este modelo autoincentivado alienta a más nodos a unirse a la red, construir una estructura de red plana, implementar enrutamiento de múltiples rutas y crear una nueva generación de estructura de transmisión de red.

Desde la perspectiva de la innovación de la infraestructura informática, NKN revolucionará el ecosistema blockchain al formar el tercer y probablemente el último pilar de la infraestructura de Internet, después de que Bitcoin y Ethereum bloquean el poder de cómputo, así como IPFS y Filecoin blockchainized storage. Complementando los otros dos pilares de la revolución de la cadena de bloques, NKN será la red descentralizada de próxima generación que se autoevoluciona, se auto incentiva y es altamente escalable.

NKN es una exploración e innovación estratégica de la infraestructura de capa de red general que entrega la red de próxima generación a otros campos. Una Internet altamente confiable, segura y descentralizada es esencial para que cada individuo y cada industria pueda alcanzar su máximo potencial en el mundo digital. NKN ofrecerá un tremendo potencial para lograr un intercambio entre pares totalmente descentralizado
sistema para hacer que Internet sea más eficiente, sostenible y seguro.

La red actual tiene grandes ineficiencias para proporcionar conectividad universal y acceso para toda la información y las aplicaciones. Es hora de reconstruir el futuro de internet.

[1] Stephen Wolfram. Statistical mechanics of cellular automata. Reviews of modern physics, 55(3):601, 1983.
[2] Stephen Wolfram. A new kind of science, volume 5. Wolfram media Champaign, 2002.
[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 2014.
[5] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.
[6] Protocol Labs. Filecoin: A decentralized storage network, 2017.
[7] Federal Communications Commission. Restoring internet freedom, 2017.
[8] NKN. NKN Economic Model and Roadmap. nkn.org, 2018.
[9] NEO. Neo white paper: A distributed network for the smart economy, 2017.
[10] Xin-She Yang and Young ZL Yang. Cellular automata networks. *Proceedings of Unconventional Computing*, pages 280–302, 2007.
[11] Carsten Marr, Mark M¨uller-Linow, and Marc-Thorsten H¨utt. Regularizing capacity of metabolic networks. *Physical Review E*, 75(4):041917, 2007.
[12] Fan Chung and Linyuan Lu. The diameter of sparse random graphs. Advances in *Applied Mathematics*, 26(4):257–279, 2001.
[13] Ali Mohammad Saghiri and Mohammad Reza Meybodi. A closed asynchronous dynamic model of cellular learning automata and its application to peer-to-peer networks. *Genetic Programming and Evolvable Machines*, 18(3):313–349, 2017.
[14] David Vorick and Luke Champine. Sia: simple decentralized storage, 2014.
[15] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. Storj a peer-to-peer cloud storage network. 2014.
[16] John Von Neumann. The general and logical theory of automata. *Cerebral mechanisms in behavior*, 1(41):1–2, 1951.
[17] John Von Neumann, Arthur W Burks, et al. Theory of self-reproducing automata. *IEEE Transactions on Neural Networks*, 5(1):3–14, 1966.
[18] David MD Smith, Jukka-Pekka Onnela, Chiu Fan Lee, Mark D Fricker, and Neil F Johnson. Network automata: Coupling structure and function in dynamic networks. *Advances in Complex Systems*, 14(03):317–339, 2011.
[19] B Chopard and M Droz. *Cellular automata*. Springer, 1998.
[20] Matthew Cook. Universality in elementary cellular automata. *Complex systems*, 15(1):1–40, 2004.
[21] John Conway. The game of life. *Scientific American*, 223(4):4, 1970.
[22] Albert-L´aszl´o Barab´asi and R´eka Albert. Emergence of scaling in random networks. *science*, 286(5439):509-512, 1999.
[23] Arati Baliga. Understanding blockchain consensus models. Technical report, Tech. rep., Persistent Systems Ltd, Tech. Rep, 2017.
[24] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
[25] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.
[26] Pavel Vasin. Blackcoins proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper.pdf*, 2014.
[27] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published* paper, August 19, 2012.
[28] BitShares. Delegated proof-of-stake consensus, 2013.
[29] Ernst Ising. Beitrag zur theorie des ferromagnetismus. *Zeitschrift f¨ur Physik*, 31(1):253–258, 1925.
[30] Mark McCann and Nicholas Pippenger. Fault tolerance in cellular automata at high fault rates. *Journal of Computer and System Sciences*, 74(5):910–918, 2008.
[31] Lud˘ek Zaloudek and Luk´a˘s Sekanina. Increasing fault-tolerance in cellular automata-based systems. In *International Conference on Unconventional Computation*, pages 234–245 Springer, 2011.
[32] Ilir C¸apuni and Peter G´acs. A turing machine resisting isolated bursts of faults. In *International Conference on Current Trends in Theory and Practice of Computer Science*, pages 16 176. Springer, 2012.
[33] Lars Onsager. Crystal statistics. i. a two-dimensional model with an order-disorder transition. *Physical Review*, 65(3-4):117, 1944.
[34] NKN. NKN Yellow Paper. *nkn.org*, 2018.
[35] Benoit B Mandelbrot. *The fractal geometry of nature*, volume 173. WH freeman New York, 1983.
[36] Michael Abd-El-Malek, Gregory R Ganger, Garth R Goodson, Michael K Reiter, and Jay J Wylie. Fault-scalable byzantine fault-tolerant services. *ACM SIGOPS Operating Systems Review*, 39(5):59–74, 2005.
[37] Kevin Driscoll, Brendan Hall, Michael Paulitsch, Phil Zumsteg, and Hakan Sivencrona. The real byzantine generals. In *Digital Avionics Systems Conference, 2004. DASC 04. The 23rd, volume 2*, pages 6–D. IEEE, 2004.
[38] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Annual International Cryptology Conference*, pages 139–147. Springer, 1992.
[39] Adam Back. A partial hash collision-based postage scheme (1997). *URL: http://www.hashcash.org/papers/announce.txt*, 2016.
[40] Vitalik Buterin. What proof of stake is and why it matters. *Bitcoin Magazine, August 26*, 2013.
[41] Rodney J Baxter. *Exactly solved models in statistical mechanics*. Elsevier, 2016.
[42] Catarina Cosme, JM Viana Parente Lopes, and Jo˜ao Penedones. Conformal symmetry of the critical 3d ising model inside a sphere. *Journal of High Energy Physics*, 2015(8):22, 2015.
[43] Bertrand Delamotte, Matthieu Tissier, and Nicol´as Wschebor. Scale invariance implies conformal invariance for the three-dimensional ising model. *Physical Review E*, 93(1):012144, 2016.
[44] Sheer El-Showk, Miguel F Paulos, David Poland, Slava Rychkov, David Simmons-Duffin, and Alessandro Vichi. Solving the 3d ising model with the conformal bootstrap. *Physical Review D*, 86(2):025022, 2012.
[45] Leemon Baird. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. Technical report, Swirlds Tech Report SWIRLDS-TR-2016-01, available online, http://www. swirlds. com/developer-resources/whitepapers, 2016.
[46] Arnab Mitra, Anirban Kundu, Matangini Chattopadhyay, and Samiran Chattopadhyay. A novel design with cellular automata for system-under-test in distributed computing. *Journal of Convergence Information Technology*, 9(6):55, 2014.
[47] Steven Janke and Matthew Whitehead. Practical fault tolerant 2d cellular automata.
[48] Yoshihiko Kayama. Complex networks derived from cellular automata. *arXiv preprint arXiv:1009.4509*, 2010.