Sociedad y Economía
DOI: 10.1556/204.2019.007

BLOQUEO Y DEMOCRACIA[1]

PETER RACSKO

Departamento de Sistemas de Información, Universidad Corvinus de Budapest, Hungría
Correo electrónico: peter.racsko@uni-corvinus.hu

En los últimos años, en muchos países, la gente ha experimentado la erosión de la confianza en los principales pilares de la democracia, los sistemas electorales y de votación. Muchos autores ven la tecnología blockchain como una herramienta para restaurar la confianza (Tapscott 2016; Swislow 2016; Shin 2016). Nuestra investigación tiene como objetivo el uso potencial de la tecnología blockchain en los sistemas sociales para mejorar la confianza y aumentar la participación. Nuestro objetivo es explorar si la tecnología blockchain es adecuada para votar o elecciones en grandes comunidades y los problemas que se abordarán para las aplicaciones del mundo real para aprovechar los derechos democráticos. Nuestra conclusión final es que existen obstáculos tanto teóricos como prácticos en el camino de tales aplicaciones directas.

Palabras clave:blockchain, protocolo de consenso, votación

Códigos JEL:C88, D72, O33

1. INTRODUCCIÓN

Blockchain es una memoria digital colectiva de un grupo de personas. Es un registro digital seguro de un conjunto de transacciones. No existe un método práctico para cambiar la cadena de bloques sin que esta interferencia pase desapercibida para los controladores o el público. No proporcionamos una descripción completa de la tecnología criptográfica y de red utilizada para configurar y mantener una cadena de bloques pública.

[1] Este trabajo fue creado en el marco de la Universidad Nacional de la Función Pública bajo el proyecto prioritario KÖFOP-2.1.2-VEKOP-15-2016-00001 titulado “Desarrollo de la Función Pública Estableciendo Buena Gobernanza”.

ver Satoshi Nakamoto (2008) para esto. Tampoco discutimos el impacto económico de Bitcoin u otras criptomonedas, y solo nos enfocamos en la aplicación potencial de blockchain como tecnología básica para proporcionar un marco seguro para las elecciones y los sistemas de votación. La discusión de la tecnología solo se involucrará en la medida necesaria para comprender el contenido.

La seguridad de la cadena de bloques la proporciona una tecnología de información específica. Después de cada adición de nuevas transacciones a una cadena de bloques, se agrega a la cadena una huella digital, llamada hash. Para obtener una explicación completa de la tecnología, consulte, por ejemplo, Antonopoulos (2017). Después de agregar un nuevo bloque a la cadena de bloques existente, se genera un nuevo hash a partir de la cadena anterior, los hash anteriores y el nuevo bloque, por lo que cambiar las transacciones anteriores después es prácticamente imposible, ya que los hash antiguos se pueden reproducir a partir de datos modificados intencionalmente con una probabilidad muy cercana a cero. El cálculo de los valores hash requiere algún trabajo u otro tipo de recursos por parte de los participantes, quienes a su vez deben ser compensados por su esfuerzo. Sin motivación, quizás nadie se haga cargo del mantenimiento de la cadena de bloques. El método de compensación hace una diferencia sustancial en varias aplicaciones. Por ejemplo, la compensación por calcular un hash en el sistema Bitcoin ahora es de 12,5 Bitcoins, y bajará a 6,25 alrededor de 2020. La compensación alta es razonable ya que los verificadores no solo tienen que generar un hash ordinario, sino uno muy especial. con un número prefijado de ceros a la izquierda, y esta operación requiere mucha potencia computacional y un poco de suerte. Los Bitcoins utilizados para la compensación son monedas recién acuñadas y se agregan a los recursos generales. A medida que aumenta el número de ceros iniciales requeridos, también aumenta el tiempo de cálculo requerido. En promedio, la generación de un nuevo bloque tarda aproximadamente diez minutos en toda la red de Bitcoin, por lo que se agrega un nuevo bloque a la cadena de bloques existente una vez cada diez minutos. El cálculo requiere no solo poder de procesamiento, sino también algo de suerte al generar un número aleatorio (llamado nonce), que se agrega al bloque real para producir el hash con los atributos requeridos. Los verificadores están en un concurso permanente, y el primero en la generación de hash adecuada es el ganador, y su solución es aceptada por los demás después de ser transmitida en la red pública. El ganador se lleva todo el incentivo. Esta operación se llama minería de Bitcoin. Uno puede comprar hardware especialmente diseñado para la minería de Bitcoin en el mercado en línea o usar tarjetas de procesador gráfico. La única restricción para la verificación y generación de nuevos Bitcoins es el razonamiento económico. La ganancia esperada debe ser mayor que el costo de la energía y el tiempo de computadora utilizados para la minería. A medida que la complejidad de la minería aumenta continuamente, el incentivo económico para la verificación está disminuyendo. No se conocen con exactitud las consecuencias de la disminución del incentivo para el sistema Bitcoin, pero ya se han encontrado más del 80% de los posibles recursos bitcoin.

Usamos el ejemplo de Bitcoin para demostrar la importancia de la verificación de las transacciones. La estructura de la cadena de bloques y las aplicaciones creadas en el marco de la cadena de bloques no funcionarán sin un método de verificación sostenible. En aplicaciones diferentes a Bitcoin, se pueden aplicar varios otros marcos de verificación y compensación, como por ejemplo voluntarios o empleados pagados, cuyo trabajo es el cálculo de hashes (uno con mucha menos complejidad que en Bitcoin). El valor hash se puede calcular muy rápida y fácilmente incluso para bloques grandes, si no se requieren las condiciones específicas como en el caso de Bitcoin. El objetivo final del proceso es incluir todas las transacciones en la cadena de bloques y "sellar" todos los bloques con un código hash, que se transmite en la red y es aceptado por los participantes.

El sistema Bitcoin, sin embargo, no funciona si la mayoría (al menos el 51%) de los participantes deciden cooperar en una acción de trampa. Si la red es lo suficientemente grande, incluso los grandes consorcios tienen mucho menos del 51% del poder. Vale la pena mencionar que si se cumplen ciertas condiciones, la cooperación del 25% de los participantes es suficiente para un llamado ataque económico (Buterin 2016), que, en sentido estricto, no es un truco técnico. En una red más pequeña, menos pública y con un número menor de participantes, la condición necesaria para el funcionamiento es la confiabilidad de la mayoría de las partes interesadas.

El papel de la memoria colectiva no es nuevo en la sociedad. El propietario y el valor de las “monedas” en la isla de Yap en Micronesia, por ejemplo, se almacenaron solo en la memoria de la población local (Friedmann 1991). Los medios de intercambio eran grandes ruedas de piedra maciza, cuyo diámetro oscilaba entre un pie y doce pies. El valor de una rueda en particular fue acordado por la sociedad local en base al trabajo invertido en el tallado y transporte de la piedra. Las monedas de piedra tenían su ubicación fija en la isla, nunca se movían aunque se cambiara de dueño. Cuando se cambiaba el propietario en una transacción de compraventa, el vendedor y el comprador simplemente informaban a sus vecinos acerca de la transacción. Así, el propietario y el valor de las monedas existían solo en la memoria colectiva de la sociedad local.

De hecho, la cadena de bloques es una base de datos de todas las transacciones pasadas. Las copias exactas de la base de datos se almacenan en varios puntos de la red. Las bases de datos transaccionales tradicionales generalmente son configuradas, operadas y controladas por completo por una organización central. La ubicación fija de la base de datos podría servir como un objetivo bien definido para los piratas informáticos, que pueden querer robar o manipular los datos. La organización operadora de la base de datos aplica todas las contramedidas a su alcance, pero la motivación de los piratas informáticos es bastante fuerte. Los bancos, por ejemplo, hacen un esfuerzo importante para evitar

acciones maliciosas, pero a pesar de estos esfuerzos, los robos de datos o dinero de los bancos de forma electrónica no son eventos raros. Si esas bases de datos fueran públicas, cualquiera podría hacer y almacenar una copia, luego cualquiera podría verificar la integridad de la base de datos comparándola con las otras copias. El almacenamiento distribuido y la falta de una organización de control central en la cadena de bloques evitan los ataques de piratas informáticos o la manipulación de una base de datos central, ya que las copias de la base de datos existen en varios nodos de la red.

Surge una pregunta natural al agregar datos de transacciones a los bloques, y el cambio debe transmitirse en la red. Qué nodo con una copia de la cadena de bloques decidirá si un cambio es válido o no y cuál es el orden correcto de la transacción. Las transacciones pueden sucederse en una fracción de segundo y, en una infraestructura de pago, el orden de las transacciones es vital por razones obvias. Si no hay un consenso general sobre la validez y el orden de las transacciones, el conjunto de copias de blockchain se desincroniza rápidamente y nadie sabrá qué copia es válida.

Si los usuarios del sistema acordaran un orden fijo de las computadoras que verifican las transacciones, el primer verificador tendría una posición privilegiada y podría influir en la modificación de la base de datos por su cuenta. Esta opción contradice claramente los principios originales basados en la igualdad de oportunidades de los participantes. Si esta computadora privilegiada falla, todo el proceso fallará. Si los participantes elaboran un algoritmo de ordenación, la pregunta es quién decide sobre el algoritmo en sí. Como se puede ver, la sincronización de todas las copias en la red no es una tarea fácil si los participantes requieren un acuerdo total sobre el mecanismo de verificación.

La solución en todos los casos es un conjunto de reglas, aceptadas por todos los participantes. El nombre de este conjunto de reglas es el*protocolo de consenso*. Un sistema de cadena de bloques operativo siempre se basa en su protocolo de consenso, que determina los nodos que tienen derecho a iniciar o validar los cambios en los nodos y el orden de las transacciones. El protocolo de consenso garantiza la sincronización de todos los nodos en cualquier instante de tiempo y evita la modificación o los datos por parte de cualquier nodo en particular. Como resultado de la correcta aplicación del protocolo de consenso, todos los participantes del sistema blockchain tendrán la oportunidad de verificar la integridad de la base de datos.

Cada bloque en una cadena de bloques contiene una referencia al bloque anterior y, por lo tanto, el orden de las transacciones verificadas se fija para siempre. Con esta propiedad, un nuevo participante puede reproducir toda la cadena de bloques desde el primer bloque (genesys) y puede verificar si alguna vez se manipuló toda la cadena de bloques.

2. VOTACIÓN CON BLOCKCHAINS

Los sistemas de votación en línea con hardware de votación electrónica se han utilizado ampliamente en algunos países, pero debido a varios problemas administrativos y de seguridad, no se han ganado una confianza inequívoca. Según MSNBC (2011), los investigadores han desarrollado un truco: por alrededor de $26 y un 8elgrado de educación científica, uno puede manipular de forma remota las máquinas de votación electrónica utilizadas por millones de votantes en todo EE. UU. Otro periódico de EE. Los expertos en seguridad dicen que un tipo específico de máquina de votación electrónica es vulnerable a ser pirateado. Influir en una elección nacional sería difícil, pero el avance del malware lo hace posible. El documental de HBO Hacking Democracy también cuestiona la confiabilidad de la votación en línea.

Se supone que la aplicación de blockchain en la votación en línea aumentará la confianza en conflicto en la votación electrónica. Investigaciones recientes muestran el creciente interés en la implementación de la tecnología blockchain en la votación en línea. Se han propuesto muchos esquemas, aunque, lamentablemente, no se dispone de documentación técnica completa. En un artículo publicado por Hardwick et al. (2018), los autores proponen un protocolo de votación electrónica potencialmente nuevo que utiliza la cadena de bloques como una urna transparente. Ofrece una descentralización limitada y permite que el votante cambie/actualice su voto (dentro del período de votación permitido). El documento también destaca los pros y los contras de usar blockchain para tal propuesta desde un punto de vista práctico tanto en el desarrollo/ implementación como en el uso. Ayed (2017) aboga por aprovechar la tecnología de cadena de bloques de código abierto y propone un diseño para un nuevo sistema de votación electrónica que podría usarse en las elecciones. El documento también traza una hoja de ruta para que la tecnología blockchain pueda admitir aplicaciones complejas. McCorry et al. (2017) describen un sistema de votación blockchain en la sala de juntas, la "Red de votación abierta", que es adecuado para las elecciones en la sala de juntas y está escrito como un contrato inteligente para Ethereum. Mora et al. (2017), en una presentación en una conferencia, argumentó que los métodos actuales, especialmente aquellos basados en plataformas electrónicas, “ofrecen niveles insatisfactorios de transparencia a los votantes, perjudicando así la confianza que los votantes tienen en el conteo de su voto por parte de los funcionarios electorales, un problema conocido como confianza de los votantes”. En cambio, sugieren la modernización de las estructuras estatales mediante el uso de tecnologías emergentes. En un Whitepaper de Bitcongress (Bit-Congress 2016) se propuso un sistema de votación basado en bitcoin, con mayor descripción y crítica en Caiazzo (2016). En su sitio web, Followmyvote. com (2017) ofrece una descripción general de su ambición de “construir una plataforma de votación en línea segura que permita una mayor transparencia electoral”.

En 2018, se probaron sistemas de votación electrónica basados en blockchain en algunos países; sin embargo, el análisis de los resultados aún no se ha publicado. Para examen-

Por ejemplo, Corea del Sur desarrolló un sistema de votación blockchain para el sector privado que fue sometido a prueba en diciembre de 2018 (Zdnet 2018).Las encuestas en las elecciones primarias de Virginia Occidental el 8 de mayo de 2018 utilizaron la primera votación respaldada por blockchain administrada por el gobierno enHistoria de estados unidos. La plataforma de votación móvil basada en blockchain solo estaba disponible para un grupo selecto de votantes(Cointelegraph 2018).

3. PROTOCOLOS DE CONSENSO

La tecnología blockchain aplicada depende en gran medida del método de verificación de la validez de los bloques. Hay varios procesos diferentes (protocolos de consenso) para crear un consenso de las partes interesadas sobre la validez de los datos inspeccionados. Son diferentes en varios aspectos, por ejemplo, tipo y cantidad de recursos requeridos, número de "censores", etc. Un protocolo de consenso es una parte integral de la aplicación de cadena de bloques dada y, por lo tanto, la aplicación misma en todos los aspectos depende del protocolo. Analizaremos los protocolos de consenso más utilizados de las aplicaciones blockchain. Mostraremos que ninguno de ellos es perfecto para un sistema de votación electrónica basado en blockchain.

Primero, demos las definiciones de alto nivel de los protocolos más importantes. Las definiciones son descriptivas más que formales ya que todos los protocolos tienen variantes debido a diferentes implementaciones.

Prueba de participación(PoS): un protocolo mediante el cual una red de cadena de bloques tiene como objetivo lograr un consenso distribuido. En las cadenas de bloques basadas en PoS, el validador de las transacciones se elige a través de la riqueza u otro interés en la cadena de bloques ("la participación").

Prueba de trabajo(PoW): el algoritmo de las cadenas de bloques basadas en prueba de trabajo resuelve tareas matemáticas computacionalmente intensivas (es decir, minería) para validar transacciones y crear nuevos bloques. El éxito del minero depende de sus recursos informáticos y de su suerte.

Prueba de tiempo transcurrido(PoET): este algoritmo se usa a menudo en redes blockchain donde los participantes compiten por los derechos mineros. Basado en sorteos aleatorios, donde cada nodo tiene la misma oportunidad de obtener los derechos de minería, se requiere que el nodo en la red espere un período de tiempo elegido al azar, y el primero en completar el tiempo de espera designado gana el nuevo bloque (Investopedia 2018a).

Prueba de Capacidad(PoC): un algoritmo que permite que los dispositivos de minería en la red usen su espacio disponible en el disco duro para decidir los derechos de minería. Cuanto mayor sea el espacio en disco disponible, mayores serán las posibilidades de que un nodo obtenga los derechos de minería (Hackernoon 2018).

Prueba de quemadura(PoB): este algoritmo funciona según el principio de permitir que los nodos que participan en la verificación de las transacciones "quemen" o "destruyan" los tokens de moneda virtual, lo que les otorga el derecho de escribir bloques en

proporción a las monedas quemadas. Quemar una moneda significa enviar la moneda a una dirección conocida públicamente donde no se pueden recuperar las monedas (Bitcoin.it 2018).

Prueba de actividad(PoA): un híbrido de PoW y PoS. En PoA, el proceso de minería comienza como un proceso PoW estándar con varios mineros que intentan superarse unos a otros con mayor poder de cómputo para encontrar un nuevo bloque. Cuando se encuentra (mina) un nuevo bloque, el sistema cambia a POS, y el bloque recién encontrado contiene solo un encabezado y la dirección de recompensa del minero.

Los tipos de protocolos de consenso no se limitan de ninguna manera a los cinco más populares, se pueden inventar protocolos nuevos e innovadores en cualquier momento (Ahmed et al. 2019).

Discutamos algunos de los detalles, comenzando con el protocolo de consenso de Bitcoin (PoW), como la aplicación más utilizada de la tecnología blockchain. El conjunto de reglas en el protocolo, entre otros, define los tipos de cambios en la base de datos, la hora en que se producen los cambios y los participantes que están autorizados para iniciar un cambio, o para hacerlo simple, cómo y cuándo se puede agregar un bloque a la cadena de bloques Las reglas aseguran que los datos de la transacción se agregarán a la base de datos de una manera inequívoca e inalterable, y la modificación es acordada por todos los participantes y ningún nodo individual o un pequeño grupo de nodos tiene la capacidad de controlar la adición de las transacciones a la base de datos. cadena de bloques.

El protocolo PoW es operado por aquellos usuarios activos que sacrifican importantes recursos informáticos para participar en la integración de nuevos bloques. Resuelven un problema informático complejo (llamado minería) y transmiten el resultado de manera que cualquier otro participante pueda verificar la validez de la solución de una manera fácil y rápida y pueda verificar la solución para el público. El reconocimiento ayuda en la aceptación del nuevo bloque y acepta la operación minera exitosa y la compensación del minero. La aplicación del protocolo de consenso PoW es inevitable con cada bloque, ya que proporciona claridad de las transacciones para prohibir el gasto doble de la misma moneda y el orden correcto. Si alguien quiere manipular una transacción, la copia de la cadena de bloques completa debe modificarse y todos los PoW anteriores deben volver a calcularse. mientras que todas las demás copias permanecerán sin cambios. Técnicamente, para un fraude exitoso, se requiere al menos la mitad de la capacidad informática total de los participantes. Como demostró Eyal (2013), un ataque "económico" no técnico es posible, es decir, un cartel de participantes con fines de lucro puede engañar al sistema incluso si sus recursos son menores que la mitad de las capacidades de la red.

Los gastos asociados al protocolo PoW son claramente una desventaja y la actividad minera está limitada en el tiempo: cuando el gasto medio de minar un bitcoin supera su valor, el incentivo para los mineros desaparece y el protocolo de consenso ya no funcionará.

Otro protocolo popular,*Prueba de participación,*se introdujo para otra criptomoneda, Nextcoin. La verificación del tipo de PoS no requiere una capacidad informática significativa ni sacrifica otros recursos. Tampoco requiere mucha energía eléctrica. Como resultado, el sistema está más descentralizado en la práctica como en el caso de Bitcoin, donde los participantes con mayores recursos están en una posición privilegiada. Incluso un teléfono inteligente es capaz de verificar un bloque con el esquema PoS. La aplicación Nextcoin utiliza un protocolo PoS de la siguiente manera. Un generador de números aleatorios selecciona una Nextcoin cada 60 segundos (todas las monedas cuentan con un número de serie) y el propietario de la moneda seleccionada tiene derecho a realizar la verificación. Si la computadora de la parte seleccionada está en línea, recopila todas las transacciones nuevas no verificadas, forma un bloque y lo transmite en la red. El participante recibe una pequeña recompensa. Si la computadora está fuera de línea, la red selecciona un nuevo verificador y no se le pagará a la persona seleccionada originalmente. La fuerza impulsora detrás de la operación continua del sistema Nextcoin es que las personas que poseen más nextcoins no apagarán sus computadoras, ya que la probabilidad de ser seleccionado para verificación y compensación es mayor, lo que genera mayores ingresos. El número de Nextcoins se fija desde el lanzamiento del sistema en mil millones. ya que la probabilidad de ser seleccionado para la verificación y compensación es mayor, produciendo un mayor ingreso. El número de Nextcoins se fija desde el lanzamiento del sistema en mil millones. ya que la probabilidad de ser seleccionado para la verificación y compensación es mayor, produciendo un mayor ingreso. El número de Nextcoins se fija desde el lanzamiento del sistema en mil millones.

A diferencia del caso del protocolo PoW, la capacidad de verificación de un propietario de Nextcoin no se define por su capacidad informática, sino por el saldo real de su cuenta. Los expertos de PoS suponen que los participantes con mayor saldo están más expuestos y cuidan mejor su inversión, ya que un ataque exitoso contra el sistema reduce la confianza en la moneda y, en consecuencia, disminuye el valor de la inversión. Si una parte interesada (o un grupo de partes interesadas que cooperan) adquiere el 51 % de todas las Nextcoins, es capaz de modificar la cadena de bloques. Como la cantidad total de Nextcoins es limitada, el precio de mercado de una moneda aumentará debido al aumento de la demanda, pero el valor de intercambio disminuirá y, al final, el fraude no dará sus frutos. En el caso del protocolo PoW, para un fraude exitoso se requiere una alta concentración de recursos, y el costo unitario de los recursos disminuye a medida que aumenta la concentración. Como resultado, el costo unitario de aumentar la influencia de uno disminuye en el proceso de PoW, mientras que aumenta en el caso de PoS.

4. USO POTENCIAL DE LA TECNOLOGÍA BLOCKCHAIN EN UN SISTEMA DE VOTACIÓN EN LÍNEA

En un sistema de votación en línea, un voto emitido equivale a una transacción. Cada transacción se adjunta a una cadena de bloques. Con el uso de un protocolo de consenso adecuado (por ejemplo, PoW o PoS), la cadena de bloques no se puede alterar y si se vota

perdido, o agregado posteriormente, será evidente para todos los participantes. El resultado final debe ser aceptado por todos, ya que todos pueden verificar si hubo votos ilegales o si alguien cambió los votos y, además, todos los votos se contaron una vez y solo una vez.

No cabe duda de que la aplicación de la tecnología blockchain resuelve algunos problemas planteados en la práctica electoral de bastantes países. Por ejemplo, en el año 2000 en Florida hubo que contar los votos, lo mismo sucedió en 2016 en algunos otros estados de EE.UU. Además, se hizo evidente que los piratas informáticos pueden influir en los sistemas de votación en línea u otros recursos de información de las elecciones. Los supuestos errores o las actividades de los piratas informáticos no cambiaron los resultados en 2000 o 2016, pero se cuestionó la confianza en la imparcialidad de los sistemas de votación y no existen métodos seguros para restaurar la confianza perfecta.

De acuerdo con los críticos de los sistemas de votación electrónica, la seguridad indiscutible solo la proporciona un proceso basado en papel. Sin embargo, en una sociedad contemporánea, los votantes no quieren esperar semanas por los resultados y no hay forma de garantizar la imparcialidad del proceso de escrutinio. Es imposible detectar el fraude, cambiar un voto o agregar votos ilegítimos. La imparcialidad del sistema depende completamente de la imparcialidad de los seres humanos participantes, y un grupo relativamente pequeño de personas que son responsables del conteo están en condiciones de influir en los resultados. Cuanto mayor sea el número de votantes en un sistema basado en papel, la opción de hacer trampa es mayor debido a la creciente complejidad del control.

Sin embargo, la aplicación de la tecnología blockchain podría garantizar la imparcialidad de la votación con una alta confianza estadística, con una probabilidad cercana a 1. Cada votante puede verificar que los votos no fueron manipulados con una probabilidad cercana a 1, y en este caso no no es necesario hacer un recuento de los votos que desafían la confianza en el sistema. Otra ventaja es el resultado final inmediato. La tecnología blockchain, sin embargo, es una herramienta real solo para una elección si se diseña e implementa de manera pragmática. El resto de este artículo discute los problemas prácticos de las aplicaciones reales.

5. SISTEMAS SIN CONFIANZA

El concepto de sistemas sin confianza es muy intrigante. Un sistema sin confianza funciona sin necesidad de confianza en los elementos del sistema. Discutimos los aspectos pragmáticos de la falta de confianza. Un sistema de transacciones computarizado como una aplicación de TI, por ejemplo, transferencia de dinero, se basa tradicionalmente en el hecho de que la fuente de la transacción, la infraestructura de comunicación y todos sus elementos y redes, y las personas que trabajan en el sistema y también todas las organizaciones

involucrados son confiables. Confiabilidad significa en este contexto que el riesgo de errores deliberados o aleatorios es aceptable para los usuarios. O el impacto potencial de un incidente es insignificante, o la probabilidad de que ocurra es pequeña, o hay un tercero, por ejemplo, una compañía de seguros, que reembolsa el daño.

Las transferencias de dinero tradicionales se consideran confiables ya que los bancos tienen la responsabilidad total de la infraestructura y las transacciones exitosas. La confianza en el sistema bancario se ve reforzada por el conocimiento de que no solo el banco, sino un tercero, por ejemplo, el gobierno o una compañía de seguros garantiza la transacción. La operación confiable y sin errores es el interés comercial directo de la organización operadora.

Los ejemplos de pérdida de confianza en los sistemas monetarios, como ocurrió en 2008, plantearon la cuestión de la existencia de un verdadero sistema transaccional donde la confianza no es una condición necesaria de la operación, donde se supone que los participantes no deben confiar entre sí ni en el sistema mismo. La construcción de blockchain es una de las soluciones candidatas. En el caso de Bitcoin, cada participante puede verificar la validez de todas las transacciones, todos pueden estar seguros de que no se cometieron errores o que nadie alteró los datos. En el sistema Bitcoin, el iniciador de una transacción transmite transacciones firmadas electrónicamente y todas las partes pueden verificar la validez de la firma. Las transacciones no validadas simplemente son eliminadas por el sistema. Los mineros validan el bloque de transacciones y las partes pueden verificar la validez.

Un sistema de cadena de bloques, como se usa para las criptomonedas, es de hecho un sistema de confianza distribuida en lugar de un sistema sin confianza (Tomaino 2016). Los participantes en realidad tienen que confiar en varias partes: los validadores de las transacciones, la solidez de los métodos criptográficos aplicados, los desarrolladores que mantienen y mejoran el código y los usuarios de la plataforma. Pero la confianza se distribuye, por lo que no se confía en ninguna de las partes.

En teoría, el protocolo de consenso de Bitcoin o mecanismos similares proporcionan la condición para una operación de confianza distribuida, al menos en teoría no requiere la participación de un solo tercero de confianza. Pero el sistema no excluye la existencia de una tercera parte única confiable o no confiable. Sin embargo, la operación "Hard Fork" de la criptomoneda Ethereum en 2016 demostró que el pasado de la cadena de bloques se puede cambiar (Coindesk 2016a). El Hard Fork fue llevado a cabo por los fundadores para recuperar 60 millones de dólares robados por piratas informáticos que explotaron una vulnerabilidad en el software. La controvertida acción demuestra que la censura central no es impensable y los participantes tienen que confiar en los fundadores.

Como lo muestra claramente Noizat (2015): “los sistemas de votación electrónica existentes adolecen de un grave defecto de diseño: son propietarios, es decir, centralizados por

diseño, lo que significa que hay un solo proveedor que controla el código base, la base de datos y las salidas del sistema y suministra las herramientas de monitoreo al mismo tiempo", lo que contradice la idea de confianza distribuida.

Sin embargo, las cadenas de bloques pueden ayudar en la auditabilidad del sistema de votación, ya que los cambios al menos no pasan desapercibidos. Pero existe la necesidad de un protocolo de consenso adecuado y práctico, aceptado por los participantes. Discutiremos más adelante la potencial aplicación de protocolos de consenso para los sistemas de votación. En nuestra opinión, la tecnología blockchain no elimina por completo los riesgos asociados con la votación, sino que reorganiza el panorama de riesgos.

6. RIESGO A NIVEL DE SISTEMA: ATAQUE ECONÓMICO

Llamamos a este tipo de riesgo económico, ya que se demostró el potencial para un ataque exitoso en el caso de Bitcoin. Eyal y Sirer (2015) demostraron que una estrategia fraudulenta pero rentable de un número relativamente pequeño de participantes puede motivar a otros a unirse al grupo del tramposo y manipular la cadena de bloques, ya que la ganancia esperada del grupo tramposo es mayor que la de los participantes honestos. . Cuando el grupo controla el 51% de los recursos puede modificar la cadena de bloques. La estrategia no es perfecta (Buterin 2016), pero en el caso de una elección, donde un pequeño número de grupos luchan por el control total, el riesgo es claro. Como muestran los experimentos de simulación, el 25% de los participantes pueden tomar el control del sistema.

7. RIESGOS DE SEGURIDAD

Las infraestructuras blockchain son sistemas de información y quizás no estén libres de vulnerabilidades. Los puntos débiles de Bitcoin, por ejemplo, se analizan en Bitcoin.it (2019), pero podemos agregar otros factores de riesgo, como el ataque de denegación de servicio o un ataque específico de Sybill, cuando una computadora ejecuta varios clientes simultáneamente para aumentar su impacto. Otro factor de riesgo es el ataque de "timejacking", cuando los piratas informáticos manipulan la hora de la red y las marcas de tiempo de la transacción no serán válidas. Los objetivos bien conocidos son las billeteras, protegidas por una criptografía relativamente débil, intercambios de claves de firma débiles y programas de firma. Se pueden repeler todos los tipos de ataques conocidos, pero el alto beneficio potencial de un ataque exitoso contra Bitcoin es motivación suficiente para soluciones innovadoras.

8. PROBLEMAS PRÁCTICOS DE LA APLICACIÓN BLOCKCHAIN EN LOS SISTEMAS DE VOTACIÓN

La tecnología blockchain claramente no es suficiente para construir un sistema de votación seguro y confiable de extremo a extremo. En un entorno de votación en línea, el votante debe certificar su autoridad para votar, y los documentos electrónicos que certifican el derecho de voto deben distribuirse en un procedimiento fuera del marco de la cadena de bloques.

Este detalle es diferente a los principios aplicados en los sistemas monetarios donde el derecho a gastar una moneda se certifica dentro del sistema, como resultado de la confianza distribuida. La autorización externa contradice el principio de falta de confianza, o más exactamente, confianza distribuida, cuando la confianza se distribuye entre un gran número de participantes y así asegura un funcionamiento justo. Por supuesto, la votación múltiple o la pérdida de votos pueden evitarse fácilmente mediante los protocolos PoW y PoS en un marco de cadena de bloques.

Hay algunas empresas y fundaciones sin fines de lucro en el mercado que desarrollan y ofrecen un sistema de votación basado en blockchain como servicio (FollowMyVote. com 2017). Por el momento, sin embargo, no existen sistemas aplicables a efectos prácticos. La tecnología blockchain podría ser una base tecnológica prometedora para un sistema de votación en línea confiable y rápido en el futuro, pero aún quedan bastantes problemas teóricos y técnicos por resolver. Para la certificación del derecho al voto de una persona, una tarjeta de identidad con chip podría ser una solución, ya que la tarjeta contiene un identificador personal a prueba de manipulaciones, y el derecho al voto podría estar claramente definido. Por supuesto, existe la necesidad de una base de datos de autorización central con los datos de identidad de los votantes legales. Los votantes deben confiar en el propietario de esta base de datos central,

En consecuencia, en caso de que los votantes controlen completamente todo el sistema, la base de datos de las credenciales de los votantes debe operar en una cadena de bloques. Es decir, los registros oficiales de votantes deben estar organizados en una cadena de bloques y las autorizaciones asignadas de forma normativa y controlable. Sin embargo, es necesario abordar el problema de los protocolos de consenso. Ni la velocidad actual ni el modo de operación son aplicables en sistemas de votación reales.

En el caso de Bitcoin, el uso del protocolo PoW supone que unirse a un nuevo bloque de aproximadamente 700 transacciones toma 10 minutos, el tamaño de un bloque es de 1 MByte, la cantidad de transacciones por segundo es entre 1 y 3,5 segundos cuando las transacciones son de tamaño medio. Estos parámetros no están controlados por un dispositivo informático u organización central, sino que están determinados por el tiempo de cálculo necesario según la complejidad del trabajo y el tiempo de comunicación. Con

el crecimiento general de la potencia informática, el período de 10 minutos podría disminuir, pero en este caso el sistema aumenta automáticamente la complejidad de la prueba. Estas limitaciones, por supuesto, no son muy amigables, y surge la necesidad de un protocolo de consenso fácilmente escalable.

Eya et al. (2016) definen un algoritmo de “próxima generación” (NG), donde el retraso depende solo de la transferencia de datos, y la cantidad de datos transferidos está definida por la capacidad de procesamiento. Si el algoritmo NG puede demostrar sus ventajas en el futuro en un entorno real, la baja velocidad de funcionamiento de la cadena de bloques no será un obstáculo para las aplicaciones prácticas.

Otra cuestión a tratar es quién reembolsará los costos ocurridos en la verificación, quién pagará a los verificadores por usar una cantidad considerable de recursos de cómputo y energía eléctrica, incluso en el caso de protocolos PoW escalables. La forma actual del protocolo PoW, incluso su versión NG, es difícilmente aplicable en un marco de votación.

Discutamos otros protocolos de consenso y su uso práctico. El supuesto básico del protocolo PoS es que un gran número de participantes están continuamente activos, es decir, están en línea. Sin embargo, si la mayoría de los votantes quieren sabotear el sistema, pueden desconectarse y el número cada vez mayor de transacciones por verificar ralentizará el sistema, y tal vez podría ocurrir una situación específica de denegación de servicio. El problema de las recompensas también es un problema. En un sistema de votación cada participante tiene un solo voto y por lo tanto nadie tiene mayor incentivo que los demás para utilizar recursos para la verificación. Así, desaparece el importante factor de motivación que opera las criptomonedas con el PoS.

El protocolo PoET fue propuesto por Intel Corporation. El algoritmo es similar al procedimiento PoW, pero con un consumo de energía mucho menor. Los nuevos bloques se crean en el hardware específico diseñado por Intel para este propósito, pero no requiere una solución computacionalmente intensiva de problemas matemáticos (Coindesk 2016b). Claramente, esta no es una solución de confianza distribuida o sin confianza, ya que los participantes deben confiar en el fabricante del hardware como un tercero. Sin embargo, la mayoría de los usuarios de la cadena de bloques comparten la opinión de que la cadena de bloques y la falta de confianza (o al menos la confianza distribuida) van de la mano.

El protocolo PoC es una forma de "pago por el esquema de participación", similar a PoW. El verificador potencial paga con su capacidad de almacenamiento. Cuanto mayor sea la capacidad de almacenamiento que ofrezca el participante, mayor será la probabilidad de ser seleccionado como verificador del siguiente bloque y ser reembolsado por el trabajo. La criptomoneda Burstcoin utiliza el protocolo PoC. En un procedimiento de votación real, es difícil suponer que un número significativo de votantes ofrecerá capacidad de almacenamiento sin recompensa. Sin embargo, un pequeño número de verificadores no garantiza la distribución aleatoria de la confianza.

En el caso de PoB, alguien que quiera participar en el procedimiento de validación debe pagar la actividad en una billetera central. El pago único se “quema”, ya que nadie recupera el dinero, solo garantiza el derecho a participar en un sorteo aleatorio donde el ganador tiene derecho a verificar un bloque y ser recompensado. El pago se acepta en la moneda nativa o en monedas externas al sistema. Aquellos participantes que pagan más tienen una mayor probabilidad de ganar, es decir, ser seleccionados para la verificación y recompensados. A medida que aumenta el número de contribuyentes, las posibilidades de ser seleccionado disminuyen, por lo que si uno quiere mantener su posición, debe realizar pagos adicionales. El sistema fue utilizado por la criptomoneda Slimcoin, con un éxito muy moderado. Este protocolo contradice claramente los principios democráticos de un sistema de votación contemporáneo, ya que en este marco se pueden comprar derechos por dinero. Las posibilidades no son iguales.

El protocolo PoA es una combinación de PoW y PoS (Investopedia 2018b). La construcción de PoA fue motivada por la limitación de la cantidad de Bitcoins en el futuro (el límite es de aproximadamente 21 millones de monedas). Si se llega al límite, el interés por la minería y la verificación desaparece, ya que no habrá recompensa por la verificación de los bloques o, para ser más exactos, la recompensa por la verificación será menor que el costo de la energía utilizada en la minería. proceso, y el sistema fallará. La combinación de PoW y PoS es una opción potencial para la solución. En el proceso, la verificación se realiza con el protocolo PoW, pero en lugar de verificar las transacciones reales, se verifica una muestra que no contiene datos transaccionales. El bloque “ganador” contiene únicamente la prueba de la obra y la identificación del verificador. Cuando se construye el bloque ganador, el sistema cambia al protocolo PoS y selecciona aleatoriamente un grupo de participantes, quienes tienen derecho a aceptar o rechazar la prueba del trabajo. La probabilidad de selección de un participante es mayor si posee más monedas en su cuenta, ya que la selección aleatoria se basa en las monedas y no en los participantes. La muestra se convierte en un bloque válido después de la aprobación de los participantes seleccionados. Si uno o más de los nodos seleccionados no están disponibles, el siguiente bloque ganador se activa y se sortea un nuevo grupo de participantes. La selección itera hasta que alcanza el número solicitado de aprobaciones para un bloque ganador. La recompensa se comparte entre los verificadores y los participantes que aprueban la verificación. el sistema cambia al protocolo PoS y selecciona aleatoriamente un grupo de participantes, quienes tienen derecho a aceptar o rechazar la prueba del trabajo. La probabilidad de selección de un participante es mayor si posee más monedas en su cuenta, ya que la selección aleatoria se basa en las monedas y no en los participantes. La muestra se convierte en un bloque válido después de la aprobación de los participantes seleccionados. Si uno o más de los nodos seleccionados no están disponibles, el siguiente bloque ganador se activa y se sortea un nuevo grupo de participantes. La selección itera hasta que alcanza el número solicitado de aprobaciones para un bloque ganador. La recompensa se comparte entre los verificadores y los participantes que aprueban la verificación. el sistema cambia al protocolo PoS y selecciona aleatoriamente un grupo de participantes, quienes tienen derecho a aceptar o rechazar la prueba del trabajo. La probabilidad de selección de un participante es mayor si posee más monedas en su cuenta, ya que la selección aleatoria se basa en las monedas y no en los participantes. La muestra se convierte en un bloque válido después de la aprobación de los participantes seleccionados. Si uno o más de los nodos seleccionados no están disponibles, el siguiente bloque ganador se activa y se sortea un nuevo grupo de participantes. La selección itera hasta que alcanza el número solicitado de aprobaciones para un bloque ganador. La recompensa se comparte entre los verificadores y los participantes que aprueban la verificación. La probabilidad de selección de un participante es mayor si posee más monedas en su cuenta, ya que la selección aleatoria se basa en las monedas y no en los participantes. La muestra se convierte en un bloque válido después de la aprobación de los participantes seleccionados. Si uno o más de los nodos seleccionados no están disponibles, el siguiente bloque ganador se activa y se sortea un nuevo grupo de participantes. La selección itera hasta que alcanza el número solicitado de aprobaciones para un bloque ganador. La recompensa se comparte entre l

9. CONCLUSIÓN

Los protocolos de consenso son partes inseparables de un sistema blockchain práctico. Sin un protocolo eficiente y seguro, la tecnología es inútil. Hemos discutido la aplicabilidad de los protocolos populares y menos populares en un entorno de votación real. El análisis sugiere que los protocolos que existen actualmente son inadecuados para su uso directo en un sistema de votación. Con todos los protocolos conocidos, los participantes que quieren jugar un papel activo en la verificación de la corrección de las transacciones tienen que sacrificar recursos (tiempo de cómputo o dinero), o tienen que tener un cierto nivel de riqueza, o abrir capacidades al público, etc. Además del derecho en el proceso de verificación, también son recompensados. En el voto democrático, sin embargo, todos los votantes deben tener los mismos derechos en todos los aspectos, su diferenciación en función de sus actividades no es una opción.

Si queremos usar blockchain para votar, es necesario crear un nuevo protocolo de consenso que cree los mismos derechos para todos. La verificación, sin embargo, debe ser recompensada, porque el sistema no funcionará sin esta motivación. A partir de hoy, todos los protocolos que satisfagan la condición de igualdad de derechos e igualdad de motivaciones sólo podrán ser operados fuera del sistema y por supuesto, los protocolos de consenso y su gestión deben ser transparentes.

La tecnología de cadena de bloques sin un protocolo de consenso, como una base de datos distribuida que preserva la integración, naturalmente puede usarse en un sistema de votación electrónica, si una organización externa, por ejemplo, un centro de certificación del gobierno, valida las transacciones (Barnes et al. 2015).

La cadena de bloques como base de datos y centro de certificación podría comprender un modelo de trabajo de la votación en línea si los votantes confían en una organización, que no pueden auditar o controlar directamente. Aquí, la auditoría de la cadena de bloques solo es posible por parte de una organización central. La votación en línea en este marco quizás sea más eficiente y rentable que la votación en papel, pero el papel del control central es ineludible ya nivel del sistema no descarta la manipulación. Sin embargo, para millones de usuarios de Bitcoin y otras criptomonedas, la falta de una organización de control central, por ejemplo, un banco, es en realidad la propiedad más atractiva del sistema.

Hemos demostrado que ninguno de los algoritmos de consenso de uso frecuente cumple completamente con los requisitos de un sistema de votación en línea. El consenso sobre la corrección de la cadena de bloques y el anonimato de los votantes son solo condiciones necesarias, pero no suficientes, para una votación en la vida real.La tecnología blockchain tiene un potencial real en el desarrollo de un sistema de votación seguro, confiable y económico, pero hay muchos problemas teóricos y prácticos que deben abordarse antes de que la tecnología sea aceptada incluso para la prueba.

REFERENCIAS

Ahmed, M. – Kostiainen, K. (2019): Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus con Robust Round Robin.*arXiv*: 1804.07391v2 [cs.CR].

Antonoupoulos, AM (2017):*Dominando Bitcoin*. O´Reilly Media.

Ayed, B. (2017): Un sistema de votación electrónica basado en blockchain seguro conceptual.*Internacional Revista de seguridad de redes y sus aplicaciones*9(3): 1–9.

Barnes, A. – Brake, C. – Perry, T. (2015): Votación digital con el uso de Blockchain. Tecnología Universidad de Plymouth. https://www.economist.com/sites/default/files/plymouth.pdf, consultado el 31/01/2019.

Bitcoin.it (2018): Prueba de quemado. https://en.bitcoin.it/wiki/Proof_of_burn, consultado el 31/01/2019.

Bitcoin.it (2019): vulnerabilidades y exposiciones comunes. https://en.bitcoin.it/wiki/Common_ Vulnerabilidades_y_exposiciones, consultado el 31/01/2019.

BitCongress (2016): Documento técnico de BitCongress: controle el mundo desde su teléfono.http://www.bitcongress.org/BitCongressWhitepaper.pdf, consultado el 31/01/2019.

Buterín, V. (2016): SelfishMining–A25%AttackagainsttheBitcoinNetwork, https://bitcoinmagazine.com/articles/egoish-mining-a-25-attack-against-the-bitcoin-network-1383578440/, consultado el 31/01/2019.

Caiazzo, F. – Chow, M. (2016): A Block-Chain Implemented Voting System, http://www.cs.tufts.edu/comp/116/archive/fall2016/fcaiazzo.pdf, consultado el 31/01/2019.

Coindesk (2016a): The Hard Fork: ¿Qué va a pasar con Ethereum y el DAO? https://www.coindesk.com/hard-fork-ethereum-dao, consultado el 31/01/2019.

Coindesk (2016b): Intel está ganando a los críticos de Blockchain al reinventar el ADN de Bitcoin. http://www.coindesk.com/intel-winning-blockchain-critics-reimagining-bitcoins-dna/, consultado el 31/01/2019.

Cointelegraph (2018): EE. UU.: Virginia Occidental completa las primeras elecciones estatales respaldadas por blockchain. https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-stateelections, consultado el 31/01/2019.

CS Monitor (2012): ¿Se podrían piratear las máquinas de votación electrónica en las elecciones de 2012? Sí.https://www.csmonitor.com/USA/Elections/2012/1026/Could-e-voting-machines-in-Election-2012-behacked-Yes, consultado el 31/01/2019.

Eyal, I. – Gün Sirer, E. (2013): La mayoría no es suficiente: la minería de Bitcoin es vulnerable.*arXiv*: 1311.0243v5 [cs.CR].

Eyal, I. – Gencer, AE – Gün Sirer, E. – van Renesse, R. (2016): Bitcoin-NG: A Scalable Block-Protocolo de cadena.*Actas del 13ºSimposio USENIX sobre diseño e implementación de sistemas en red*. Santa Clara, CA, Estados Unidos.

FollowMyVote.com (2017): Follow My Vote: la plataforma de votación en línea del futuro. https://followmyvote.com, consultado el 31/01/2019.

Friedman, M. (1991): La isla del dinero de piedra.*Documentos de trabajo de la Institución Hoover en economía* E-91-3.

Hackernoon (2018): BitcoinBurst, Parte 3: Prueba de capacidad, ¿la alternativa verde? https://hackernoon.com/burst-part-3-proof-of-capacity-the-green-alternative-8e2651211671, consultado el 31/01/2019.

Hardwick, FS – Apostolos, G. – Akram, R. N, - Markantonakis, K. (2018): E-Voting with Block-cadena: un protocolo de votación electrónica con descentralización y privacidad del votante.*arXiv*: 1805.10258v2 [cs. R].

Investopedia (2018a): Prueba de tiempo transcurrido (criptomoneda). https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp, consultado el 31/01/2019.

Investopedia (2018b): Prueba de actividad (Criptomoneda). https://www.investopedia.com/terms/p/prueba-actividad-criptomoneda.asp, consultado el 31/01/2019.

McCorry, P – Shahandashti, SF – Hao, F. (2017): Un contrato inteligente para la votación en la sala de juntas con Máxima privacidad de los votantes en la Conferencia internacional sobre criptografía financiera y seguridad de datos. En: Kiayias, A. (ed.):*Criptografía Financiera y Seguridad de Datos. Apuntes de clase en informática*.Cham: Springer, págs. 357–375.

Moura, T. – Gomes, A. (2017): Blockchain Voting y sus efectos en la transparencia electoral y Confianza del votante.*Actas del 18ªConferencia Internacional Anual sobre Investigación de Gobierno Digital*. Nueva York, Nueva York, Estados Unidos.

MSNBC (2011): Solo se necesitan $26 para piratear una máquina de votación.http://www.nbcnews.com/id/44706301/ns/technology_and_science-security/t/it-only-takes-hack-voting-machine/#.XM1oPGN7nX4, consultado el 31/01/2019.

Noizat, P. (2015): Voto Electrónico Blockchain. En: Lee, D. (ed.):*Manual de Moneda Digital*. Elsevier, págs. 453–461.

Satoshi, N. (2009): Bitcoin: un sistema de efectivo electrónico de igual a igual https://bitco.in/pdf/bitcoin.pdf, consultado el 31/01/2019.

Shin, L. (2016): Nueva iniciativa tiene como objetivo eliminar la corrupción con la tecnología Blockchain. https://www.forbes.com/sites/laurashin/2016/06/20/new-initiative-aims-to-eliminate-corruption-withblockchain-technology/#4c7f48413094, consultado el 31/01/2019.

Swislow, D. (2016): Qué podría significar Blockchain para la democracia en la era digital. https://www.demworks.org/what-blockchain-could-mean-democracy-digital-age, consultado el 31/01/2019. Tapscott,

A. (2016): Democracia Blockchain: Gobierno del Pueblo, por el Pueblo, para el Pueblo. https://www.forbes.com/sites/alextapscott/2016/08/16/blockchain-democracy-government-ofthe-people-by-the-people-for-the-people/#6fde228c4434, consultado el 31/01/ 2019.

Tomaino, N. (2016): Trustless es un nombre inapropiado. https://medium.com/@ntmoney/trustless-is-a-nombre inapropiado-956066661b79, consultado el 31/01/2019.

Zdnet (2018): Corea del Sur desarrollará un sistema de votación Blockchain. https://www.zdnet.com/article/south-korea-to-develop-blockchain-voting-system/#ftag=RSSbaffb68, consultado el 31/01/2019.