RIESGOS Y OPORTUNIDADES DE BLOCKCHAIN BASADO EN VOTO ELECTRÓNICO SISTEMAS

YOUSIF ABUIDRIS, ABDELRHMAN HASSAN, ABDALLA HADABI, ISSAMELDEEN ELFADUL

Escuela de Informática e Ingeniería, Universidad de Ciencia y Tecnología Electrónica de China, Chengdu 611731, China

CORREO ELECTRÓNICO: yousif_cs@std.uestc.edu.cn

Resumen:

Las elecciones son uno de los pilares principales de una sociedad democrática, pero la influencia emergente de Internet desafía continuamente el proceso de votación. Recientemente, Blockchain basado en votación electrónica ya ha tenido lugar en algunos países. Sin embargo, existen problemas de vulnerabilidades en torno a la cadena de bloques basada en el sistema de votación electrónica. Este documento tiene como objetivo resaltar algunos de los riesgos y oportunidades de los sistemas de voto electrónico basados en blockchain. Además, creemos que este estudio puede aportar una valiosa contribución, ya que ilustra algunos de los riesgos y oportunidades de los sistemas de voto electrónico basados en blockchain. Eso para ofrecer a los usuarios y desarrolladores una visión amplia de los riesgos y oportunidades potenciales asociados con la adopción de blockchain en el sistema de voto electrónico.

Palabras clave:

cadena de bloques; vulnerabilidades; sistema de votación electrónica; Riesgos.

1. Introducción

Blockchain es un desafío para asegurar los sistemas de votación electrónica, dada la complejidad creada por la sinergia de personas, procedimientos, equipos, tecnología, políticas y legislación que influyen en el resultado de un solo acto y voto individual. Debido a que el sistema en línea utiliza equipos que cruzaron fronteras internacionales, es posible lanzar un ataque desde cualquier parte del mundo. Como investigadores en aplicaciones basadas en blockchain [1], creemos en varias industrias en el potencial transformador de los sistemas blockchain. Las cadenas de bloques, como la cadena de bloques de Bitcoin y otras criptomonedas, pueden hacer mucho más que permitir que extraños se envíen dinero entre sí sin temor al fraude o la manipulación [2]. La tecnología blockchain también creó nuevas formas para que las personas inviertan en proyectos que han atraído miles de millones de dólares. y algún día podrán almacenar documentos que hagan que los certificados de educación, la propiedad de la tierra y la emisión del voto sean más abiertos y más difíciles de falsificar. Los datos y la información adjuntos a una cadena de bloques no se pueden eliminar ni cambiar porque se mantienen múltiples copias en computadoras en poder de diferentes personas u organizaciones y se pueden distribuir en todos los países. Controles estrictos puede imponerse sobre el contenido de una cadena de bloques, evitando la entrada de información no autorizada. Las redes Blockchain están diseñadas para ser transparentes, a veces legibles por cualquier dispositivo informático que se una al sistema desde cualquier parte del mundo. Sin embargo, como investigadores que han estudiado la votación basada en cadenas de bloques, creemos que, si bien las cadenas de bloques pueden ayudar con ciertos problemas de seguridad específicos, ese no es el final de la historia. Los riesgos de seguridad de Blockchain [3] existen, y si Blockchain mantiene su compromiso de cambiar la forma en que se almacenan y actúan los datos, debe reconocerse y mitigarse, lo que podría empeorar las cosas. En el peor de los casos, podría poner a la comunidad democrática en riesgo de manipulación al emitir votos o comprar votos.

Este documento destaca algunos de los riesgos y oportunidades del voto electrónico basado en blockchain, mientras que las características de seguridad inherentes a blockchain hacen que la tecnología de contabilidad distribuida (DLT) sea resistente a los ataques, no inmune. Hacia el final del documento, en la Tabla 1, proporcionamos una taxonomía de riesgos y oportunidades para los sistemas de votación basados en Blockchain.

El resto del trabajo se organiza de la siguiente manera: En la sección. 2, para el alcance de las aplicaciones de blockchain, discutimos y evaluamos el trabajo relacionado con los sistemas de votación electrónica. Sección. 3, presenta las vulnerabilidades de los sistemas de voto electrónico basados en Blockchain en el contexto de riesgos y oportunidades. Finalmente, en la Sección. 4, concluimos este trabajo.

2. Trabajo relacionado

En esta sección, presentamos varios sistemas de voto electrónico que pretenden proporcionar voto electrónico basado en Blockchain.

Follow My Vote es una organización de un sistema de votación electrónica que sigue un número restringido de activos de seguridad [4]. Incluye una fase de autenticación que asegura la elegibilidad del votante. Permite a los votantes ubicar sus votos y usar su identificación de votante única para verificar que estén presentes y sean correctos. Sin embargo, algunas propiedades de seguridad

978-1-7281-4242-5/19/$31.00 ©2019 IEEE

no cumplen con este sistema de voto electrónico. De hecho, para garantizar la confidencialidad de los votantes, se requiere que una autoridad de confianza oculte la correspondencia entre la identidad real de los votantes y su clave de votación. Si esta autoridad se corrompe, no habrá más votaciones anónimas. Esta autoridad también puede cambiar votos ya que tiene frases de contraseña para todos los votantes, comprometiendo así la integridad de las elecciones. Este sistema no verifica la confidencialidad de los votos porque no hay encriptación de los votos emitidos. La capacidad de cambiar los votos, junto con la capacidad de realizar un seguimiento de las elecciones en tiempo real, viola la propiedad de la equidad.

Singh y Chatterjee propusieron un modelo para la elección del campus universitario para mantener un sistema de voto electrónico basado en blockchain (SecEVS) [5]. Durante la fase de análisis de seguridad, se validó el método propuesto. El esquema de seguridad del sistema propuesto se basa en el hash raíz de Merkle. Este sistema mantuvo la privacidad de los datos transmitidos, la confidencialidad de los votantes y la unicidad, en la que no se presentan duplicidades durante la etapa de votación. Sin embargo, este sistema propuesto tiene limitaciones en algunas características de seguridad como el anonimato, la auditabilidad, la verificabilidad universal, la consistencia, la coerción, que hacen que este sistema propuesto no sea robusto en absoluto.

Wang y Sun propusieron un esquema para asegurar los sistemas de votación electrónica a gran escala basados en una cadena de bloques [6]. Uso de encriptación homomórfica ElGamal y técnica de firma de timbre único para asegurar y preservar la privacidad del sistema de votación electrónica. Sin embargo, la principal desventaja de este sistema es que no soporta la robustez y no mantiene la resistencia a la coerción.

Z. Wenbin et al.,propuso un protocolo de voto electrónico basado en blockchain preserva la privacidad de extremo a extremo y mantiene la detectabilidad y corrección contra el fraude sin que un tercero se comprometa [7]. Esta implementación de protocolo respetando la estructura de Hyperledger demuestra la validez y aplicabilidad práctica. Sin embargo, las principales desventajas de este protocolo no son la consistencia, la equidad, la verificabilidad individual, la verificabilidad universal y la resistencia a la coerción.

Como podemos ver en los trabajos existentes mencionados anteriormente, la falta de diseños de sistemas concretos en sus documentos técnicos hace que sea difícil determinar si sus sistemas cumplen o no con las propiedades correctas que se indica.

3. Las vulnerabilidades del voto electrónico basado en Blockchain

Existen algunas vulnerabilidades con el método actual de emitir votos y mantener los votos seguros usando blockchain. En esta sección, destacaremos algunas de estas vulnerabilidades. La figura 1 muestra algunas vulnerabilidades del voto electrónico basado en blockchain.

3.1. Las vulnerabilidades del endpoint

Una de las vulnerabilidades de la DLT probablemente provenga de fuera de la cadena de bloques. Sin embargo, estos problemas están afectando la seguridad de la tecnología blockchain en su conjunto, denominadas "vulnerabilidades de punto final", y, por lo tanto, deben abordarse. Los puntos finales son los espacios donde se encuentran los electores y las cadenas de bloques. Los puntos finales son en su mayoría las máquinas utilizadas por los usuarios y las empresas para acceder a los servicios basados en blockchain. Si las instituciones democráticas, las empresas o las criptomonedas son proveedores de dichos servicios, el uso de una cadena de bloques comienza con la entrada de información en una computadora y termina con la salida de información de una computadora. Los datos de la cadena son más vulnerables durante el proceso de acceso a la cadena de bloques. El motivo son las credenciales necesarias para acceder a un libro mayor distribuido compartido y cómo las vulnerabilidades de seguridad podrían exponer estas credenciales en los puntos finales [8]. Si bien existen restricciones en la cadena de bloques, esto es más una restricción del usuario, como veremos.

3.1.1. La seguridad de la clave pública y privada

El acceso a la cadena de bloques requiere tanto una clave privada como una pública. Las claves son cadenas enigmáticas de caracteres de longitud suficiente para que las posibilidades de adivinarlas sean realmente inimaginables. Debido a que es prácticamente imposible acceder a los datos dentro de una cadena de bloques sin la combinación adecuada de claves públicas y privadas, refleja el poder y la debilidad de la tecnología de cadenas de bloques. Ningún atacante podrá acceder a los datos sin las claves correctas. No obstante, todo lo que el atacante quiere son las claves correctas para acceder a la información y hacer lo que quiera con ella. Como los atacantes saben que no sirve de nada tratar de estimar las claves de nadie, se concentran en robarlas. Por lo tanto, la mejor oportunidad para obtener claves es atacar el punto más débil de todo el sistema, computadora personal o dispositivo móvil. Los investigadores han descubierto repetidamente que los terminales de votación de diferentes fabricantes son vulnerables a los ataques [9]. Si la unidad en sí no está protegida contra interferencias, no tiene sentido usar la tecnología blockchain, incluso si las intenciones son buenas.

Los dos puntos altamente efectivos para evitar que los atacantes roben las claves de la cadena de bloques son:

- Ejecute escaneos regulares en busca de anti-malware.
- Las claves de blockchain nunca deben almacenarse en un archivo de texto, documento de Word u otra carpeta en la que la persona no autorizada pueda leerlas fácilmente.

Así como se necesita un enfoque de sentido común para mantener el resto de la información a salvo de los atacantes y evitar que las claves de la cadena de bloques salgan de la computadora o del dispositivo móvil.

siguiendo unos sencillos pasos.

3.2. No probado en escala completa (escalabilidad)

Otra incógnita es la ampliación de una votación electrónica basada en blockchain para atender lo que podría estar procesando cientos de millones de votos. La escalabilidad es una de las preocupaciones críticas de seguridad de la cadena de bloques. La arquitectura de la tecnología de contabilidad distribuida es fundamentalmente escalable. Blockchain se ampliaría cada vez que ocurriera algún cambio. Una vez que Bitcoin alcanzó un precio de casi $20 000 en diciembre de 2017[10], la cantidad de personas que intentaban comprar y vender la criptomoneda hizo que las transacciones fueran mucho más lentas. Si esto sucede con la votación, causará problemas porque se necesitan resultados electorales en cuestión de horas. Sería increíblemente difícil de escalar. En las transacciones de bitcoin, hay una estadística que solo puede manejar siete segundos. Si hacemos eso en una elección, podríamos votar si tenemos miles de personas, no millones. Sin embargo, si hablamos de millones de votos, tómese como ejemplo los 35 millones de votos emitidos en el referéndum del Brexit [11]; si solo pudiéramos verificarlos a los siete segundos, tomaría cincuenta y cinco días para que todo funcionara. Un campo en el que blockchain puede impulsar las elecciones es la transparencia, no solo porque se puede acceder fácilmente a los libros de contabilidad, sino también porque las empresas emergentes que proporcionan tecnología pueden publicar un código de fuente abierta que demuestra cómo funciona el sistema y cómo se puede confiar.

Recientemente, los investigadores propusieron una solución a este tipo de problema de seguridad crítico basado en el estilo de fragmentación [12], que rompe la barrera de la baja tasa de transacciones y la velocidad de generación de bloques.

3.3. Anonimato y verificación

Una de las principales condiciones de votación es ser anónimo, con personas externas que no pueden acceder a la información sobre cómo votó alguien. Sin embargo, para lograr que los ciudadanos voten, deben ser elegibles y debe haber alguna forma de verificarlo. Es un desafío equilibrar estos dos requisitos. Una vez que está en la cadena de bloques, queremos que la persona vea que es su voto, pero no queremos que nadie más vea lo que está pasando, porque no ayuda asegurarse de que la votación sea razonable.

Sin embargo, los países están presionando junto con un intento de introducir la votación de blockchain; uno de ellos es Brasil [13], que utiliza la cadena de bloques Ethereum para almacenar datos electorales. Es una tarea enorme recopilar y validar la información de alrededor de 145 millones de votantes registrados. Por lo tanto, para llevar a cabo una votación electrónica completamente basada en blockchain, se deben superar diferentes problemas.

Verificar la identidad de los votantes desde varios ángulos es siempre una desafío; algunos trabajos [14] han probado las soluciones biométricas, como la comparación facial, la huella dactilar, el iris y el escaneo de la retina, pero esto puede ser sesgado y fácilmente manipulado o robado. Sin embargo, creemos que una forma de proteger los datos biométricos robados es mediante el uso de algoritmos complejos que son difíciles de descifrar. Se puede codificar utilizando cualquier algoritmo de cifrado en lugar de guardar la información biométrica como datos binarios y luego almacenarla como una cadena de referencia. El modelo de muestra debe convertirse en un valor hash durante el proceso de validación e identificación y luego compararse con el valor de referencia.

3.4. Compra de votos (Coerción)

Otra forma en que la cadena de bloques basada en el voto electrónico podría agravar los problemas de votación existentes es aumentando la posibilidad de comprar votos [15]. En elecciones a gran escala, la compra de votos es felizmente rara, en parte porque el voto secreto hace que sea muy difícil verificar un voto comprado y porque existen severas sanciones penales. La colocación de votos en cadenas de bloques elimina la confidencialidad de la cabina de votación. El cifrado no ayuda, y el software puede probar matemáticamente a un comprador de votos que el dispositivo de un votante cifró el nombre de un candidato. Sin embargo, los extraños que pueden tratar de influir en los votos de las personas son muy difíciles de procesar. Muchas empresas de votación afirman que sus sistemas solo reconocen públicamente a los votantes mediante identificadores numéricos aleatorios, por lo que no están sujetos a coerción ni acoso. Sin embargo, las identidades de votantes en muchos de estos sistemas se pueden conectar a cuentas en sistemas de criptomonedas donde un elector puede obtener un soborno, probablemente sin revelar a quién se le cobró, cuánto o por quién. Al tratar de utilizar cadenas de bloques como elemento de protección, se pueden introducir nuevas amenazas en la mecánica crucial de la democracia.

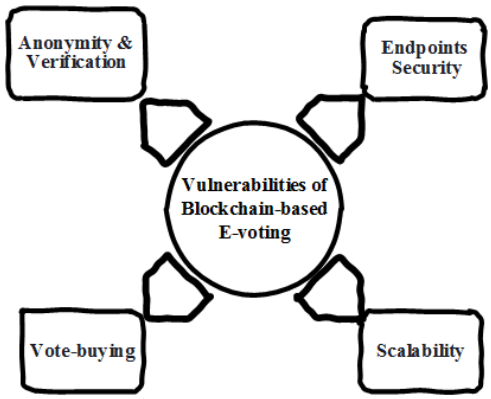

Figura 1las vulnerabilidades de los sistemas de voto electrónico basados en cadena de bloques

Como podemos ver en la Tabla 1, una taxonomía de riesgos y oportunidades para el sistema de voto electrónico usando blockchain

La tecnología se ha discutido en términos de algunas vulnerabilidades que requieren más mejoras en el futuro.

tabla 1taxonomía de riesgos y oportunidades de blockchain-sistemas de voto electrónico basados

Riesgo	Razón	Solución Oportunidad
punto final	Usuario particular seguridad. perder privado clave de seguridad. Nuevo malware y registradores de teclas	Ejecución de confianza Ambiente
No probado en escala completa (Escalabilidad)	Consenso , Datos Tamaño, tiempo de respuesta, Costo	estilo fragmentación, Red Rayo.
Anonimato y Verificación	Gestión de identidad tecnicas	biométrico cifrado solución
compra de votos (Coerción)	Un poder superior influencias o presiones distintas a votar en una dirección.	Difícil de lograr

4. Conclusiones

En breve, es probable que la tecnología de cadena de bloques basada en el voto electrónico continúe evolucionando. Los beneficios incluyen eficiencias mejoradas, costos más bajos, mayor transparencia y un registro inalterable de todas las transacciones de votación. Sin embargo, existen riesgos y amenazas asociados con los beneficios. Este documento destaca estos riesgos y oportunidades de los sistemas de votación electrónica basados en blockchain. Finalmente, es esencial reconocer que la tecnología basada en la cadena de bloques del voto electrónico aún está en pañales. Por lo tanto, es probable que blockchain tarde años en transformarse en su forma más efectiva.

Referencias

[1] V. Dhillon, D. Metcalf y M. Hooper, Blockchain habilitadas: comprender la cadena de bloques Ecosistema y cómo hacer que funcione para usted. Springer, 2017.

[2] S. Nakamoto. Bitcoin: un sistema de efectivo electrónico peer-to-peer [En línea]. Disponible: https://bitcoin.org/bitcoin.pdf

[3] Y.-S. Chung y J.-S. Cha, "El riesgo de seguridad y las contramedidas del comercio de moneda virtual basado en Blockchain", The Journal of Korea Institute of Information, Electronics, and Communication Technology, vol. 11, núm. 1, págs. 100-106, 2018.

[4] seguir mi voto. (2016). Presentamos una solución de votación en línea segura y transparente para la era moderna: FOLLOWMYVOTE. Disponible: https://followmyvote.com/

[5] A. Singh y K. Chatterjee, "SecEVS: Sistema seguro de votación electrónica con tecnología Blockchain", en la Conferencia Internacional sobre Tecnologías de Computación, Energía y Comunicación (GUCON) de 2018, 28 y 29 de septiembre de 2018, Piscataway, NJ, EE. UU. , 2018, págs. 863-7: IEEE.

[6] B. Wang, J. Sun, Y. He, D. Pang y N. Lu, "Elecciones a gran escala basadas en blockchain", Procedia Computer Science, vol. 129, págs. 234-237, 01/01/2018/2018.

[7] Z. Wenbin et al., "Un protocolo de votación que preserva la privacidad en blockchain", en 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2-7 de julio de 2018, Los Alamitos, CA, EE. UU., 2018, págs. 401-8: Sociedad de Informática IEEE.

[8] F. Caron, "Blockchain: Identificación de riesgos en el camino hacia los libros de contabilidad distribuidos", ISACA Journal, vol. 5, 2017.

[9] R. Osgood, "El futuro de la democracia: votación de Blockchain", COMP116: Seguridad de la información, págs. 1-21, 2016.

[10] M. CAMPBELL - VERDUYN y M. Goguen, "Blockchains, redes de confianza y acción: extendiendo las patologías de la globalización financiera", Global Networks, vol. 19, núm. 3, págs. 308-328, 2019.

[11] HD Clarke, M. Goodwin y P. Whiteley, "Por qué Gran Bretaña votó por el Brexit: un análisis a nivel individual de la votación del referéndum de 2016", Asuntos Parlamentarios, vol. 70, núm. 3, págs. 439-464, 2017.

[12] H. Dang, TTA Dinh, D. Loghin, E.-C. Chang, Q. Lin y BC Ooi, "Towards scaling blockchain systems via sharding", en Conferencia internacional sobre gestión de datos de 2019, SIGMOD 2019, 30 de junio de 2019 - 5 de julio de 2019, Ámsterdam, Países Bajos, 2019, págs. 123 - 140: Asociación de Maquinaria de Computación.

[13] T. Fujiwara, "Tecnología de votación, aplicaciones políticas capacidad de respuesta y salud infantil: Evidencia de Brasil", Econometrica, vol. 83, no. 2, pp. 423-464, 2015.

[14] Voatz, "Voatz: Un voto seguro en cada mano", libro blanco, 2019.

[15] S. Zhang, L. Wang y H. Xiong, "Chaintegrity: sistema de votación electrónica a gran escala habilitado por blockchain con robustez y verificabilidad universal", International Journal of Information Security, págs. 1-19, 2019.