Uso y retos de *blockchain* en plataformas de votación electrónica

Victor Garcia-Font
Departament d'Enginyeria Informàtica i Matemàtiques,
Universitat Rovira i Virgili (URV)
CYBERCAT-Center for Cybersecurity Research of Catalonia
victor.garcia@urv.cat

Helena Rifà-Pous
Internet Interdisciplinary Institute (IN3),
Universitat Oberta de Catalunya(UOC)
CYBERCAT-Center for Cybersecurity Research of Catalonia
hrifa@uoc.edu

***Resumen*—Aunque los proyectos de votación electrónica son una realidad desde hace ya algunos años, muchos países se resisten a adoptar esta tecnología en sus procesos electorales fundamentalmente por falta de confianza en las soluciones propuestas y por motivos de coste. En 2009, la aparición de Bitcoin y su tecnología subyacente *blockchain* supuso una revolución en los sistemas TI descentralizados, y su influencia también se produjo en el contexto de la votación electrónica para superar los problemas de seguridad y coste. La adopción de *blockchain* en los sistemas de votación se ha realizado de dos maneras: utilizando criptomonedas o *tokens* criptográficos para representar votos o utilizando la *blockchain* como registro inmutable. En este artículo revisamos sistemas representativos de ambos usos, estudiamos que aporta *blockchain* a cada proyecto, y discutimos los beneficios y problemáticas de esta tecnología en el escenario de la votación electrónica.**

***Index Terms*—votación electrónica, blockchain, seguridad información**

I. Introducción

La transición de un sistema de voto convencional a electrónico es un paso que muchos países y juntas electorales se resisten a tomar. De hecho, innovaciones tecnológicas como DRE (*Direct Recording Electronic*) para facilitar el voto o el recuento ya han probado ser vulnerables y tener bugs difícilmente detectables [1] y por lo tanto, la falta de confianza en este tipo de sistemas es notable. En sistemas que funcionan online la preocupación es aún mayor ya que las transacciones están expuestas a ciberataques, puede haber vulnerabilidades en los dispositivos de votación personal, hay un elevado riesgo de coacciones, etc.

Por otro lado, la votación electrónica mejora problemas de los sistemas tradicionales, como las dificultades para ejercer el derecho a voto de residentes en el extranjero [2], la dificultad de participar que tienen personas enfermas o con problemas de movilidad, el desincentivo para la participación que suponen largas colas en frente de una mesa electoral (en las elecciones de presidenciales americanas de 2012 se registraron colas de hasta 7 horas [3]), etc. También abren un abanico de nuevas posibilidades, permitiendo, además de las típicas votaciones a candidatos cada varios años, otro tipo de consultas sobre temas específicos que podrían producirse más a menudo, o incluso permitirían reformar más profundamente el proceso electoral introduciendo conceptos de democracia líquida [4], donde por ejemplo, se pudiera delegar el voto a otro participante en consultas relacionadas con un tema concreto.

Todo esto hace que empresas tecnológicas y organismos públicos sigan trabajando en sistemas de votación electrónica e investiguen la incorporación de nuevas tecnologías para mejorar la seguridad y la transparencia de sus sistemas. En este sentido *blockchain* es una tecnología que recientemente ha ganado popularidad en varios sectores, y podría contribuir a mejorar el campo de las votaciones electrónicas gracias a propiedades como la inmutabilidad, la integridad y la auditabilidad. En este artículo, revisamos algunos de los principales proyectos de votación electrónica y vemos que las principales contribuciones de *blockchain* en este campo pueden dividirse entre los proyectos que usan criptomonedas o *tokens* criptográficos como representación de votos, por lo que *blockchain* representa una parte fundamental del sistema de votación, y por otro lado, los proyectos que usan *blockchain* como registro inmutable para mejorar o sustituir parte de un sistema de votación electrónico implementado con otras tecnologías. En este artículo estudiamos sistemas representativos de ambos usos, vemos que aporta *blockchain* a cada proyecto en términos de seguridad, y de forma más general discutimos las ventajas e inconvenientes de la tecnología *blockchain* en este contexto. El resto del paper está organizado en las siguientes secciones: la Sección II introduce las tecnologías básicas para contextualizar este artículo; en la Sección III se describen los diferentes usos de *blockchain* en diferentes iniciativas de votación electrónica; en la Sección IV se discuten las contribuciones y los problemas que trae *blockchain* en este contexto; y finalmente en la Sección V se concluye el paper.

II. Contexto tecnológico

Esta sección revisa los conceptos y las tecnologías básicas para contextualizar el resto del paper. Para ello, la Sección II-A revisa los conceptos más importantes y las propiedades de seguridad que deben cumplir los sistemas de votación electrónica. Posteriormente, la Sección II-B introduce la tecnología *blockchain*.

II-A. Votación electrónica

Entre los sistemas que permiten votaciones electrónica, se puede encontrar tanto sistemas que han estado concebidos sin alterar el espíritu de las votaciones tradicionales en papel (*i.e.* votaciones grandes y muy espaciadas en el tiempo, con registros de votantes centralizados), como sistemas que pretenden añadir funciones al proceso (democracia líquida, consultas populares, ...). En esta sección revisamos las propiedades de seguridad que deben cumplir estos sistemas y describimos los componentes y servicios más destacados para este artículo que

integran un sistema de votación electrónica. Información más exhaustiva sobre este tema puede encontrarse en [5].

A continuación listamos las características relacionadas con la seguridad y la privacidad que los sistemas de votación electrónica buscan conseguir:

- **Elegibilidad**: sólo los votantes legítimos (forman parte del censo o de un registro de votantes) pueden votar.
- **Autenticidad** e **integridad**: el voto debe ser emitido por un votante y no debe haberse modificado entre su emisión y su recuento.
- **Privacidad de los votantes**: ningún ente, tanto interno como externo de la votación, debe poder conocer el voto de un votante.
- **Secreto de los resultados intermedios**: hasta que no se finaliza la votación, no deben poder conocerse resultados parciales.
- **Incoercibilidad**: los votantes deben poderse proteger ante intentos de coerción.
- **Verificabilidad E2E** (extremo a extremo): las partes implicadas deben poder verificar que el proceso en el que están implicados finaliza satisfactoriamente, *i.e.*, los votantes comprueban que su elección se ha registrado al sistema, y se puede verificar que los votos escrutados corresponden a los votos emitidos y están bien contabilizados.

A continuación, veremos los componentes y servicios relacionados con este artículo más destacados de un sistema de votación electrónica:

- **Aplicación cliente**: utilizada por el votante para seleccionar y enviar la opción que desea votar. Esta aplicación puede estar en un dispositivo del votante (*e.g.* teléfono móvil, *PC*), y por lo tanto está en un entorno que debe ser considerado como hostil, no controlado por el proveedor del sistema de votación.
- **Servicio de filtrado *(cleansing)***: elimina votos duplicados o inválidos, y los datos personales (p.e., firma del votante) asociados a cada voto.
- **Servicio de mezclado**: recifra los votos cifrados y los mezcla, de forma que los votos se reordenan completamente en la urna y no sea posible correlarlos con ningún votante.
- **Sistema multi autoridad**: impide que una sola parte acceda al contenido de los votos. Con estos sistemas se suelen cifrar los votos utilizando una clave dividida en N partes, requiriendo M de las partes para poder recuperar la clave para descifrar los votos.
- **Servicio de recuento de votos *(talling)***: descifra los votos y hace el recuento.
- **Tablón de anuncios *(Bulletin board)***: panel público donde se registran datos importantes sobre la votación.
- **Servicio de *logs***: registra los eventos destacados del sistema de votación.

II-B. Blockchain

En 2008, el *white paper* titulado *Bitcoin: A peer-to-peer electronic cash system* [6] no sólo actúa de punto de partida para Bitcoin, sino que también introduce la tecnología *blockchain* (cadena de bloques en español), un sistema descentralizado que, mediante un protocolo de consenso, permite a los participantes del sistema registrar datos de forma inmutable sin utilizar una tercera parte de confianza. Posteriormente, utilizando la misma filosofía de la *blockchain* propuesta en Bitcoin, se han creado otros sistemas que se adaptan a otros propósitos o requerimientos. Por ejemplo, algunas propuestas interesantes que intentan mejorar el diseño original de Nakamoto plantean la implementación de técnicas orientadas a preservar la privacidad de los usuarios, como el uso de *ring signatures* en CryptoNote [7] o de las pruebas de conocimiento nulo zk-SNARKs en ZeroCash [8].

Otra característica destacada de la *blockchain* de Bitcoin, y de la de la mayoría de criptomonedas, es que se trata de un sistema público, en el cual no sólo los registros pueden ser consultados libremente, sino que también, cualquier nodo que siga las normas del protocolo puede participar en el protocolo de consenso e incluir nuevos datos sin necesidad de contar con permisos especiales. Por esto a estas *blockchain* se las denomina sin permisos (*permissionless*). Por otro lado, siguiendo otros requerimientos de seguridad y accesibilidad, posteriormente se propusieron las *blockchains* denominadas con permisos (*permissioned*), que podían tener contenido privado y requerir permisos especiales para poder participar en el consenso. Ripple[1] es uno de los proyectos más destacados usando este tipo de *blockchain*.

La tecnología *blockchain* ha evolucionado bastante desde su diseño original. Aun así, las propiedades básicas de seguridad que la distinguen como un sistema de registro descentralizado e inmutable están presentes de forma transversal entre todas las nuevas propuestas. En este artículo, nos centramos en el uso que hacen los diferentes proyectos de votación electrónica de las características de seguridad y privacidad vinculadas a las *blockchain* utilizadas. Para más información sobre la tecnología, el lector puede consultar otros artículos como [9].

III. Tipología de uso de blockchain

Aprovechando las características de seguridad en sistemas descentralizados que aporta la tecnología *blockchain*, algunos proyectos de votación electrónica han incluído esta tecnología ya sea para mejorar la seguridad de alguno de sus componentes, o incluso para que forme parte del corazón del sistema. De entre los usos que hemos observado, se pueden diferenciar claramente dos maneras de emplear la *blockchain*: por un lado, algunos proyectos utilizan una criptomoneda o *token* (i.e una representación de un recurso o utilidad que reside en la parte superior de una *blockchain*) y representan un voto a través de una transacción; y por otro lado, otros proyectos usan *blockchain* tan solo por sus propiedades de registro inmutable, básicamente para implementar el tablón de anuncios o para enviar pruebas de integridad de *logs*, votos, o algún otro evento. En las siguientes secciones veremos ejemplos representativos de estas dos tipologías de uso.

III-A. Criptomonedas para representar votos

De entre los proyectos revisados que usan criptomonedas para representar votos, queremos destacar la propuesta hecha por *P. Tarasov et al.* [10], donde los autores proponen el uso de la criptomoneda Zcash. Para entender el sistema propuesto, primero es necesario conocer que las criptomonedas utilizan

[1]Ripple, https://ripple.com/

unos identificadores llamados direcciones que tienen un uso parecido al número de una cuenta bancaria, se utilizan para enviar y recibir criptomonedas. Una dirección está asociada a una clave pública y cuando un usuario recibe una transacción en ella, puede utilizar el contenido recibido si dispone de la clave privada correspondiente. Las direcciones y claves privadas de cada usuario se almacenan en un monedero. Zcash dispone de dos tipos de direcciones: las direcciones transparentes (*t-address*) que son direcciones asimilables a las direcciones de Bitcoin en las que el envío de las criptomonedas es transparente, y las direcciones blindadas (*z-address*) que son direcciones para preservar la anonimidad en las transacciones. Así, dependiendo de la combinación de direcciones que se usen para el envío y recepción de las criptomonedas podemos diferenciar entre 4 tipos de transferencias: (1) pública cuando se usan dos *t-address*; en este caso se conoce el importe y se permite la trazabilidad de la moneda, (2) *shielding* cuando se usa una *t-address* de envío y una *z-address* de recepción; en este caso se revela el saldo enviado pero se quiebra la enlazabilidad con una futura dirección transparente, (3) *deshielding* cuando se usa una *z-address* de envío y una *t-address* de recepción; en este caso, la dirección transparente de recibo anula el blindaje de las monedas y revela en el *blockchain* el valor recibido, y (4) privada cuando se usan dos *z-address* y se mantiene secreto el saldo y las direcciones de la transacción.

De esta forma los autores proponen un sistema de votación basado en 4 etapas básicas en las que usando movimientos de ZEC (criptomoneda de Zcash) entre diferentes tipos de direcciones de los votantes, de los candidatos y de la junta electoral, se busca mantener las propiedades básicas de un sistema de votación descritas en II-A y a la vez tener un sistema seguro, flexible y más económico de implementar y desplegar que un sistema de votación electrónica convencional. Las 4 etapas que propone el sistema son las etapas que en líneas generales proponen todos los sistemas de *e-voting*: registro, notificación, votación y recuento/auditoría. A continuación explicaremos de forma resumida estas etapas.

Para empezar, poco antes de iniciar el periodo electoral, los usuarios registrados como votantes en el sistema reciben un *email* con un enlace que se activa con el inicio oficial de los comicios. Al acceder al enlace, al votante se le presenta un formulario donde puede escoger a su candidato y donde introduce una *t-address* controlada por él. Una vez que el usuario rellena el formulario y autoriza el voto, se transfiere cierta cantidad de ZEC desde una dirección de un monedero de la junta electoral a la *t-address* del votante. Estos ZEC son reenviados automáticamente utilizando una *z-address* del votante para preservar su privacidad a una dirección de un monedero del candidato que se haya escogido. Una vez finaliza la elección, los *tokens* de las direcciones de los candidatos se transfieren otra vez al monedero de la junta electoral para su recuento. En la Figura 1 se puede ver un esquema simplificado de la etapa de votación de esta propuesta. Existen dos variantes del sistema dependiendo de si los candidatos reciben los *tokens* en direcciones del tipo *z-address* o *t-address*. Con el uso de *z-addresses* se incrementa la privacidad del sistema, pero se rompe la enlazabilidad de las transacciones, con lo que un votante no podría tracear que

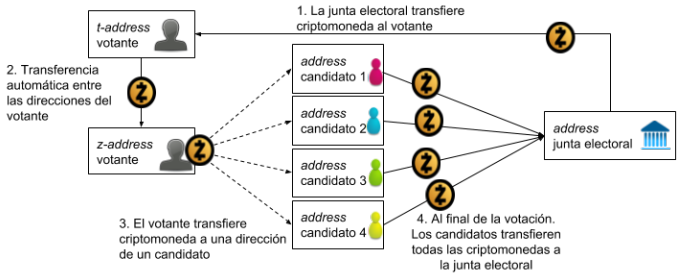

Figura 1. Esquema simplificado de la etapa de votación propuesto en [10]

su voto ha sido vaciado del monedero del candidato al de la junta electoral para su recuento. Por contra, si los candidatos usan *t-addresses* para recibir los *tokens*, entonces los votantes pueden comprobar que su voto ha sido enviado a la junta electoral para su recuento, facilitando la verificabilidad E2E. Sin embargo, el uso de estas direcciones también comporta que las direcciones de los candidatos puedan ser observadas en tiempo real, vulnerando el principio de no poder conocer resultados parciales antes de que finalice el proceso electoral.

El uso de *tokens* criptográficos como representación directa de votos se ha propuesto también en otros proyectos que no utilizan una criptomoneda, sino que optan por implementar su propio *token*. Por ejemplo, Democracy.earth[2] propone desplegar su propio *vote token*. Al desplegar su propio *token*, estos proyectos no sólo pueden implementar más fácilmente las funciones de votación, sino que también evitan algunos problemas asociados al uso de criptomonedas como *tokens*, como por ejemplo el riesgo asociado al valor de mercado que tiene la criptomoneda. Además, al utilizar su propio *token*, estos proyectos pueden customizar más los proyectos y ofrecer sistemas de votación que van mucho más allá de las características democráticas ofrecidas por las votaciones en papel, ofreciendo mecanismos de democracia líquida, o permitiendo la creación y el mantenimiento de organizaciones descentralizadas en una jurisdicción digital sin fronteras, como es el caso de Aragon[3].

III-B. Blockchain como registro inmutable

Uno de los proyectos más avanzados de votación electrónica que utiliza *blockchain* como registro inmutable como pieza central de su tecnología es Agora[4]. La arquitectura de este proyecto [11] está dividida en 4 capas: un tablón de anuncios, Cotena, la *blockchain* de Bitcoin y Votapp. A continuación describiremos los componentes relacionados con la *blockchain*.

Por un lado, el tablón de anuncios es una *blockchain* con permisos con una arquitectura de *skipchain* [12], donde a ciertos nodos operados por Agora o por terceros se les concede permisos o bien de escritura o de solo lectura. Esta *blockchain* se utiliza de registro inmutable de datos generados durante el proceso electoral (p.ej. votos, pruebas de conocimiento nulo evidenciando la corrección de un subproceso del sistema de votación). Así, existen un conjunto de nodos con permisos suficientes de escritura conocidos como Cothority (Collective authority), que confirman de forma colectiva la inserción de

[2]Democracy.earth, https://www.democracy.earth/
[3]Aragon, https://aragon.one/
[4]Agora, https://agora.vote/

transacciones en el tablón de anuncios. La forma de funcionar de la Cothority se basa en la elección rotativa de un nodo especial al que se denomina oráculo y que es el encargado de realizar la mayor parte de la gestión, dejando a los otros nodos básicamente tareas de colaboración y de monitorización del oráculo. De esta manera, todos los nodos reciben las transacciones con los votos emitidos por los votantes, entre otros datos de la votación, pero es el oráculo el encargado de proponer nuevos bloques para ser incluídos en la *blockchain* con las transacciones recibidas. Además, el tablón de anuncios actúa de canal central de comunicación y de memoria, siendo el oráculo el encargado de escribir bloques en el *log* de Cotena (explicado más adelante) y enviar pruebas de integridad a la *blockchain* de Bitcoin. Así, los nodos tienen la responsabilidad de: (1) mantener una copia del tablón de anuncios; (2) recibir los votos encriptados de los votantes, autenticar sus datos y asegurar que los votos son enviados por un votante autorizado; (3) confirmar los bloques propuestos por el oráculo; (4) descifrar los votos una vez que se ha acabado la elección y crear votos en texto en claro para que puedan ser recontados; y (5) mantener una copia del *log* de Cotena y monitorizar que es correcto.

La segunda capa de la arquitectura de Agora es conocida como Cotena. Este componente es básicamente un mecanismo de *logging tamper-resistant* construido encima de la *blockchain* de Bitcoin, donde se escriben pruebas de integridad del tablón de anuncios. De esta forma, Agora usa el poder computacional y la transparencia que ofrece la red de Bitcoin para proteger la integridad de su *blockchain* con permisos. La *blockchain* de Agora permite que haya una constancia pública de cada paso de la votación y que las etapas sean fácilmente auditables. El sistema es verificable extremo-a-extremo ya que un auditor podría comprobar que: los parámetros de configuración son correctos (no lo hemos mencionado pero otros muchos datos son publicados por los nodos de la Cothority en el tablón de anuncios, como los ficheros de configuración); que los votos cifrados corresponden a votantes autenticados especificados en la lista de configuración y reflejan sus elecciones (se utiliza una validación *cast-or-challenge* en la que votantes descifran de forma aleatoria votos de tipo test para comprobar que el voto emitido es correctamente registrado en el sistema); que la red de mezclado funciona correctamente y que las pruebas de conocimiento nulo que se generan corresponden a pasos correctos para hacer una verificación aleatoria y anonimizar correctamente los votos y que los votos descifrados parcialmente por cada nodo son correctos y el texto en claro ha sido reconstruido correctamente; y que el recuento final está bien computado. Finalmente, auditores oficiales pueden firmar un atestado y registrarlo también en el tablón de anuncios. De esta manera, Agora utiliza una arquitectura híbrida de *blockchain* con permisos y sin permisos, donde se usa el tablón de anuncios para escribir todos los datos del proceso de votación (*e.g.* votos recibidos en cada nodo) que requieren de un sistema con poca latencia, y posteriormente se hacen capturas del tablón de anuncios en la *blockchain* de Bitcoin, asegurando de esta manera la integridad y la inmutabilidad en una *blockchain* más segura pero que requiere de una latencia más alta para registrar transacciones. Con este diseño, los creadores de Agora aseguran que el sistema dispone de una arquitectura escalable, de alta disponibilidad, usable, de bajo coste, de baja latencia, sin puntos únicos de falla, que permite una verificabilidad fuera de línea y que permite ser adaptada a las regulaciones de diferentes tipos de elección. Aunque todos los pasos son publicados en la *blockchain* y por lo tanto son accesibles por todas las partes, cabe destacar que esta propuesta también respeta otras propiedades de privacidad mencionadas anteriormente requeridas en un sistema de votación electrónica. Por un lado no permite conocer el resultado parcial de la elección, ya que los votos se publican cifrados con un sistema de multi autoridad. Por otro lado, también protege la privacidad del votante, ya que la red de mezclado aporta anonimidad, el voto es secreto, y además, a diferencia de otros sistemas, no se provee al votante con un recibo de votación que pueda después enseñar a un tercero, evitando posibles maniobras de coerción. El uso de *blockchain* como registro inmutable también ha sido propuesto en otros proyectos. Por ejemplo, *J.Cucurull et al.* [13] de Scytl[5] proponen registrar pruebas de integridad de su sistema de *logs* en la *blockchain* de Bitcoin, con una propuesta parecida a lo comentado en Agora. Por otro lado, TIVI[6] proponen en [14] y [15] usar *blockchain* en un servicio de sellado de tiempo digital. Así, con este sistema pueden asegurar que un dato ha existido en un cierto momento en el tiempo. Por ejemplo, se envía una huella dactilar de cada voto en el servicio externo de sellado de tiempo. El sello de tiempo se guarda junto al voto y se le pasa al votante, quien puede verificar que el voto se registró correctamente, y no fue alterado ni eliminado del sistema.

IV. Discusión

Como hemos visto, los sistemas de votación electrónica que incluyen tecnología *blockchain* pueden dividirse claramente entre los que usan la *blockchain* para registrar transacciones que representan directamente los votos (de forma anàloga a las transacciones de una criptomoneda), o sistemas que usan la *blockchain* tan solo para publicar ciertos datos del proceso de voto en un registro inmutable. Además, también hemos visto que la importancia de la *blockchain* en el conjunto de la arquitectura puede ser muy dispar. Sistemas como Agora o [10] tienen la *blockchain* como pieza central, en cambio *J.Cucurull et al.* [13] tan solo proponen mejorar algún elemento dentro de la arquitectura típica de un sistema de *e-voting*.

En cualquier caso, la *blockchain* se incluye en los diferentes proyectos para contribuir en los requerimientos de seguridad y verificabilidad que debe cumplir un sistema de votación electrónica. En la Tabla I se puede ver un resumen de cómo la *blockchain* puede contribuir a estas propiedades.

Además de las propiedades resumidas en la tabla, también merece la pena destacar para los proyectos que usan transacciones con criptomonedas como sistema de votación, que por la naturaleza pública y sin permisos de la mayoría de criptomonedas, éstas están siendo atacadas continuamente y numerosos estudios analizan las vulnerabilidades de estas *blockchains* y describen los ataques descubiertos [16], lo que

[5]Scytl, https://www.scytl.com

[6]TIVI, http://www.smartmatic.com/voting/online-voting-tivi/

resulta en sistemas altamente probados y mucho más seguros que sistemas privados y más cerrados.

Sobre todos los proyectos estudiados, también cabe destacar la voluntad de hacer pública y accesible gran parte de la información del proyecto, licenciar el código como *open source*, en muchos casos haciéndolo fácilmente accesible en repositorios como Github[7]. Sin embargo, en la mayoría de proyectos, a la hora de la verdad, se echa en falta documentación clara, revisada por fuentes externas (*e.g.* artículos revisados por pares o auditorías) y certificada especificando claramente las funciones de los elementos tecnológicos utilizados. En cambio, generalmente lo único que se ofrece son *white papers* o *brochures* donde se explica de forma muy superficial la arquitectura de los sistemas. Esto requiere que cualquier evaluación del sistema tenga que hacerse revisando el código fuente directamente, o con poca asistencia documental, dificultando el estudio de la seguridad de estos proyectos. En este sentido, los proyectos que utilizan criptomonedas como base tecnológica tienen la ventaja que, en el caso de usar criptomonedas populares, ya se cuenta con multitud de expertos que conocen sus propiedades de seguridad y no tienen que ser auditadas desde zero.

Sin embargo, el uso de *blockchains* de las criptomonedas más populares, ya sea como *token* o simplemente para registrar datos como pruebas de integridad, también trae consigo algunos inconvenientes. Para empezar, el valor monetario de los *tokens* supone un riesgo de que los votantes intenten robar el *token* en vez de utilizarlo para votar. También la volatilidad de los precios del *token* puede suponer un riesgo para la viabilidad de algunos comicios, con el posible agravio de que ciertos actores puedan manipular los precios de los criptoactivos [17]. Posibles soluciones a estos inconvenientes pasan por el uso de *smart contracts* que impidan a los votantes o cualquier otra parte implicada en el proceso poder controlar las transferencias con las criptomonedas, sino que las criptomonedas deben ser transferidas directamente de monederos controlados por la junta electoral a direcciones representando al votante y de allí automáticamente a otras direcciones controladas por los candidatos o por la misma junta electoral. También estos problemas pueden mitigarse con el uso de las unidades más pequeñas de una criptomoneda (*i.e. satoshi* en el caso de bitcoin o *zatoshi* en el caso de Zcash) que suelen tener precios muy bajos, con lo que se mitiga el riesgo de robo de estos *tokens*. Sin embargo, en muchos casos no es menospreciable ni el precio de las comisiones por transacción, ni la posible demora entre la emisión de una transacción y su inclusión en un bloque (sin contar el tiempo requerido para que se minen el suficiente número de bloques para poder considerar una transacción como confirmada, *i.e.* 6 bloques en Bitcoin que equivalen a un mínimo de 1 hora de tiempo). En el caso de Bitcoin, las comisiones llegaron a situarse alrededor de los 55 USD de media el 22 de diciembre de 2017[8], y el 12 de noviembre del 2017, de mediana las transacciones tardaban 27 minutos en ser aceptadas en un bloque minado[9].

Además, estos proyectos deben demostrar que los ataques conocidos sobre las *blockchain* no afectarán a un proceso electoral. Entre ellos destaca el ataque del 51 % [16], donde un atacante que reuniera la suficiente fuerza de computación podría manipular la cadena de bloques, por ejemplo eliminando transacciones (lo que supondría la eliminación de votos en este contexto). Por esto es necesario estudiar la resistencia de estas *blockchains* para su utilización en un proceso electoral, donde los adversarios pueden llegar a ser estados poderosos con un poder computacional muy elevado. Esto hace que a nivel de seguridad, las *blockchain* con más capacidad de computación (medido por el *hashing rate*, número de *hashes* por segundo que computa de forma global una red de una criptomoneda) sean más seguras, y por lo tanto, el uso de criptomonedas minoritarias sea totalmente desaconsejable. A día de hoy (abril de 2018), el *hashrate* de Bitcoin está alrededor de 27 EH/s[10] y el de Ethereum alrededor de 250 TH/s[11]. Bastante inferior es el *hashrate* de Zcash, que dispone alrededor de 475 MH/s[12].

De los proyectos analizados, ninguno publica un estudio

[7]Github, https://github.com/

Tabla I
RESUMEN DE LAS CONTRIBUCIONES EN LAS PROPIEDADES DE SEGURIDAD DE LOS SISTEMAS DE VOTACIÓN ELECTRÓNICA CON EL USO DE TECNOLOGÍA BLOCKCHAIN EN FORMA DE (1) TRANSACCIONES CON MONEDAS, Y (2) REGISTRO INMUTABLE.

Elegibilidad	
(1)	No mejora los mecanismos existentes. Por otro lado, algunos de los proyectos proponen el uso de mecanismos descentralizados también utilizando *blockchain* para poder identificar a los usuarios, como por ejemplo el propuesto en [4].
(2)	Permite la inclusión de la lista de votantes autorizados en un tablón de anuncios público.
Autenticidad e integridad	
(1)	*Blockchain* asegura la autenticidad y la integridad de sus transacciones.
(2)	El registro de pruebas de integridad en una *blockchain* asegura su inmutabilidad y protege a los sistemas de ataques de modificación y truncado en caso de exposición de claves privadas.
Seguridad en general	
(1)	El sistema evita inherentemente que un votante vote dos veces gracias a que *blockchain* evita *double spending*.
(2)	El sistema facilita el registro de pruebas de integridad como capturas del estado del sistema cada cierto tiempo.
Privacidad de los votantes	
(1)	Algunos incorporan mecanismos para anonimizar a los usuarios. Esto hace que servicios adicionales como las redes de mezclado no sean necesarios.
(2)	No mejora los mecanismos existentes.
Secreto de los resultados intermedios	
(1)	Algunos incorporan mecanismos multi autoridad que pueden contribuir a no realizar transacciones hasta que la votación haya concluído.
(2)	No mejora los mecanismos existentes.
Incoercibilidad	
(1)	No mejora los mecanismos existentes.
(2)	No mejora los mecanismos existentes.
Verificabilidad	
(1)	Las *blockchain* aportan transparencia. Las transacciones en la *blockchain* son públicas y por lo tanto, el rastreo de los *tokens* puede ayudar a conseguir verificabilidad E2E.
(2)	La *blockchain* sirve de registro donde publicar las pruebas que aseguran que el proceso ha funcionado correctamente.

[8]Bitcoininfocharts. Media del coste de las comisiones por transacción., https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

[9]Blockchain.info. Mediana del tiempo de confirmación de una transacción., https://blockchain.info/charts/median-confirmation-time

[10]Bitcoininfocharts. *Hashrate* de Bitcoin., https://bitinfocharts.com/comparison/bitcoin-hashrate.html

[11]Bitcoininfocharts. *Hashrate* de Ethereum., https://bitinfocharts.com/comparison/ethereum-hashrate.html

[12]Bitcoininfocharts. *Hashrate* de Zcash., https://bitinfocharts.com/comparison/zcash-hashrate.html

en profundidad de cómo afectarían los principales ataques conocidos a los ecosistemas *blockchain*. De hecho, tan solo los autores de [10] mencionan que algunos de los ataques podrían suponer un problema.

A todo esto hay que añadirle los problemas de escalabilidad de las principales criptomonedas [19]. Aunque gracias al despliegue de SegWit[13] en la red principal de Bitcoin, o al incremento del tamaño del bloque en Bitcoin Cash[14], se haya incrementado ligeramente el máximo de 7 transacciones por segundo que tenía Bitcoin [19], actualmente las principales *blockchains* todavía tienen un límite que se sitúa lejos del que debería poder soportar una plataforma de votación electrónica. En los proyectos analizados, esta limitación es o bien ignorada, o se utiliza un sistema de menor latencia para el registro de las acciones que requieran un *throughput* alto, como por ejemplo en Agora, donde se usa una *blockchain* con permisos. Otra solución pasaría por desarrollos de capas por encima de las *blockchain*, como las Lightining Network[15], las cuales prometen incrementar de forma exponencial la capacidad de las *blockchain*.

Además, estos proyectos también tienen que demostrar que en un futuro los datos almacenados en las *blockchain* públicas no podrán usarse para revelar la identidad de los votantes. Aunque en estos momentos parece un riesgo lejano, es necesario evaluar los riesgos que puede tener la computación cuántica en un futuro, ya que es conocido que la seguridad de algunas técnicas criptográficas podrían romperse [18]. También es necesario considerar que pueden aparecer fallos no descubiertos que lleven a identificar a los usuarios. Por ejemplo, los autores de [20] recientemente han comprobado empíricamente que es posible vincular varias transacciones de Monero[16], una moneda que tiene como principal característica ser anónima y no linkable.

V. Conclusiones

En este artículo hemos estudiado varios proyectos que proponen diferentes usos de *blockchain* dentro de un contexto de votación electrónica. Hemos visto que en general, estos proyectos pueden dividirse entre los que pretenden utilizar un *token* criptográfico como *token* de votación, y por otro lado los que básicamente utilizan *blockchain* tan sólo como un registro inmutable. Los primeros son proyectos ambiciosos y todavía tienen que solventar muchos problemas tecnológicos (*e.g.* escalabilidad de *blockchain*) para que se pueda plantear seriamente su uso en elecciones oficiales. Por otro lado, los segundos plantean mejorar alguno o varios de los elementos dentro de un sistema de votación electrónica convencional, basando la mayor parte de la seguridad del sistema en los principios ya conocidos, como sistemas multi autoridad, redes de mezclado, etc. implementados completamente a parte de la *blockchain*, por lo que parece que el posible uso de estos sistemas de votación electrónica esté más cerca. Sin embargo, la utilización de un *token* de votación plantea un cambio de paradigma mayor, que podría suponer la creación de plataformas de votación electrónica más rentables, de más fácil despliegue, soportando nuevas formas de participación democrática.

[13]Segregated Witness, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[14]Bitcoin Cash, https://www.bitcoincash.org/

[15]Lightining Network, https://lightning.network/

[16]Monero, https://getmonero.org/

Agradecimientos

Este trabajo está financiado parcialmente por el Ministerio de Economía y Competitividad a través del proyecto SMART-GLACIS (TIN2014-57364-C2-2-R).

Referencias

[1] J. Bannet, D. Price, W. Rudys, J. Singer y D.S. Wallach: "Hack-a-vote: Security issues with electronic voting systems", en *IEEE Security & Privacy*, vol. 2, n. 1, pp. 32-37, 2004.

[2] M.P. López: "El desdichado voto exterior" [Online], 2017. Disponible: LaVanguardia.com, http://www.lavanguardia.com/politica/20171221/433787580695/voto-extranjero-expatriados-documentacion-electoral-elecciones-cataluna-21d.html. [Accedido 9 de Abril, 2018].

[3] C. Famighetti: "Long voting lines: explained" [Online], 2016. Disponible: BrennanCenter.org, https://www.brennancenter.org/analysis/long-voting-lines-explained. [Accedido 9 de Abril, 2018].

[4] Democracy.earth: "The Social Smart Contract" [Online], 2018. Disponible: Democracy.earth, https://www.democracy.earth/#paper. [Accedido 9 de Abril, 2018].

[5] D.Y. Marcos del Blanco, L. Panizo y J.A. Hermida: "Review of cryptographic schemes applied to remote electronic voting systems: remaining challenges and the upcoming post-quantum paradigm", en *Open Mathematics*, vol. 16, n. 1, pp. 95-112, 2018.

[6] S. Nakamoto: "Bitcoin: A peer-to-peer electronic cash system" [Online], 2008. Disponible: Bitcoin.org, https://bitcoin.org/bitcoin.pdf. [Accedido 9 de Abril, 2018].

[7] N. van Saberhagen: "Cryptonote v 2. 0" [Online], 2013. Disponible: Cryptonote.org, https://cryptonote.org/whitepaper.pdf. [Accedido 9 de Abril, 2018].

[8] E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer y M. Virza: "Zerocash: Decentralized anonymous payments from bitcoin", en *IEEE Symposium on Security and Privacy (SP)*, pp. 459-474, 2014.

[9] M. Crosby, P. Pattanayak y S. Verma y V. Kalyanaraman: "Blockchain technology: Beyond bitcoin", en *Applied Innovation*, vol. 2, pp. 6-10, 2016.

[10] P. Tarasov y H. Tewari: "The future of e-voting", en *Int. Journal on C.S. & I.S.*, vol. 12, n. 2, pp. 148-165, 2017.

[11] Agora: "Agora 0.2" [Online]. Disponible: Agora.vote, https://agora.vote/Agora_Whitepaper_v0.2.pdf. [Accedido 9 de Abril, 2018].

[12] K. Nikitin, E. Kokoris-Kogias, P. Jovanovic, N. Gailly, L. Gasser, I. Khoffi, J. Cappos y B. Ford: "CHAINIAC: Proactive software-update transparency via collectively signed skipchains and verified builds", en *26th USENIX Security Symposium*, pp. 1271-1287, 2017.

[13] J. Cucurull y J. Puiggalí : "Distributed immutabilization of secure logs", en *Int. Work. on Security and Trust Management*, pp. 122–137, 2016.

[14] Smartmatic y Cibernetica: "TIVI. Successfully solving the challenges." [Online]. Disponible: Smartmatic.com, http://www.smartmatic.com/fileadmin/user_upload/Whitepaper_Online_Voting_Challenge_Considerations_TIVI.pdf. [Accedido 9 de Abril, 2018].

[15] Smartmatic y Cibernetica: "TIVI. Verifiable voting. Accessible, anytime, anywhere." [Online]. Disponible: Smartmatic.com, http://www.smartmatic.com/fileadmin/user_upload/Smartmatic_Cybernetica_RemoteVoting.pdf. [Accedido 9 de Abril, 2018].

[16] M. Conti, C. Lal y S. Ruj: "A survey on security and privacy issues of bitcoin", en *arXiv preprint arXiv:1706.00916*, 2017.

[17] N. Gandal, J.T. Hamrick, T. Moore, y T. Oberman: "Price manipulation in the Bitcoin ecosystem", en *Journal of Monetary Economics*, 2018.

[18] J. Proos y C. Zalka: "Shor's discrete logarithm quantum algorithm for elliptic curves", en *Quantum Information & Computation*, vol. 3, n. 4, pp. 317-344 , 2003.

[19] K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E.G. Sirer y otros: "On scaling decentralized blockchains", en *Int. Conf. on Financial Cryptography and Data Security*, pp. 106-125, 2016.

[20] A. Miller, M. Möser, K. Lee, K. y A.Narayanan: "An empirical analysis of linkability in the Monero blockchain", en *arXiv preprint arXiv:1704.04299*, 2017.