Universidad de La Habana
Facultad de Matemática y Computación

Sistema de subasta a ciegas sobre Quorum

Autor:
Alben Luis Urquiza Rojas

Tutor:
Dr.C. Yaidir Mustelier Ruiz

Trabajo de Diploma
presentado en opción al título de
Licenciado en Ciencia de la Computación

Fecha: Noviembre 2022

github.com/ic-matcom/blind-auction-quorum

Contents

List of Figures

Ejemplos de código

Introducción

Cuando el 31 de octubre de 2008 Satoshi Nakamoto publicó el artículo *Bitcoin: A Peer-to-Peer Electronic Cash System* (documento técnico original de la bien conocida y primera criptomoneda: Bitcoin) (Nakamoto, 2008), creó las bases de una tecnología que está revolucionando al mundo, y el autor no se refiere al que bien pudiera ser el sistema de pago que sustituya al dólar y al dinero fiat en un futuro, sino a la blockchain.

Blockchain se traduce como cadena de bloques. Básicamente, blockchain es un conjunto de tecnologías que permiten llevar un registro seguro, descentralizado, sincronizado y distribuido de operaciones digitales, sin necesidad de la intermediación de terceros (Solunion, 2021).

En ese sentido, la definición más completa es la dada por Don & Alex Tapscott en su libro Blockchain Revolution : "un libro de contabilidad digital incorruptible de transacciones económicas que se puede programar para registrar no solo transacciones financieras, sino prácticamente todo lo que tiene valor" (Tapscott & Tapscott, 2016). Cada uno de los bloques de datos se encuentra protegido y vinculado entre sí criptográficamente. Las transacciones no las verifica un tercero, sino la red de nodos (computadores conectados a la red), que también es la que autoriza en consenso cualquier actualización en la blockchain (Solunion, 2021).

A finales de 2013, Vitalik Buterin publica el que luego se convertiría en el documento técnico (white paper) de Ethereum (Buterin, 2013). Este joven, quien hasta ese momento era uno de los programadores involucrado en el ecosistema Bitcoin, había notado el potencial de la criptografía para el desarrollo de aplicaciones descentralizadas. No obstante, su propuesta de crear un lenguaje de scripting para Bitcoin, que hiciera esto posible, no tuvo resonancia suficiente. Fue entonces cuando se propuso el desarrollo de una red independiente, con su propia infraestructura, para el desarrollo de un criptoactivo y una cadena de bloques capaz de soportar aplicaciones descentralizadas. Y el 30 de julio de 2015, Vitalik conjuntamente con otros programadores pusieron en línea la blockchain de Ethereum. (Díaz, 2018)

La red de Ethereum llevó a la práctica un nuevo concepto, los contratos inteligentes, en inglés conocidos como *smart contracts*. La definición más simple

al respecto es que se trata de contratos que tienen la capacidad de cumplirse de forma automática una vez que las partes han acordado los términos. Su nombre hace recordar a los contratos legales firmados en papel. Pero a pesar de que tienen cosas en común, son totalmente diferentes.

Los contratos inteligentes son programas informáticos. No están escritos en lenguaje natural, sino en código virtual. Son un tipo de software que se programa, como cualquier otro software, para llevar a cabo una tarea o serie de tareas determinadas de acuerdo a las instrucciones previamente introducidas. Su cumplimiento, por tanto, no está sujeto a la interpretación de ninguna de las partes: si el evento A sucede, entonces la consecuencia B se pondrá en marcha de forma automática. Su implicación legal ha caído -como toda la tecnología relacionada a Bitcoin- en una zona gris. No se requiere de ningún intermediario de confianza (como una notaría), pues este papel lo adopta el código informático, que asegurará sin dudas el cumplimiento de las condiciones. Por tanto, se reducen tiempo y costes significativamente. (Pérez, n.d.)

Las ventajas son obvias, y pueden reducirse a tres palabras: autonomía, seguridad y confianza. Utilizando contratos inteligentes ya no resulta necesario recurrir a un tercero —como un abogado o un notario—, que además de que pueden provocar errores, ocasiona gastos significativos. La blockchain es capaz de resguardar la información en una red cifrada que puede consultarse desde cualquier lugar del mundo, por lo que la velocidad y seguridad saltan a la vista.

Con esta nueva tecnología se puede crear una gran cantidad de nuevas aplicaciones para hacer trámites y transacciones hasta ahora difíciles de realizar con las tecnologías existentes, o simplemente mejorar servicios gracias a la descentralización de la blockchain y de los contratos inteligentes.

Una de estas aplicaciones de los contratos inteligentes está dada a las subastas. Una subasta es una venta generalmente pública en la que se adjudica una cosa, especialmente bienes o cosas de valor, a la persona que ofrece más dinero por ella. La blockchain puede y está cambiando, la manera en la que se hacen las subastas, ya sin necesidad de un subastador o de alguna entidad que haga de mediador. Ya muchas casas de apuestas han actualizado sus políticas, para adaptarse a los nuevos métodos, de hacer subastas.

Los mercados de deuda pública o de bonos soberanos(o del estado) siempre han hecho uso de subastas para hacer sus ventas. Con la blockchain se abre una nueva puerta para una forma segura, eficiente y sencilla de efectuar estas subastas.

Específicamente, en el presente trabajo se estudian las subastas a ciegas. Una subasta a ciegas es aquella en la que solo el ofertante sabe el monto de su oferta y nadie más. Él no conoce las ofertas de los demás y viceversa.

La implementación de subastas a ciegas sobre blockchain presupone una dificultad, pues toda información que se almacena es pública y verificable por cualquiera que esté

conectado a la red de nodos. La solución a esto podría ser el cifrado de las ofertas que hacen los pujadores. Por tanto, el problema consiste en la selección del algoritmo adecuado para el desarrollo de un sistema de subasta a ciegas sobre Quorum.

El **objetivo** general de este trabajo es el diseño e implementación de un conjunto de algoritmos que permita el desarrollo de subastas a ciegas sobre Quorum. Quorum es una blockchain basada en Ethereum.

Para lograr el objetivo general se definen los siguientes objetivos específicos:

1. Identificar las soluciones técnicas y tecnologías que se emplean para el desarrollo de aplicaciones relacionadas con subasta electrónica.

2. Valorar las posibilidades de Quorum como plataforma para el desarrollo de aplicaciones de este tipo.

3. Estudio de Solidity como lenguaje de programación para el desarrollo de contratos inteligentes sobre Quorum.

4. Implementar contratos inteligentes (algoritmos) que permitan efectuar subastas a ciegas.

La memoria escrita está organizada en 3 Capítulos. En el Capítulo 1 se aborda el tema de las subastas, qué beneficios presenta la blockchain para el desarrollo de subastas y una comparación entre algunos tipos de protocolos de subastas a ciegas sobre blockchain. En el Capítulo 2 se explica la utilización de la blockchain de Quorum para el desarrollo de un sistema de subastas a ciegas. El Capítulo 3 está dedicado a la evaluación de los resultados y mostrar el desempeño del método propuesto. Finalmente, se dan las conclusiones de la investigación, recomendaciones, así como la bibliografía y los anexos necesarios para la mejor comprensión de la propuesta.

Chapter 1

Subastas y blockchain

1.1 Subastas

Una subasta es el proceso de comprar y vender bienes o servicios. Este proceso implica ofrecer artículos para vender, esperar que sean enviadas las ofertas y vender los bienes a la mayor oferta, bajo la supervisión de un subastador (Krishna, 2009).

Por la relevancia del término, se considera importante revisar qué definiciones formales de "subasta" existen:

- Definición de la RAE: 1. f. Venta pública de bienes o alhajas que se hace al mejor postor, y regularmente por mandato y con intervención de un juez u otra autoridad. 2. f. Adjudicación de una contrata, generalmente de servicio público, como la ejecución de una obra, el suministro de provisiones, etc., a quien presenta la propuesta más ventajosa (Real Academia Española, n.d.).

- Economipedia: Una subasta es un procedimiento de venta donde los interesados compiten entre sí para adjudicarse el bien o servicio a ser subastado (Roldán, 2017).

1.1.1 Tipos de subastas

Las subastas pueden clasificarse en diferentes tipos. A continuación se resumen las características de las más conocidas.

- English Auction (Subasta Inglesa o ascendente). Este es el tipo de subasta más conocido. Las pujas comienzan con un precio bajo, y se incrementan progresivamente a medida que se solicitan pujas más altas, hasta que se cierra la subasta o no se reciben pujas más altas. A menudo el vendedor fija un precio de reserva por debajo del cual

el artículo no se vende y la subasta se cancela. Permite a un vendedor asegurar el precio más alto para un artículo.

- Dutch Auction (Subasta holandesa o descendente). El precio empieza alto y va bajando hasta que algún participante está dispuesto a pagar el precio, y este es el que gana y paga el último precio que se menciona.

- Blind Auction (Subasta a ciegas o de sobre cerrado). También conocida en la literatura como First-Price sealed-bid auction (FPSBA) En este tipo de subasta, todas las ofertas se envían simultáneamente y nadie sabe qué oferta hizo el resto de los participantes. Gana el que mayor oferta hizo y paga esa cantidad al vendedor.

- Vickrey Auction (Subasta Vickrey). Conocida también en la literatura en inglés como sealed-bid second-price auction (SBSPA) . Es un tipo de subasta de puja sellada, donde los oferentes presentan ofertas por escrito sin conocer la oferta de las otras personas en la subasta, y en la que gana el postor más alto, pero el precio que paga este es la segunda oferta más alta (2017).

- All-pay auction (Subasta americana). Es como la subasta inglesa, en este caso todos los postores deben pagar la oferta que hacen, pero solo el que realiza la mejor oferta obtiene el producto.

- Silent auction (Subasta Silenciosa). Las pujas se escriben en hojas de papel. Al final de la subasta, la puja más alta se adjudica la subasta. Este tipo de subasta se utiliza frecuentemente en eventos de beneficencia, en los que se subastan muchos objetos simultáneamente, y se "cierra" a una hora predeterminada común a todos los objetos. La subasta es "silenciosa" porque no hay subastador y los pujadores escriben sus pujas en una hoja que usualmente se deja en una mesa cercana al objeto. En las subastas de beneficencia, las hojas usualmente indican una puja inicial mínima, los incrementos que se pueden hacer sobre dicha puja mínima y una cantidad, llamada "puja garantizada" que si se paga se obtiene el objeto de forma inmediata. Otras variaciones de este tipo de puja pueden incluir pujas selladas. El pujador con la puja más alta paga el precio que indicó en su hoja y obtiene el bien (Investopedia.com, n.d.).

- Reverse auction (Subasta inversa o reversa). Es un tipo de subasta en la que se invierten los papeles de comprador y el vendedor. En una subasta ordinaria, los compradores compiten para obtener un bien o servicio, ofreciendo precios cada vez más altos. En una subasta inversa, los vendedores compiten para obtener negocio del comprador y los precios suelen disminuir a medida que los vendedores hacen sus ofertas.

- Candle Auction (Subasta de velas). Es una variación de la subasta típica inglesa que se hizo popular en los siglos XVII y XVIII. En una subasta de velas, el final de la subasta se indica con el vencimiento de la llama de una vela, que tenía la intención de garantizar que nadie pudiera saber exactamente cuándo terminaría la subasta y hacer una oferta de último segundo. A veces, se utilizaron otros procesos

impredecibles, como una carrera a pie, en lugar de la expiración de una vela (Patten, 1970).

- Double Auction (Subasta Doble). Una doble subasta es un proceso de compra y venta de bienes cuando los compradores potenciales y los posibles vendedores presenten simultáneamente sus ofertas, su demanda, los precios de una casa de subastas, y luego un subastador elige algún precio p que equilibra el mercado: todos los vendedores que solicitaron menos de p venden y todos los compradores que pujaron más de p compran a este precio p (Friedman, 1992).

Hay algunos otros tipos de subasta, pero mucho menos conocidas. Como fue explicado en la Introducción, la presente investigación se enfoca precisamente en subastas a ciegas.

1.1.2 Mercado de deuda

El mercado de deuda o bonos es donde se emiten y negocian los títulos de deuda, cuando los participantes no están en condiciones o no desean pedir préstamos o créditos a la banca. En él participan el Gobierno Federal, los gobiernos estatales o locales y las empresas paraestatales o privadas que necesitan financiamiento, ya sea para realizar un proyecto de inversión o para mantener sus propias actividades. Una parte de este mercado se conoce como mercado del dinero, que es donde se intercambian los bonos que por su corto plazo, liquidez y alta seguridad se pueden considerar sustitutos del dinero.

El mercado de deuda también se conoce con otros nombres, dependiendo del tipo de instrumentos de deuda negociado. Por ejemplo, si en el mercado se negocian principalmente instrumentos de deuda que pagan una tasa fija, entonces se denomina mercado de renta fija, mercado de renta variable, mercado de deuda internacional, de deuda pública, etc. En términos generales, para que una persona pueda comprar o vender títulos de deuda es necesario que acuda a un banco o a una casa de bolsa para que dichas instituciones puedan efectuar las transacciones necesarias a nombre de esta persona (Banco de México, n.d.).

La presente investigación se enfoca específicamente en el mercado de deuda pública o el mercado de bonos del Estado. Un bono del Estado es un tipo de inversión basada en deuda, en la cual se le presta dinero a un gobierno a cambio de una tasa de interés acordada. Los gobiernos los utilizan para generar fondos que pueden gastar en nuevos proyectos o infraestructura, mientras que los inversores pueden usarlos a fin de que se les pague un retorno establecido en intervalos periódicos.

Cuando se compra un bono del Estado, se le presta al Gobierno una cantidad acordada de dinero durante un período también acordado. A cambio de esto, el Gobierno devuelve el dinero con un nivel establecido de interés de forma periódica,

lo que se conoce como cupón. De esta manera, los bonos conforman un activo de ingreso fijo.

Cuando el bono venza, se devolverá la inversión original (denominada principal). El día en el que se recibe el valor de capital adeudado se conoce como la fecha de vencimiento. Diferentes bonos tienen distintas fechas de vencimiento; por ejemplo, se puede comprar un bono que vence en menos de un año o uno que vence en 30 años o más.

Algunos inversores dicen que los bonos del Estado son inversiones libres de riesgo. Dado que un gobierno siempre puede imprimir más dinero para saldar sus deudas, teóricamente hablando, siempre se devolverá tu dinero cuando venza el bono.

En la realidad, esto es mucho más complicado. En primer lugar, los gobiernos no siempre pueden producir más capital. Incluso si es que pudieran hacerlo, esto no evita que incumplan el pago de los préstamos. No obstante, aparte del riesgo crediticio, existen otros posibles problemas de los cuales preocuparse con los bonos del Estado, por ejemplo, el riesgo de las tasas de interés, la inflación y las divisas (ig.com, n.d.).

1.1.3 Mercado de Deuda Pública en Cuba

Cuando en la economía doméstica los gastos superan a los ingresos no queda más remedio que pedir prestado, de lo contrario no se pudiera pagar lo que necesitamos o debemos. En otras palabras, se tendría que disminuir o aplazar las compras. Al presupuesto del Estado le sucede exactamente lo mismo y sus ausencias de dinero se llaman déficit fiscal. La deuda pública es la suma del déficit fiscal del año, más las garantías que se activen en esos 12 meses (porque el presupuesto del Estado es garante de determinadas operaciones económicas como inversiones en sectores priorizados) y las amortizaciones de deudas anteriores provenientes de los bonos que se colocaron en lo años anteriores.

Pero, ¿cómo se financia el déficit presupuestario? Esto ocurre mediante bonos soberanos de la República de Cuba que emite el Ministerio de Finanzas y Precios (MFP) y que hasta el momento han sido adquiridos por el sistema bancario nacional.

El Banco de Inversiones es el encargado de colocar, emitir y registrar la emisión. El MFP le solicita una emisión de bonos y este lo coloca en el sistema bancario, y cada banco comercial (Banco de Crédito y Comercio, Popular de Ahorro y Metropolitano) adquiere el monto que puede asumir. En caso de que los bancos no tengan suficiente liquidez para cubrir totalmente el bono, interviene el Banco Central de Cuba (BCC) con la emisión de nuevos billetes.

Hasta 2013, el déficit se financiaba solo de esta manera (con la emisión de monedas por el BCC), pero debido a la inflación que provoca el exceso de dinero en circulación fueron instrumentados los bonos soberanos y siempre se busca que la participación

del BCC sea en última instancia, porque es un dinero que se pone en circulación sin respaldo productivo (Tamayo & Ferrer, 2021).

A pesar de que ya desde 2014 estan siendo emitidos los títulos de deuda soberana y de que legalmente es posible transar estos valores, la inexistencia de incentivos que promuevan la demanda de los títulos públicos y de condiciones básicas institucionales y de infraestructura del mercado han condicionado que las primeras colocaciones de bonos se hayan realizado mediante asignaciones administrativas. Lo anterior demuestra que no resulta suficiente con emitir los títulos, si ello no se acompaña de transformaciones y reformas institucionales, estructurales, normativas y regulatorias que permitan ordenar, organizar e incentivar el funcionamiento de un Mercado de Deuda Pública. El sistema empleado hasta ahora esta muy lejos de ser el ideal. Para profundizar en este tema, se puede revisar (Barceló, 2017).

Por parte del Instituto de Criptografía se desarrolla para el Banco Central de Cuba una plataforma para el Mercado de Deuda Pública de Cuba. Una de las propuestas a utilizar en esta plataforma es una variación de la subasta holandesa (como se utiliza en casi todo el mundo), pero en este caso, a ciegas sobre una blockchain, específicamente la blockchain de Quorum 1.1.

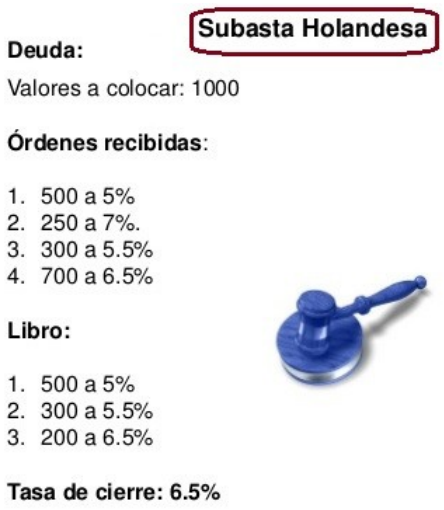

Figure 1.1: Ejemplo de subasta holandesa en el mercado de deuda

1.2 Blockchain

Las subastas tradicionales usualmente requieren una tercera persona, ya sea un subastador o una casa de subastas que maneje el proceso completo de subasta, lo cual puede llegar a tener muy altos impuestos por comisiones. También sufren de un punto de fallo, los subastadores pueden en ocasiones tener malas intenciones (Wu

et al., 2019). En este contexto, blockchain surge como una plataforma descentralizada que puede ser empleada para aplicaciones de subastas en línea confiables. En 2018, por primera vez en el mundo una colección de arte valuada en varios millones de dólares perteneciente a Andy Warhol fue tokenizada y subastada satisfactoriamente, usando la blockchain de Ethereum (Emem, 2018; Wood, 2021). Es también conocido que una de las mayores casas de subastas (e.g., Sotheby's and Christie's) está activamente trabajando en aplicar blockchain para subastas seguras y confiables (Neuendorf., 2018).

La tecnología blockchain elimina efectivamente los intermediarios, por lo tanto, reduce los costos de transacción y asegura la confianza entre las partes interesadas en la subasta. En general, la tecnología blockchain puede mejorar las subastas en los siguientes aspectos (Shi et al., 2021):

- Inmutabilidad de las transacciones de la subasta. Cada transacción ejecutada en la blockchain es pública, verificable e inmutable. Esto significa que la blockchain puede ser empleada como dispositivo de certificado de auditoría que previene que los participantes hagan trampa durante la subasta. El ganador puede usar la blockchain como prueba de la transacción.

- Automatización del proceso de subasta. Un contrato inteligente automatiza el proceso de la subasta en la blockchain. Casi toda la lógica de la subasta puede ser predefinida en contratos inteligentes para facilitar el intercambio de bienes y servicios, así como el pago de los tokens.

- Descentralización del manejo de la subasta. No hay necesidad de designar una tercera persona como subastador, que asegure la confiabilidad. Las tradicionales subastas centralizadas pueden ser muy costosas y sujeta a posibles subastadores tramposos; casas de subastas típicamente cargan del 8 al 20% como comisión.

- Flexibilidad en el pago de la subasta. Las criptomonedas existentes en la blockchain pueden mejorar la seguridad y flexibilidad del pago de la subasta. Al mismo tiempo, un sistema de pago descentralizado, no necesita de intermediarios financieros, haciendo las transacciones más convenientes y menos costosas.

1.2.1 Quorum

Blockchain es de los términos más usados en el mundo de la tecnología en estos días. Mientras esta tecnología es el elemento núcleo de las criptomonedas que están llegando a los mercados financieros, su utilidad no es limitada a las criptos y tiene muchos más casos de uso. Con el pasar de los años, diferentes plataformas blockchain han sido desarrolladas con sus propios mecanismos de consenso y métodos de encriptación.

Una de estas plataformas es la blockchain de Quorum, la cual ha ganado

popularidad en los últimos tiempos, como resultado de la larga lista de casos de uso que Quorum provee a sus usuarios. La red de Quorum está basada en una bifurcación de la blockchain de Ethereum. Es un protocolo blockchain de código abierto especialmente diseñado para usar en redes blockchain privadas. Algo a destacar de esta red es su nueva característica llamada *"private transaction identifier"* que asegura la privacidad de los datos. El objetivo de construir Quorum es utilizar la tecnología existente tanto como sea posible. Por lo tanto, incluso si la red Ethereum se somete a diferentes actualizaciones en el futuro, habría pocos o ningún cambio en la blockchain de Quorum para mantener la sincronización entre estas redes.

1.2.2 Subastas a ciegas sobre blockchain

Las subastas sobre blockchain han sido una área centro de muchas investigaciones en los últimos años, razón por la cual ya se han desarrollado algunos protocolos de subastas a ciegas sobre blockchain. Algunos de los cuales son:

- Kosba et al., 2016: propuso Hawk, una combinación de la privacidad de Zcash con la programabilidad de Ethereum. Los contratos inteligentes que preservan la privacidad han sido empleados para manejar la privacidad de las transacciones en la *blockchain* de Ethereum. Ellos se enfocan en presentar un *framework* que puede simultáneamente admitir varias aplicaciones como subasta de puja sellada, el juego de piedra, papel y tijera, aplicación de *crowfunding* e intercambiar instrumentos financieros. La principal limitación de Hawk es que depende de un gestor, de confianza explícita, para no filtrar entradas secretas al contrato inteligente.

- Blass and Kerschbaum, 2018: Strain presenta un protocolo para construir una subasta de puja sellada sobre una blockchain, preservando la privacidad de las ofertas contra partes maliciosas. Se utiliza un tablón de anuncios para publicar la oferta ganadora que es determinada comparándolas por pares. Dos conocimientos de prueba cero (*zero-knowledge proofs (ZKP)*) aseguran que los participantes usan sus ofertas originales bajo compromiso y que el subastador declare el ganador, sin ninguna manipulación. Los participantes maliciosos son castigados por abrir su compromiso, ya que su clave privada está parcialmente compartida entre todos los participantes a través de un proceso de generación distribuida de claves.

- Galal and Youssef, 2018b: Galal y Youssef propusieron una subasta de puja sellada en la *blockchain* Ethereum con contrato inteligente y pruebas de conocimiento cero (*zero-knowledge proofs*). Ofertantes envían sus pujas al contrato inteligente usando *Pedersen commitment* Pedersen, 1991. Los compromisos (commitments) son secretamente revelados al subastador vía un esquema *Public Key Encryption (PKE)*. Después de declarar el ganador, por cada oferta perdedora, el subastador tiene que participar en un conjunto de protocolos interactivos de compromiso-desafío-verificación para demostrar que la puja ganadora es mayor que las pujas perdedoras y

como consecuencia, la complejidad de la interacción depende del número de ofertantes. Luego Galal and Youssef, 2018a mejoraron este protocolo presentando un contrato inteligente con una verificablemente concisa *ZKP* que permite una sola prueba de verificación para todo el proceso de la subasta. Similar a Zcash, ellos emplearon *Multi-Party Computation (MPC)* entre el subastador y pujantes. El esquema propuesto implementa la validez, imparcialidad y secreto de las transacciones en la subasta. Sin embargo, depende de un subastador externo.

- Sánchez, 2020: un contrato inteligente privado y verificable, se introduce como una combinación de *Multi-Party Computation* segura y *Proof-carrying code* enfocada principalmente en garantizar la correctitud, privacidad y verificabilidad para contratos inteligentes en la *blockchain*. Este enfoque puede ser utilizado para varias aplicaciones tal como privadas y verificables *crowdfundings*, fondos de inversión y subastas dobles para intercambios descentralizados.

- Sharma et al., 2021: introdujo un protocolo genérico para comercio anónimo de manera justa usando solamente estándar construcción de bloques criptográficos. Las propiedades confidencialidad y anonimato son alcanzadas utilizando *Designated Verifier Ring Signature (DVRS)* y la transparencia y auditabilidad de la plataforma blockchain se aprovecha para realizar el proceso de subasta públicamente verificable. Se asume la existencia de una *blockchain* que permita transacciones anónimas y confidenciales. También se analiza la eficiencia de emplear primitivas criptográficas en la *blockchain* de Ethereum e investigar la complejidad y vulnerabilidades que un entorno *blockchain* podría introducirse durante la implementación.

- H. Li, 2021: se propone un esquema de subasta electrónica de puja sellada basada en *blockchain* con algoritmo de compromiso, contratos inteligentes y *zero-knowledge proof (ZKP)* para proteger la fuga de información de las pujas y verificar el resultado de la subasta con todos los ofertantes anónimamente, que implementa satisfactoriamente la seguridad y justicia de la subasta sin necesidad de un subastador externo. El esquema propuesto presenta limitaciones en cuanto al tiempo de corrida. El tiempo de ejecución de dos de las fases, abierta y finalización, están determinadas por el número de ofertantes. Esto significa que la subasta se convertiría en un trabajo que consume mucho tiempo en el caso de ser usando en plataformas abiertas como Internet.

De acuerdo a la revisión de la literatura hecha anteriormente, los estudios relacionados tienen algunos defectos para los esquemas de subasta de puja-sellada. Y en especial para el que se quiere implementar, una variación de la subasta holandesa con subasta a ciegas.

1 - Los riesgos del modo de transacción centralizado: como se discutió anteriormente, en subastas tradicionales, todas las transacciones están en control de los subastadores. Ha sido demostrado que subastadores no confiables pueden causar filtración del precio de la puja y alterar el resultado de la subasta. En los

estudios relacionados, la mayoría de subastas electrónicas, incluso las basadas en *blockchain*, todavía utilizan subastadores para controlar las transacciones. Por lo tanto, la equidad y fiabilidad de las subastas no están perfectamente garantizadas.

2 - Ocultar el precio: ocultar el precio de las pujas es el núcleo de las subastas de puja sellada. En la mayoría de los estudios relacionados, el precio de la puja es protegido por encriptación. Sin embargo, en la fase abierta, el precio de la puja es desencriptado y directamente revelado por verificación, lo cual puede causar filtración de precios.

3 - Precio ganador: todos los esquemas vistos basan sus algoritmos para encontrar un único ganador, la puja más alta. Sin embargo, para el problema en cuestión es posible y casi seguro que haya varios ganadores. Es necesario buscar una estrategia factible para este caso.

Bibliography

Banco de México. (n.d.). Mercados financieros [Recuperado el 21 de Septiembre de 2022, de http://educa.banxico.org.mx/banco_mexico_banca_central/sist-finc-mercados-financiero.html]. (Cit. on p. 6).

Barceló, A. (2017). Mercado de Deuda Pública, una propuesta de acciones de política para Cuba. [Tesis de Maestría. La Habana, Cuba]. https://www.bc.gob.cu//storage/investigaciones/March2018/AGZ1q0hd9wboRpF1L93d.pdf. (Cit. on p. 8)

Blass, E., & Kerschbaum, F. (2018). Strain: A Secure Auction for Blockchains. [In ESORICS; Springer: Berlin/Heidelberg, Germany, 2018; Volume 11098, pp. 87–110.]. (Cit. on p. 10).

Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform [Recuperado el 16 de Octubre de 2022, de https://ethereum.org/en/whitepaper/]. (Cit. on p. 1).

Díaz, G. (2018). Ethereum: historia de la plataforma de contratos inteligentes más usada [Recuperado el 11 de Septiembre de 2022, de https://www.criptonoticias.com/tecnologia/ethereum-historia-plataforma-contratos-inteligentes-usada/]. (Cit. on p. 1).

Emem, M. (2018). Andy Warhol's Multi-Million Dollar Painting Tokenized and Sold on Blockchain. (Cit. on p. 9).

Friedman, D. (1992). The Double Auction Market Institution: A Survey [http://www.its.caltech.edu/~pbs/expfinance/Readings/FriedmanDA.pdf]. (Cit. on p. 6).

Galal, H., & Youssef, A. (2018a). Succinctly Verifiable Sealed-Bid Auction Smart Contract [In Data Privacy Management, Cryptocurrencies and Blockchain Technology; Springer: Berlin/Heidelberg, Germany]. (Cit. on p. 11).

Galal, H., & Youssef, A. (2018b). Verifiable Sealed-Bid Auction on the Ethereum Blockchain [In Financial Cryptography; Springer: Berlin/Heidelberg, Germany]. (Cit. on p. 10).

H. Li, W. X. (2021). A Blockchain-Based Sealed-Bid e-Auction Scheme with Smart Contract and Zero-Knowledge Proof. (Cit. on p. 11).

ig.com. (n.d.). ¿Qué son los bonos del Estado y cómo comerciar con ellos? [Recuperado el 21 de Septiembre de 2022, de https://www.ig.com/es/bonos/que-son-los-bonos-del-estado-y-como-comerciar-con-ellos]. (Cit. on p. 7).

Investopedia.com. (n.d.). (Cit. on p. 5).

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts [In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016; pp. 839–858.]. (Cit. on p. 10).

Krishna, V. (2009). Auction Theory. (Cit. on p. 4).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. (Cit. on p. 1).

Neuendorf., H. (2018). Christie's Will Become the First Major Auction House to Use Blockchain in a Sale. (Cit. on p. 9).

Patten, R. (1970). Tatworth Candle Auction (N. 2. (1. Folklore 81, Ed.). (Cit. on p. 6).

Pedersen, T. (1991). Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing [In CRYPTO; Springer: Berlin/Heidelberg, Germany]. (Cit. on p. 10).

Pérez, I. (n.d.). Qué son los contratos inteligentes [Recuperado el 11 de Septiembre de 2022, de https://www.criptonoticias.com/criptopedia-old/que-son-contratos-inteligentes-blockchain-criptomonedas/]. (Cit. on p. 2).

Real Academia Española. (n.d.). Subasta [Recuperado el 18 de Septiembre de 2022, de https://dle.rae.es/subasta]. (Cit. on p. 4).

Roldán, P. N. (2017). Subasta (Economipedia.com, Ed.) [Recuperado el 19 de Octubre de 2022, de https://economipedia.com/definiciones/subasta.html]. (Cit. on pp. 4, 5).

Sánchez, D. C. (2020). Raziel: Private and Verifiable Smart Contracts on Blockchains [https://eprint.iacr.org/2017/878]. https://eprint.iacr.org/2017/878. (Cit. on p. 11)

Sharma, G., Verstraeten, D., Saraswat, V., Dricot, J.-M., & Markowitch, O. (2021). Anonymous Sealed-Bid Auction on Ethereum. [Electronics 2021, 10, 2340. https://doi.org/10.3390/electronics10192340]. (Cit. on p. 11).

Shi, Z., de Laat, C., Grosso, P., & Zhao, Z. (2021). When Blockchain Meets Auction Models: A Survey, Some Applications, and Challenges [1v43521.0112:viXra]. (Cit. on p. 9).

Solunion. (2021). ¿Qué es y para qué sirve la tecnología blockchain? [Recuperado el 10 de Septiembre de 2022, de https://www.solunion.cl/blog/que-es-y-para-que-sirve-la-tecnologia-blockchain/]. (Cit. on p. 1).

Tamayo, E. C., & Ferrer, L. I. (2021). ¿Cómo se financia el déficit presupuestario de Cuba? (cubadebate.com, Ed.) [Recuperado el 21 de Septiembre de 2022, de

http://www.cubadebate.cu/especiales/2021/06/08/como-se-financia-el-deficit-presupuestario-de-cuba/]. (Cit. on p. 8).

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Portfolio / Penguin. https://books.google.com.cu/books?id=L1QHjwEACAAJ. (Cit. on p. 1)

Wood, G. (2021). Ethereum: A Secure Decentralised Generalised Transaction Ledger. (Cit. on p. 9).

Wu, S., Chen, Y., Wang, Q., Li, M., Wang, C., & Luo, X. (2019). CReam: A smart contract enabled collusion-resistant e-auction (I. T. I. F. Security, Ed.) [vol. 14, no. 7]. (Cit. on p. 8).