UTN.BA FACULTAD REGIONAL BUENOS AIRES

TRABAJO FINAL INTEGRADOR

Especialización en Ingeniería en Sistemas de Información

Título:

"Marco de trabajo para el análisis forense de delitos en la Blockchain"

Autor: Fernandez Diego

Tutor: Dr. Hernán Merlino

UTN.BA FACULTAD REGIONAL BUENOS AIRES

Marco de trabajo para el análisis forense de delitos en la Blockchain

Alumno
Lic. Fernandez Diego

Directores
Dr. Hernán Merlino

TRABAJO FINAL PRESENTADO PARA OBTENER EL GRADO DE ESPECIALISTA EN INGENIERÍA EN SISTEMAS DE INFORMACIÓN

ESCUELA DE POSGRADO FACULTAD REGIONAL DE BUENOS AIRES UNIVERSIDAD TECNÓLOGICA NACIONAL

Julio, 2023

RESUMEN

En el mundo actual de tecnologías nuevas y cambios constantes, las criptomonedas están dando que hablar, muchas personas están pasando sus ahorros y sus inversiones a porfolios virtuales sin saber que hay detrás de las mismas ni los riesgos que esto conlleva.

El presente trabajo expone la tecnología que las soporta y les da vida, realiza un repaso por sus distintas partes ytrata los problemas que trae acarreados, desde la seguridad hasta los delitos que se presentan con y sobre estas, para dar lugar a un futuro marco de trabajo para el análisis forense de delitos donde las criptomonedas se vean involucradas.

Palabras claves

Bitcoin, Criptomonedas, Monedas virtuales, Blockchain, Billetera virtual, Delitos cibernéticos, PoW, Bloques.

ABSTRACT

In today's world of new technologies and constant changes, cryptocurrencies are making people talk, many people are passing their savings and investments to virtual portfolios without knowing what is behind them or the risks that this entails.

The present work will expose the technology that supports them and gives them life, will review their different parts and will deal with the problems that they bring about, from security to the crimes that occur with and on them, to give rise to a future framework. work for the forensic analysis of crimes where cryptocurrencies are involved.

Keywords

Bitcoin, Cryptocurrencies, Virtual currencies, Blockchain, Virtual wallet, Cybercrime, PoW, Blocks.

ÍNDICE

Índice de imágenes

Índice de Gráficos

Índice de Tablas

1. Introducción

En las secciones posteriores se examina la importancia del trabajo de especialidad en la actualidad (sección 1.1) y se plantea el objetivo principal como los objetivos específicos a abordar en el presente trabajo de investigación (sección 1.2).

1.1 Importancia del trabajo de investigación

La cadena de bloques vino a ser una tecnología disruptiva, ya que cambia el concepto utilizado a nivel mundial del dinero y lo que representa.

Pensar en un sistema de pagos totalmente distribuido y realizado entre pares sin necesidad de un tercero de confianza, da cierta libertad, pero a contrapartida puede generar varios problemas, ya que no hay una entidad que avale la transacción.

El presente trabajo transmite qué son las criptomonedas, la tecnología que las soporta y cuáles son sus riesgos, ya que muchas empresas y particulares se están volcando a estas sin conocer cómo funcionan ni a que están expuestos.

1.2 Objetivo principal

El objetivo principal de este trabajo de especialidad es el entendimiento de la tecnología blockchain, las criptomonedas y sus delitos como así también la investigación de los Framework actuales aplicables a la investigación forense informática con la finalidad de dar lugar al desarrollo de un marco de trabajo que permita el análisis forense de las criptomonedas y sus delitos asociados.

1.3 Objetivos Específicos

- Recolectar información sobre la tecnología Blockchain.
- Analizar los distintos algoritmos de consenso.
- Describir las principales criptomonedas del mercado.
- Investigar los delitos relacionados.
- Llevar a cabo un análisis de los actuales Framework de análisis forense informático.

2. Estado del Arte

En las siguientes secciones se explora la tecnología Blockchain (sección 2.1)para luego ver qué son las criptomonedas (sección 2.2), cómo se almacenan en las billeteras virtuales (sección 2.3) y los distintos tipos de delitos perpetuados hasta la fecha en donde los criptoactivos están relacionados (sección 2.4).

2.1 Blockchain

En las siguientes secciones se expone la historia de Blockchain (sección 2.1.1) para luego ver su funcionamiento (sección 2.1.2), los usos de la tecnología (sección 2.1.3), su trazabilidad y seguridad (sección 2.1.4).

2.1.1 Historia

La cadena de Bloques (Blockchain) como se conoce hoy en día se fue desarrollando por partes, el primer concepto se conoció mediante la publicación presentada por los científicos Stuart Haber y W. Scott (Haber and Stornetta, 1991) en la cual, se plantea el concepto de una cadena de bloques para poder darle una marca de tiempo a los distintos documentos computacionales con el fin de que los mismos no se pudieran modificar; en su trabajo, ellos se plantean dos necesidades básicas: que se pueda sellar un documento independientemente de su soporte y que el mismo no pueda ser alterado de ninguna manera, para lo cual plantean utilizar un cálculo de Hash (algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija) sumado a la marca de tiempo, para firmar los documentos uniendo el cálculo de un documento con el siguiente formando la cadena en donde si se altera un documento, se va a alterar toda la cadena por la unión previamente mencionada.

En 1992, suman a su teoría el concepto de los árboles de Merkel (Bayer et al., 1999) con la finalidad de hacer más eficiente el protocolo de sellado, pensando en la cantidad de usuarios posibles y en los recursos disponibles que siempre son finitos.

La tecnología planteada originalmente en 1991 quedó en desuso y su patente se liberópara el año 2004; fue cuando el ingeniero Hal Finney (“RPOW - Reusable Proofs of Work | Satoshi Nakamoto Institute,” n.d.) propuso la RPOW (prueba de trabajo reutilizable) pensada para la creación de dinero digital basando su idea en el concepto de Nick Szabo (“Shelling Out: The Origins of Money | Satoshi Nakamoto Institute,” n.d.)(Academy, 2019).

El concepto de Hal fue fundamental para la tecnología actual dado que planteaba la creación de un token RPOW, proporcionando una cadena de prueba de trabajo que se asignan

a la firma privada; luego el cliente podría transferir esos token a otra clave privada. Este proceso se centraba en un servidor seguro centralizado.

Para el año 2008, Satoshi Nakamoto (aún se desconoce si es una persona o un grupo de personas) presentó un trabajo titulado “Bitcoin: A Peer-to-Peer Electronic Cash System” o “White paper” en donde introduce un sistema de efectivo electrónico descentralizado llamado “Bitcoin” (Nakamoto, n.d.).

Bitcoin se basa en la prueba de trabajo, pero en vez de utilizar la solución propuesta por Hal, donde utilizaba un hardware especializado y centralizado, Bitcoin le delega esta tarea de prueba de trabajo a la red donde los mineros realizan la misma y todos los miembros de la red descentralizada verifican que el resultado sea correcto.

El3 de enero del 2009, se puso en marcha la red de Bitcoin con el minado del primer bloque por la cual Satoshi Nakamoto recibió una recompensa de 50 Bitcoin. La primera transacción de la red fue realizada por Satoshi Nakamoto el 12 de enero del mismo año en donde le envió a Hal Finney 10 Bitcoin(Ast, 2019).

En el año 2013, Vitalik Buterin plantea en la comunidad la necesidad de un lenguaje de scripting para crear aplicaciones descentralizadas que trabajen sobre la blockchain de Bitcoin. Como no tuvo aceptación, presentó Ethereum(“Ethereum Whitepaper,” n.d.), una plataforma basada en Blockchain en donde se puede, mediante un lenguaje de programación, generar contratos inteligentes, aplicaciones descentralizadas, etc.

Ethereum tiene su propia moneda virtual llamada “Ether” que permite realizar transacciones económicas, tal como hace el Bitcoin, pero también permite “pagar” por el cálculo informático utilizado para generar las transacciones de los contratos inteligentes entre otros.

2.1.2 Funcionamiento de la tecnología

Cuando se habla de criptomonedas hay que mencionar a la tecnología de Blockchain. La idea en sí es la de generar un registro distribuido en donde todos los nodos participantes le den robustez al sistema al estar en sincronización con la cadena; los mismos son los que dan el consenso. Sin esta tecnología, no se podría haber implementado las criptomonedas tal como las conocemos.

Antes de detallar la tecnología, hay que mencionar que la robustez descentralizada está dada por distintos algoritmos de consenso. En el presente trabajo, se define la PoW (prueba de trabajo) dado que es uno de los algoritmos más robustos y difícil de vulnerar como también lo es la PoS (prueba de participación), ya que es utilizada por muchas plataformas de Blockchain en la actualidad. Hay varios algoritmos más en uso como DPoS, LPoS, PoET, etc., pero no están tan difundidos y de allí es que no se hace mención en el presente.

Tomando el caso de la Blockchain consensuada por PoW, la cadena está formada por bloques; estos bloques están conformados por transacciones, un hash del bloque anterior y un

hash especifico del propio bloque. El hash del propio bloque está formado por un cálculo muy complejo en donde interviene un Nonce que le da complejidad al cálculo. Obtener este número de hash va a generar que la comprobación del bloque sea muy difícil de lograr, de ahí la seguridad de la cadena. La verificación del hash obtenido es muy rápida de efectuar, lo que genera que la tecnología sea eficaz.

En la imagen siguiente se puede ver lo mencionado(“Bloques y transacciones,” n.d.)

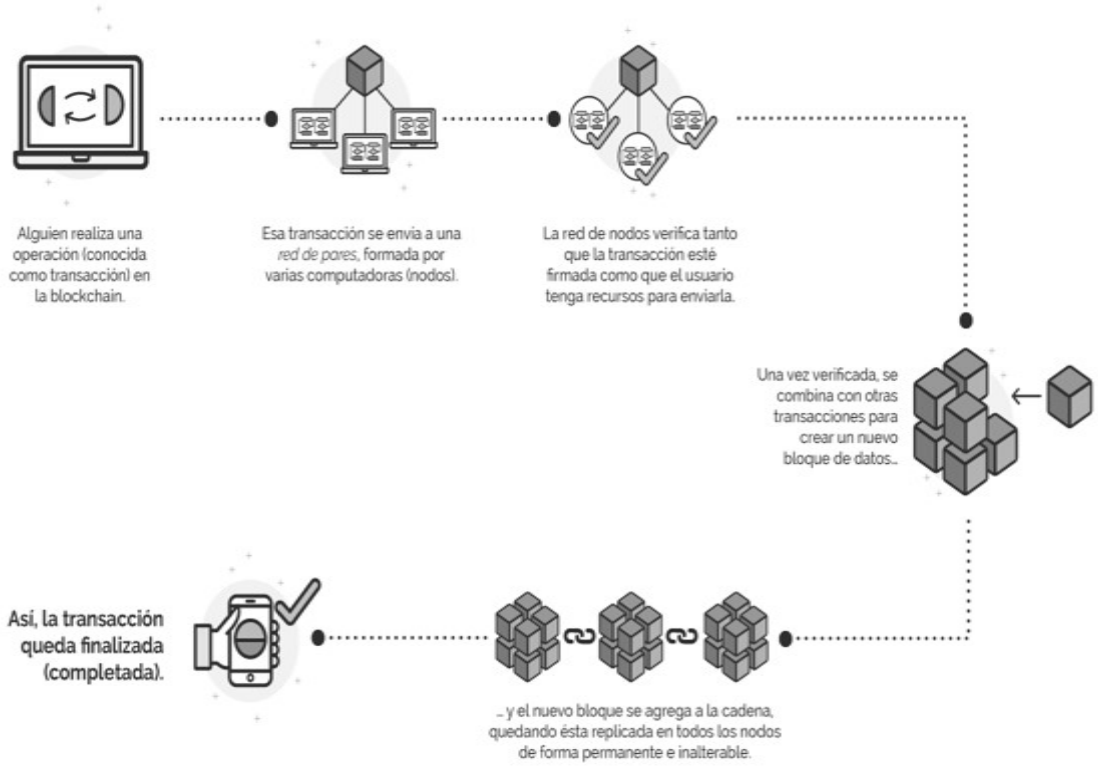

Imagen 1- Funcionamiento de la cadena de bloques

A continuación, se analiza la plataforma de Bitcoin, ya que es la criptomoneda más difundida, de mayor valor en la actualidad y desde donde parten las diferentes blockchain que utilizan otras monedas virtuales.

Satoshi Nakamoto, creador del Bitcoin, presenta su trabajo titulado “White paper” (Nakamoto, n.d.). Nakamoto toma los trabajos previos de Hal Finney, Haber y W. Scott para armar la plataforma de Bitcoin. Su motivación está dada en generar un sistema de transacciones económicas para la nueva era de internet donde se puedan efectuar entre pares (p2p), sin un tercero de confianza que testifique la misma, pero dotando al sistema de seguridad y trazabilidad.

Para comenzar, Nakamoto define a una moneda virtual o electrónica como una cadena de firmas. Hay que tener en cuenta que, en el concepto de Bitcoin, una criptomoneda no tiene

ningún respaldo físico ni documento que demuestre la tenencia, en este punto, entran en juego las transacciones. Un propietario transfiere x cantidad de Bitcoin a otro firmando un hash y colocando la clave pública del nuevo propietario y añade estos datos al final de la moneda. Aquí, Nakamoto plantea el primer problema que es el del doble gasto(Nakamoto, n.d.).

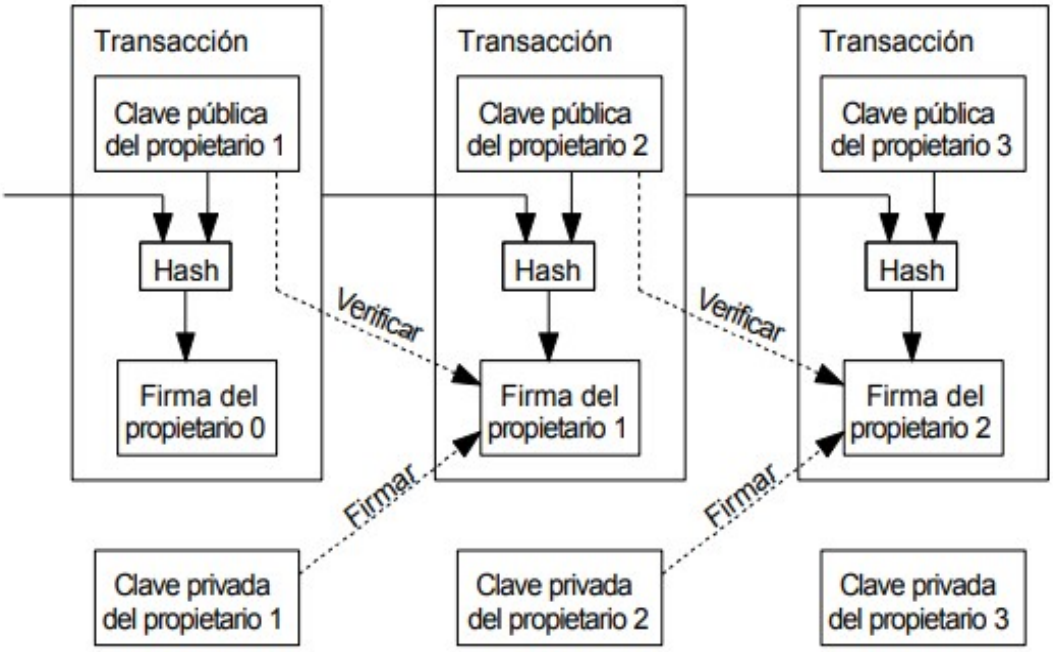

Imagen 2 - Esquema de doble gasto planteado por Nakamoto

El doble gasto se explica en que una persona o entidad pueda gastar dos veces la misma moneda, siendo esto un problema para el beneficiario, el cual no puede verificarlo inmediatamente. En la actualidad, en los sistemas electrónicos utilizados por los bancos y mismo en casi todas las transacciones comerciales, el doble gasto queda solventado con un tercero de confianza que controle y arbitre la transacción en sí. Nakamoto propone que la única manera de tener controlado el problema del doble gasto sea conocer todas las transacciones y, para lograr esto, las mismas tienen que ser anunciadas públicamente como también confirmadas como válidas por todos los miembros de la red. Si este proceso se cumple, el beneficiario puede asegurarse que esa transacción fue la primera en realizarle, ya que fue confirmada por la mayoría de los nodos.

Aquí nace el primer paso de la blockchain de Bitcoin el “servidor de sellado de tiempo”, Este trabaja tomando el hash de un bloque y sellándolo en el momento exacto en el que se genera el bloque para luego hacer público dicho hash; esto demuestra que dichos datos dentro del bloque existieron. El sellado del tiempo incluye el dato del hash anterior formando así una cadena, pero la naturaleza que Nakamoto quería insertar era la tecnología distribuida y sin terceros de confianza. Allí nace la “prueba de trabajo”.

Para lograr un sellado de tiempo distribuido en la red p2p, se requiere implementar una prueba de trabajo o “Proof of work”. Nakamoto se basa en el trabajo de Adam Back (Back, 2002); la prueba de trabajo propuesta consiste en buscar un valor de hash para que el bloque comience con “n” cantidad de cero bit, lo que genera una gran cantidad de procesamiento y tiempo, dependiendo de la cantidad de cero bit requeridos, pero puede verificarse rápidamente con un solo hash(Nakamoto, n.d.).

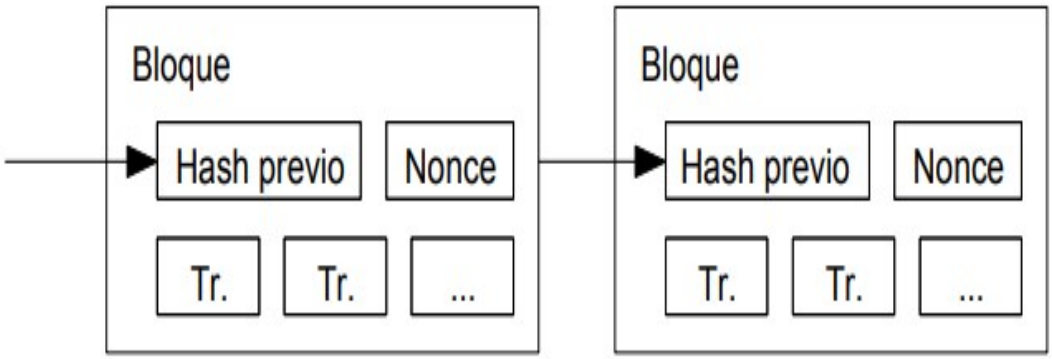

Imagen 3- PoW, Unión de bloques por Hash

En la prueba de trabajo mencionada, Nakamoto agrega un “nonce” (valor aleatorio), el cual se va a ir incrementando hasta lograr obtener el hash específico del bloque con la cantidad de ceros requeridos en el mismo. Una vez encontrado el hash que satisfaga los requerimientos, el bloque no se puede modificar en su contenido sin realizar nuevamente toda la prueba de trabajo y, con el avance de la cadena, se complejiza más la posibilidad de modificarlo, ya que se tendría que rehacer la prueba de trabajo de dicho bloque y todos los posteriores, puesto que, su hash obtenido mediante la prueba de trabajo queda encadenado al siguiente y este al siguiente, por lo que cualquier modificación en un bloque modificaría los datos de entrada del siguiente.

La dificultad de la prueba se modifica según la capacidad de cómputo disponible en la red y la velocidad de obtención.

Como se vio anteriormente, la fortaleza se sustenta en su trabajo distribuido y seguro, por lo cual, la prueba de trabajo es fundamental en el esquema. Esta requiere mucho tiempo y capacidad de cálculo, lo que conlleva también un gran gasto de energía. Por esto, Nakamoto define un sistema de incentivos para quienes logren encontrar el hash específico para cada bloque.

Dado que no hay una entidad que regule al Bitcoin, no hay nadie que los “genere”. Esto está en la naturaleza de la tecnología, sumado a que se necesita personas que se unan a la red para generar los hash de cada bloque. Se plantea que al momento de sellar un bloque se le asigne a quien obtiene el hash “n” cantidad de Bitcoin sumado a un cargo de “tarifa de transacción”, el cual se descuenta de los Bitcoin enviados desde un origen a un destino.

La manera descripta es la única forma de generar un Bitcoin. En su concepción, se estableció una generación total de 21 millones de Bitcoin, se estipula que será para el año 2140 cuando se alcance el total de Bitcoin posibles. Para que esto suceda, cada 210000 bloques generados, la recompensa por el minado (nombre puesto al trabajo de encontrar el hash del bloque con la dificultad planteada en ese momento) disminuye a la mitad. En el inicio de la cadena, la recompensa era de 50 Btc, al momento de la reacción de este trabajo, está en torno a los 6.25 Bitcoin por bloque sellado. El sistema de Bitcoin suma un cálculo de dificultad automático que establece que los bloques deben generar cada 10 minutos. Si los bloques se están sellando antes de ese tiempo, se incrementa la dificultad; si demoran más, se disminuye.

Dados ciertos problemas con el algoritmo PoW, se desarrolla el consenso por Prueba de Participación (PoS), este algoritmo fue planteado por **Sunny King en su Whitepaper** (King and Nadal, n.d.) en el año 2012. Sunny desarrolla esta técnica para solventar algunos problemas de PoW tales como **"la falta de escalabilidad y velocidad"**, el proceso de minería basado en PoW agrega mucho tiempo en la aprobación de nuevas transacciones y en la confirmación de un nuevo bloque;**"el alto consumo energético del proceso de minería"**, el minado por PoW demanda mucho poder de cómputo lo que se traduce en un gran gasto energético;**"la descentralización de la red"**, si bien el concepto de PoW es distribuido, el problema viene porque cada vez más grupos de mineros se juntan para concentrar más capacidad de cómputo.

Dicho esto, King propone que el consenso sedé por la tenencia de monedas, a mayor cantidad de monedas más posibilidad de que el proceso de selección aleatoria lo elija como candidato y así poder validar transacciones y crear nuevos bloques (esto va a derivar en recibir ganancias e incentivos por el trabajo realizado).

Algunas de las características más destacadas de PoS son:

- Tecnología que cuida el medioambiente al consumir muy poca energía y generar poco calor (no requiere grandes cantidades de HW como PoW).
- Permite una mejor alineación de objetivos e incentivos entre los integrantes de la red. De esta forma, cada uno de los que forman parte de la red buscan mantenerla por un largo periodo de tiempo.
- Descentralización y democratización de la red: todos pueden participar de la red mientras cumplan con su cuota de participación
- La entrega de recompensas es más proporcional. Esto gracias al sistema de selección aleatoria dentro de la red, el cual tiene como finalidad asignar tareas a aquellos que tienen tenencia de monedas. Quienes tienen mayor posesión, tienen mayor posibilidad de ser elegidos, de hacer verificaciones y de recibir ganancias con ello.
- Ofrece una mayor escalabilidad: al lograr una velocidad mucho mayor en la confirmación de transacciones y generación de nuevos bloques, la hace ideal para implementarse en la economía doméstica cotidiana, donde una

demora de diez minutos entre que se paga y se ve el impacto, puede ser catastrófico.

Siguiendo con el concepto de la Blockchain de Bitcoin, otros impedimentos a solucionar por la tecnología fueron el espacio en disco, la verificación rápida y simplificada de transacciones y el problema de “dar el vuelto”.

El espacio en disco no era un problema en principio, ya que el espacio utilizado por la cadena original era de 4.2MB por año.En la actualidad, el sistema de Bitcoin, para sumar un nodo, está en torno a los 70GB, por lo cual Nakamoto plantea la implementación de los árboles de Merkel en donde considera que si la última transacción ya fue sellada varios bloques atrás, las transacciones anteriores se pueden descartar para disminuir el espacio en disco, pero esto hay que realizarlo sin romper el hash del bloque, por lo que a las transacciones anteriores se les realiza un cálculo de hash y se insertan en un árbol de Merkel, incluyendo solo raíz en el hash del bloque para luego “podar” los bloques anteriores(Nakamoto, n.d.).

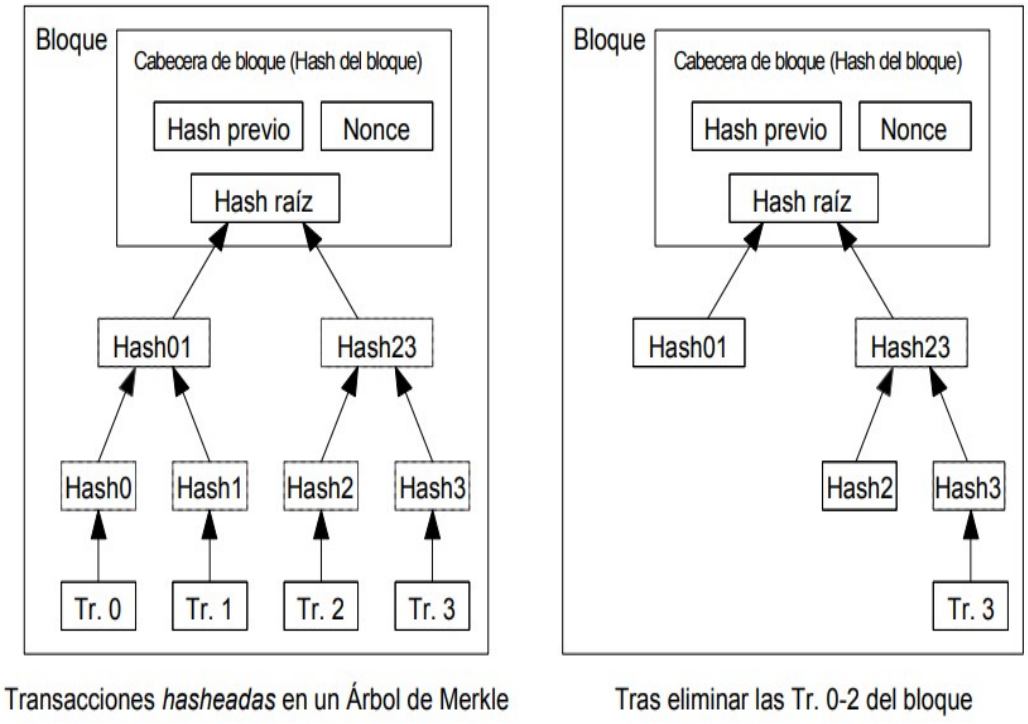

Imagen 4- Árbol de Merkel aplicado a la cadena

Sobre el inconveniente de verificar una transacción se supone, en principio, que para poder verificarlo, debería ser un nodo permanente con un copia actualizada de la cadena, pero esto no es necesario, el usuario solo debe solicitar a los nodos una copia de las cabeceras de los bloques y verificar donde está enlazada la transacción en sí. El usuario no puede comprobar la transacción por sí mismo, pero al poder ubicarla dentro de la cadena con su respectiva confirmación por un nodo y la continuidad de la misma en bloques subsiguientes, puede asumir que la red aceptó la transacción en cuestión.

Otro de los problemas es el de la devolución de valor, que se refiere a cómo se manejan las transacciones, en dónde hay una o varias entradas y una o dos salidas, aunque el sistema podría manejar monedas individualmente no sería eficaz hacer una transacción por cada fracción a transferir, por lo que se plantea enviar los enteros de las monedas, que sea igual o mayor al monto a transferir, y en todo caso que la transacción tenga una segunda salida, que sería la devolución de “n” monedas al remitente.

Como último, y habiendo visto todos los puntos principales de la tecnología que soporta al Bitcoin, se puede resumir los pasos de este proceso dentro de la red p2p como:

a) Las transacciones nuevas se transmiten a todos los nodos pertenecientes.
b) Cada nodo introduce las mismas en un bloque.
c) Se comienza, individualmente, a tratar de resolver la prueba de trabajo descripta anteriormente.
d) El nodo que logre resolver la PoW se la envía a todos los nodos de la red.
e) Los nodos verifican que las transacciones contenidas sean válidas y no sehaya gastado con anterioridad el saldo contenido.
f) Se empieza a trabajar en un nuevo bloque, dando por aceptado el bloque anterior, utilizando el hash del recién resulto.
g) Se validan todas las transacciones contenidas del bloque y el minero recibe su incentivo, tanto los Btc del minado como las comisiones por transferencia.

Puede darse el caso de que a un nodo le llegue un bloque con información distinta y luego el bloque correcto. El nodo va a trabajar en el primer bloque recibido, pero guardará el segundo bloque; luego, en la próxima PoW, se verificará el nodo de la cadena más larga y ahí se corregirá la desviación, sin llegar a un Fork que se explicará más adelante.

2.1.3 Usos de la tecnologia

En la actualidad, la tecnología de Cadena de Bloques soporta muchas aplicaciones de distintos usos, más allá de las criptomonedas, tales como Storj (“Decentralized Cloud Storage — Storj,” n.d.) para almacenar archivos; Proof of Existence (“Proof of Existence,” n.d.) para generar perpetuidad y trazabilidad a documentos; Healthchain (“Healthchain,” 2020) para unificar y mantener la historia clínica de los pacientes, (“Blockchain Voting,” n.d.)sistemas de votación soportado en la tecnología de blockchain, de trazabilidad de alimentos como (“Tecnología blockchain en el Sistema Informático de Trazabilidad Citrícola,” 2019) un sistema para la inversión en el sistema inmobiliario (Latifi et al., 2019) y muchos software más, basados en blockchain, que dan nuevas funcionalidades a la tecnología o que mejoran los usos actuales (Nyaletey et al., 2019).

2.1.4 Trazabilidad y seguridad

Cuando se habla de la seguridad de Blockchain, de la tecnología general, pero principalmente de las criptomonedas, se hace referencia, en primera instancia, a la prueba de trabajo.

La PoW, proceso por el cual se encuentra el hash específico del bloque, da al sistema complejidad y seguridad; a contrapartida, se genera un gran consumo de recursos computacionales.

Por otro lado, la generación de consenso, que se da en un voto por CPU, deja de lado que una persona mal intencionada pueda romper el sistema, por ejemplo, si fuera un voto por ip pública, un atacante con muchas direcciones ip públicas podría burlar esta dificultad.

Lógicamente, un grupo podría acaparar muchos recursos de cómputo y tratar de generar un “Fork” (bifurcación de la cadena), a esto se lo llama “problema del 51%”, ya que el grupo de atacantes tendría el 51% del poder de cómputo de toda la red, pero en la práctica, esto sería menos redituable que utilizar dicho poder en minar las criptomonedas y obtener de manera legal un beneficio.

Otro aspecto fundamental en la tecnología es que el bloque se conforma con el hash obtenido, mediante la PoW del bloque anterior, sumado a las transacciones lo que va a derivar en un hash de PoW nuevo de este bloque. Si alguien reemplaza un bloque, por ejemplo el bloque “B”, tendrá que rehacer todo los bloques subsiguientes, por lo que tendrá que generar la prueba de trabajo de cada bloque nuevamente. A mayor cantidad de tiempo que pase, más cantidad de bloques nuevos se generan, por lo que la probabilidad de lograr alterar la cadena se ve disminuida.

Todo lo mencionado genera la trazabilidad del sistema, ya que toda transacción queda registrada en la cadena y es prácticamente imposible modificarla.

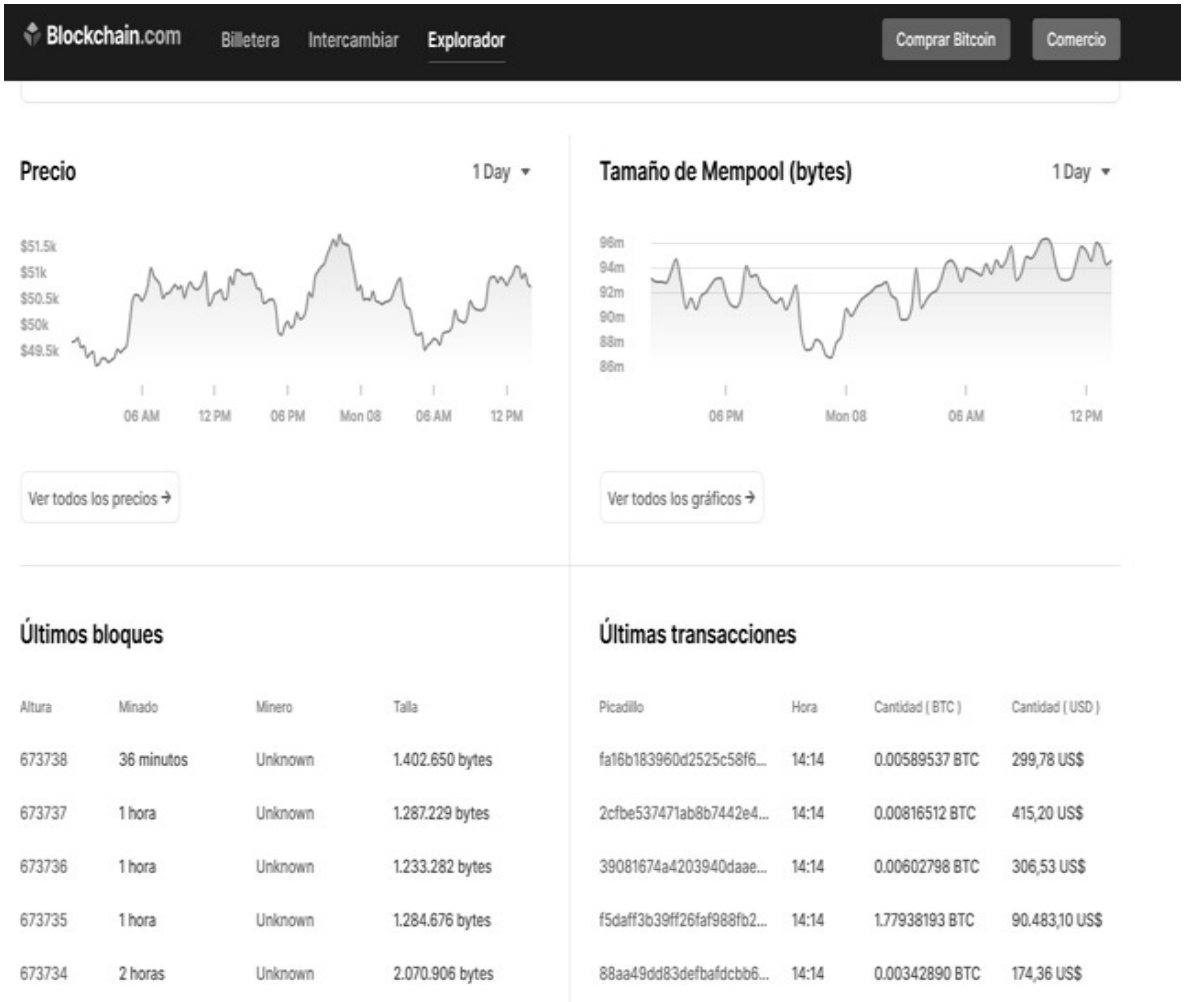

Imagen 5- Muestra de bloques y transacciones.

A su vez, el acceso a los datos es público por lo que cualquier persona que quiera corroborar una transacción, puede hacerlo de manera sencilla, ingresando a los recursos generados para este fin como por ejemplo:
https://www.blockchain.com/explorer?utm_campaign=dcomnav_explorer
donde se puede explorar varias de las blockchain principales y ver los bloques generados, con sus transacciones, sus comisiones, direcciones, etc (“Blockchain.com Explorer | BTC | ETH | BCH,” n.d.).

Bloque 726003

Hash	00000000000000000000051f03713fc049c5c0a93d1190f80eb316b1c18a377f30
Confirmaciones	5
Sello de tiempo	2022-03-05 08:09
Altura	726003
Minador	AntPool
Número de transacciones	2887
Complejidad	27.550.332.084.343,84
Raiz de merkle	ff44c973abdb176cdc7fbe6f4cc1ead8ac0d454774ac162cc4de5846dafef4a3
Versión	0x20000004
Bits	386.545.523
Peso	3.993.440 WU
Tamaño	1.559.009 bytes
Único	1.039.927.884
Volumen de transacciones	11628.95011168 BTC
Recompensa de bloque	6.25000000 BTC
Recompensa de tasa	0.10610288 BTC

Imagen 6- Muestra de un bloque

A continuación, se encuentra el ejemplo de las últimas transacciones del bloque y la generación de las nuevas monedas asignadas al minero que encontró el hash sumado a la recompensa de las transacciones(“Blockchain.com Explorer | BTC | ETH | BCH,” n.d.).

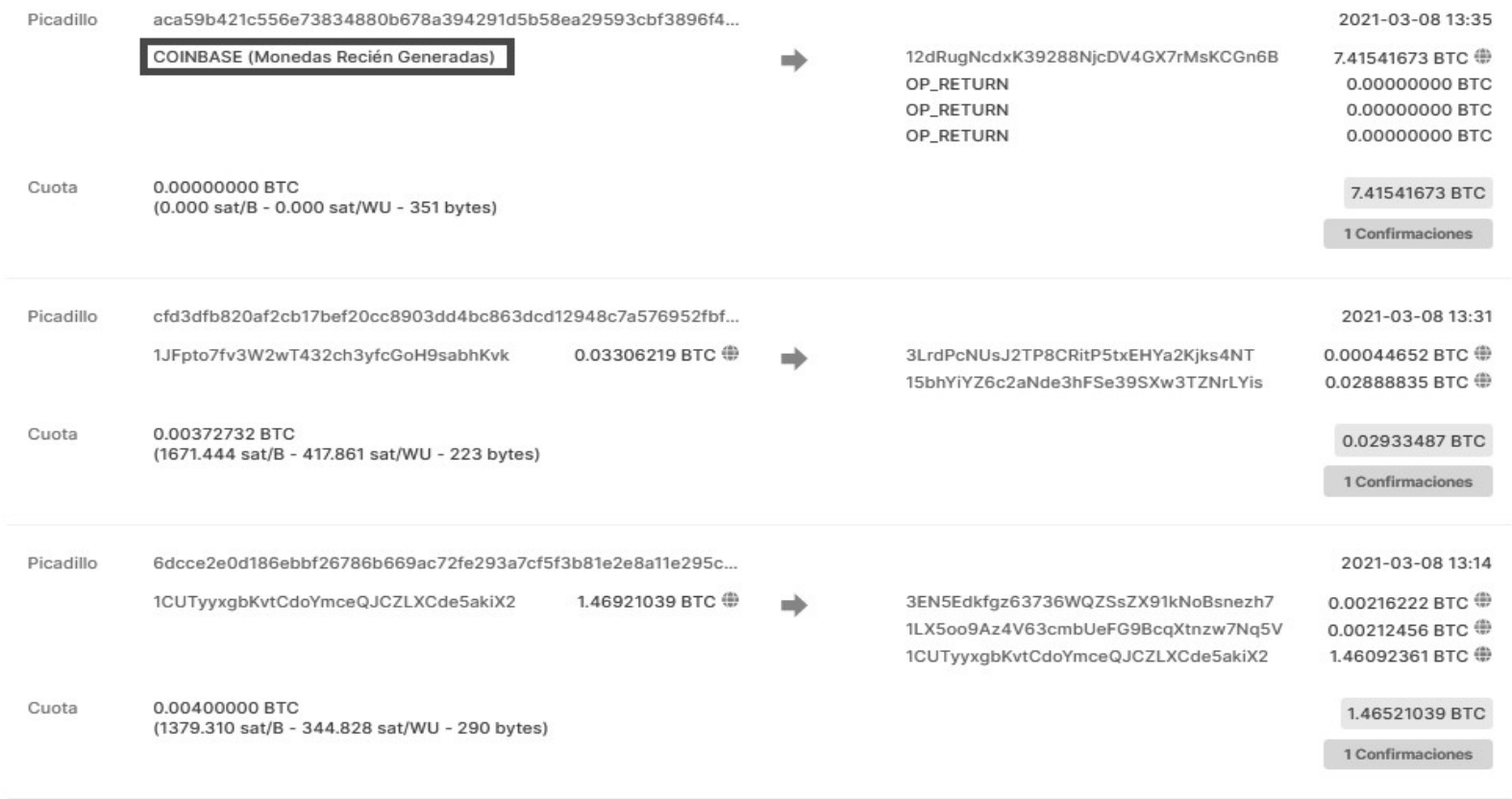

Imagen 7- Transacción Coinbase dentro de un bloque

Si bien la cadena está abierta para que cualquiera pueda ver su contenido, dirección origen, cantidad y dirección destino, la tecnología está diseñada para que no figuren más datos que los mencionados, por lo cual se mantiene un anonimato en las transacciones, en ningún momento se necesita saber ningún dato personal del emisor o receptor de la monedas virtuales o de cualquier bien o servicio transaccionado mediante esta tecnología.

Esto es una gran ventaja a nivel de privacidad con respecto a los sistemas tradicionales, ya que en los mismos se conocen el origen y el destino de la transacción como también la participación de un tercero de confianza para testificar.

2.2 Criptomonedas

En las siguientes secciones, se analizara qué son las criptomonedas (sección 2.2.1), su historia (sección 2.2.2) y sus usos en la actualidad, tanto a nivel mundial como puntualmente en la Argentina (sección 2.2.3).

2.2.1 Concepto

Previo a la definición de criptomonedas, se debe realizar una diferencia entre dinero digital, monedas virtuales y criptomonedas(Nieto, 2018).

Si bien se suele utilizar los términos de moneda virtual y criptomonedas como sinónimos, cada uno tiene significados diferentes.

Dinero digital hace referencia a las transacciones que se realizan sin el billete o moneda física, pero que están respaldadas por un banco y cuenta bancaria por detrás, ejemplo de esto es un pago con tarjeta de débito, de crédito o mismo una transferencia de una cuenta bancaria a otra(“Diferencias entre criptomoneda, moneda virtual y dinero digital,” n.d.).

Moneda Virtual: En el año 2012, el banco central europeo define a las monedas virtuales como "un tipo de dinero digital no regulado, el cual es emitido y generalmente controlado por sus desarrolladores; es usado y aceptado entre los miembros de una determinada comunidad virtual" (“Dinero virtual,” 2021); esto quiere decir que estas monedas virtuales no están respaldadas por ninguna entidad central, solo están generadas y respaldadas por los mismos desarrolladores. Lógicamente, este desarrollo puede ser de una empresa con gran renombre, pero fuera de ese entorno no tienen valor comercial, un ejemplo conocido de las monedas virtuales podría ser un videojuego en donde al conseguir superar desafíos, el mismo juego nos beneficie con una “moneda” propia y esta nos permita luego comprar accesorios para nuestro juego. Dicha moneda tiene valor dentro del mismo juego, pero ninguno por fuera de este.

Criptomonedas: son las más recientes, tienen varias similitudes con las monedas virtuales pero grandes diferencias; como su nombre lo indica están formadas a base de criptografía compleja lo que las hace mucho más seguras, por otro lado no están soportadas ni generadas por un desarrollador en particular sino que, como es el caso del Bitcoin y varias de las cripto derivadas de este, la validación y generación se da de manera distribuida y automática, por lo que nadie podría acaparar ni monopolizar la creación de las mismas (se podría acaparar la generación de criptomonedas, pero es técnicamente complicado por la gran cantidad de recursos computacionales necesarios).

Cuando se habla de Bitcoin y de la gran mayoría de las criptomonedas, hay que mencionar a las UTXO o **Unspent transaction output (transacción de salida no gastada);** en cada transacción de Bitcoin figuran estas entradas que son las transacciones de salida no

gastadas. Para poder realizar un envío de Btc, la billetera tiene que contener x cantidad de utxo que sumen más que el total a enviar, esas utxo se van a convertir en utxo de la dirección destino (Academy, 2020). Las utxo son parte fundamental de las criptomonedas de blockchain, ya que además de permitir la transferencia de saldos entre direcciones también evitan el doble gasto, ya mencionado anteriormente.

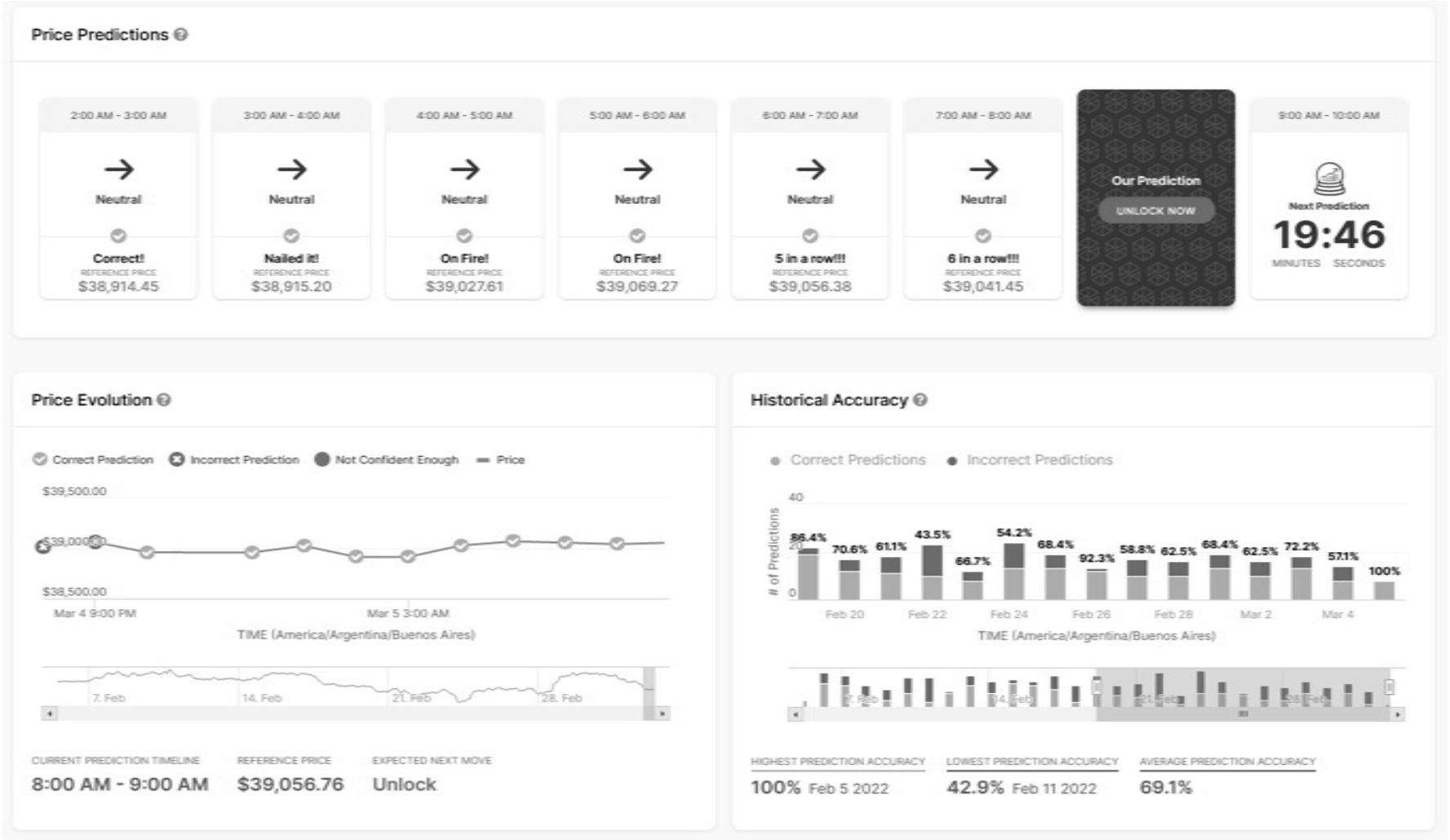

Imagen 8- Movimiento UTX

En la siguiente imagen vemos las predicciones para Bitcoin y Ethereum.

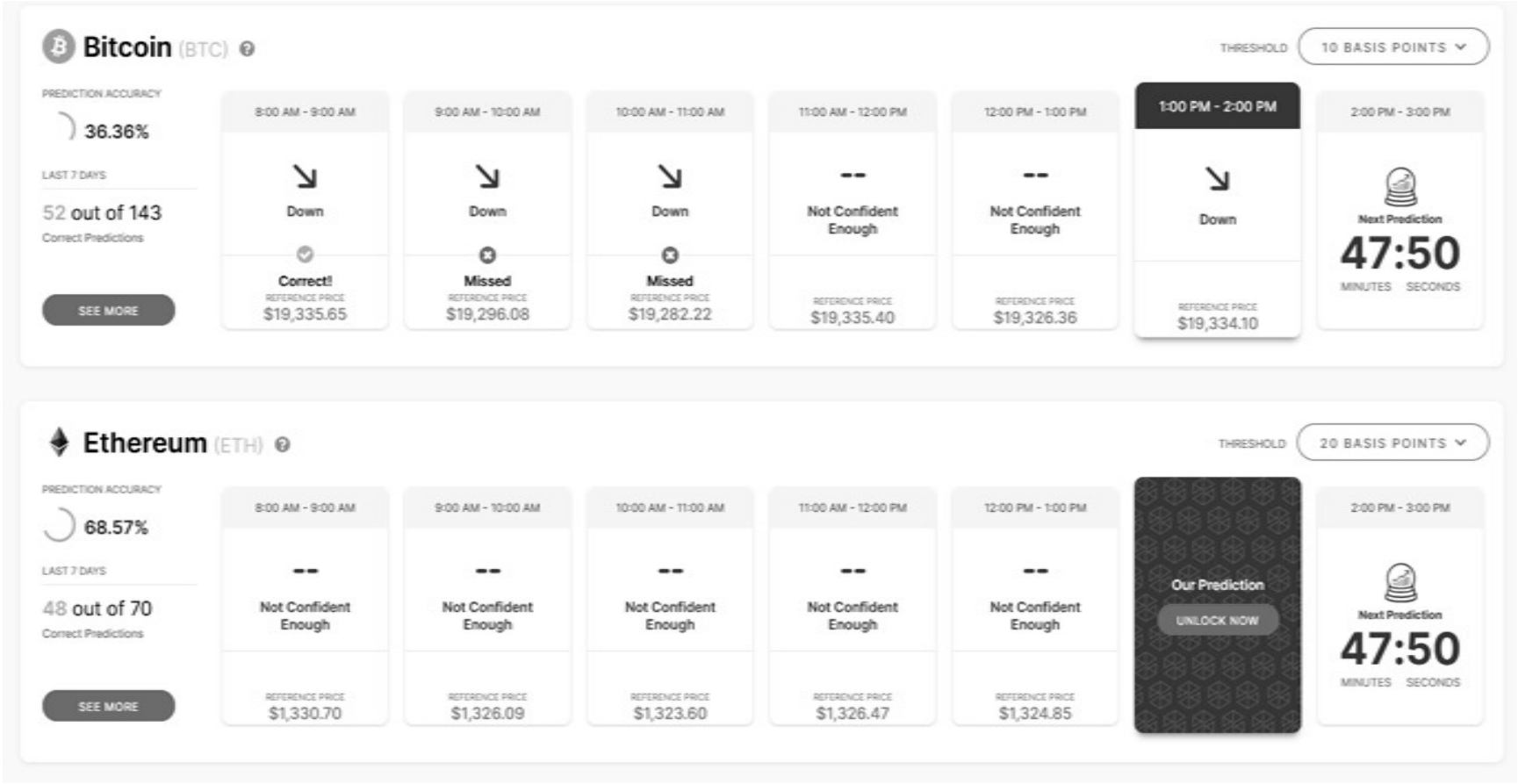

Imagen 9- Predicciones Bitcoin/Ethereum

En la siguiente imagen vemos las predicciones para Litecoin y Bitcoin Cash.

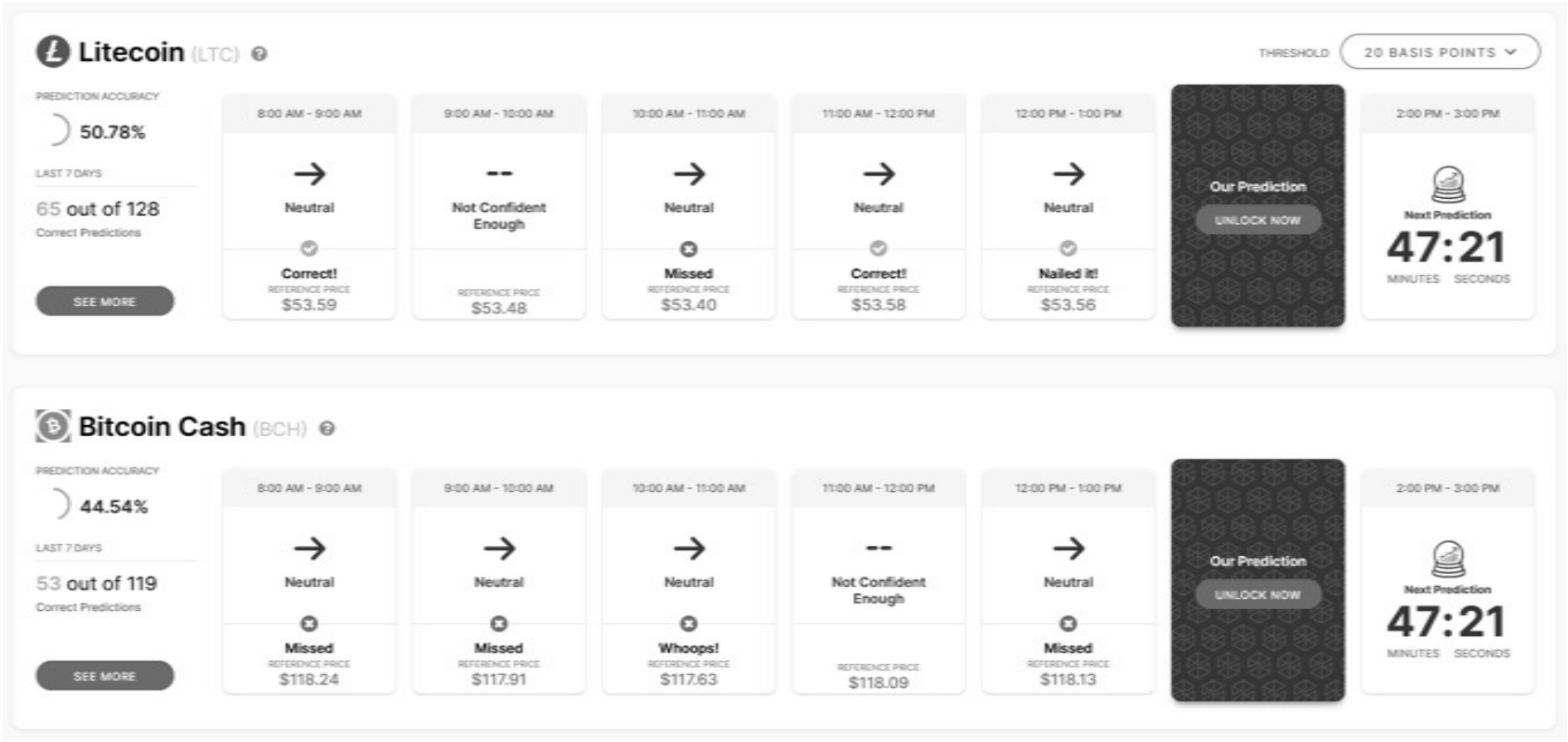

Imagen 10- Predicciones Litecoin/Bitcoin Cash

En la actualidad, hay muchas empresas que ponen foco en mirar los movimientos de las utxo para intentar realizar predicciones dejando de lado la visión de los montos en sí transferidos, ejemplo de esto es la web “intotheblock” (“Bitcoin (BTC) price predictions,” n.d.)(“El análisis de Utxo revela mucho sobre bitcoin, litecoin, dash y otros criptoactivos,” n.d.).

2.2.2 Historia

En el año 1983 el criptógrafo David Chaum presentó un paper donde describía un sistema de pagos electrónico basado en claves criptográficas para intercambiar dinero sin la necesidad de un tercero de confianza (Chaum, 1983).

En 1989/1990, Chaum funda DigiCash con la idea de poner en marcha el primer sistema de moneda virtual para el comercio electrónico basado en criptografía, la DigiCash o e-cash (se lo llamó de las dos maneras) fue la primera criptomoneda en concepto; en el año 1998 DigiCash fue a la quiebra, según su creador la caída fue dada porque no era el momento para las criptomonedas.

Durante el periodo de DigiCash, Adam Back propuso la PoW (Back, 2002) que va a ser fundamental en el concepto de Nakamoto sobre Bitcoin.

En 1998, Nick Szabo presentó un trabajo donde hablaba de Bit Gold, la primera criptomoneda en concepto muy parecida a Bitcoin, pero que no llegó a ser implementada. Una de las grandes diferencias de Bitcoin con la propuesta de Szabo es que Bitcoin logra solucionar el problema del doble gasto.

En octubre del 2008, Satoshi Nakamoto presenta su paper “Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer” y en enero del 2009, fue minado el primer bloque de la blockchain de Bitcoin, el “Bloque Génesis”.

El primer defensor y futuro colaborar en el proyecto fue el Ingeniero informático Hal Finney; al leer el proyecto de Satoshi Hal se intereso mucho y comenzó a plantear cambios sobre la tecnología los cuales fueron bien vistos por Satoshi (“¿Quién es Hal Finney?,” n.d.).

Las evidencias muestran que Hal fue la primera persona en descargar y ejecutar el cliente de Bitcoin luego de su creador.

La primera transacción fue el 12 de enero del 2009 donde Satoshi le envía a Hal Finney 10 Bitcoin mostrando que el sistema funcionaba y abriendo una nueva era de la economía alternativa.

Bitcoin fue la cripto pionera y desde allí, comenzaron a aparecer muchas derivadas de esta.

La primera transacción comercial con Bitcoin como forma de pago se dio el 22 de mayo del 2010. Laszlo Hanyecz, entusiasta del Bitcoin, propuso en un foro de Bitcoin que le pagaría 10000 Btc a quien le llevara 2 pizzas a su domicilio, en su publicación aclaro que no le importaba si las mismas eran de un local o realizadas por la propia persona pero su idea era que alguien le diera 2 pizzas a cambio de los Bitcoin.

Esta transacción tardo 4 días en efectuarse, esto sucedió cuando Jeremy Sturdivant se comunico con Laszlo y le llevo las pizzas pedidas, las pizzas fueron del local Papa John´s aunque fue Jeremy quien hizo de intermediario en la transacción (“Bitcoin Pizza Day,” n.d.).

2.2.3 Usos

La primera transacción comercial con Btc fue la compra de dos pizzas, el 22 de mayo del 2010. El intercambio fueron 2 pizzas por 10000 Btc, que en ese momento sumaban unos 41 dólares. La realidad es que no fue una compra directa al comercio Papa John´s sino que, fue Lazlo Hanyec, uno de los programadores que colaboró con el proyecto Bitcoin,quien ofreció en un foro, en el cual participaba, que alguien le llevara dos pizzas por el pago de 10000 Btc.Lazlo quería impulsar el uso de las criptomonedas para el pago del delivery de comida.

Al día de la fecha, los Btc se pueden utilizar prácticamente para todo tipo de intercambio, siempre que el comercio acepte el pago con esta criptomoneda. Muchas tiendas a nivel mundial están aceptando el valor de esta moneda. En la actualidad, se pueden pagar entradas de teatro, comida, distintos servicios, dispositivos electrónicos, videojuegos, etc.(Academy, 2016). Lamentablemente, también se utilizan mucho las criptomonedas para realizar transacciones ilegales, dada su naturaleza parcialmente anónimas. Las mismas pueden usarse para la venta de drogas, armas, base de datos robados, etc.

En la Argentina, el pago con Bitcoin tuvo un auge muy grande por el año 2018.Como caso resonante se encuentra el de la ciudad de Pinamar en donde un balneario comenzó en ese año a aceptar Bitcoin como pago por sus servicios (Galinsky, 2018).

A nivel mundial, el último en anunciar que aceptará pagos en Bitcoin fue la automotriz Tesla, que en las primeras dos semanas de febrero del 2021compró el equivalente a 1500 millones de dólares en Btc. Solo el anuncio de este movimiento hizo que el precio del bitcoin tenga un fuerte aumento(“¿Cuán arriesgado es comprar un Tesla usando bitcoin?,” 2021).

Imagen 11- Propiedades publicadas en Btc.

A fines de abril del 2021, Mercadolibre anunció que aceptará la venta de inmuebles mediante Bitcoin (solo con esta criptomoneda) (“Mercado Libre Argentina incorpora sección para compraventa de inmuebles con bitcoin,” 2021).

2.3 Billeteras Virtuales

En la sección 2.3.1, se explicará el concepto de las billeteras virtuales y sus tipos, entre los cuales se encuentran las Hardwallet (billeteras por hardware), Softwallet (billeteras por software) y PaperWallet (billeteras papel), como así también una segunda clasificación donde se pueden considerar como HotWallet (billeteras calientes o conectadas) y ColdWallet (billeteras frías o desconectadas).

2.3.1 Concepto

Cuando se habla de Wallet o billeteras virtuales, se hace referencia a donde se guardan las criptomonedas (es como la billetera para guardar billetes pero en este caso para las criptomonedas). No todas las billeteras aceptan todas la cripto que existen, por lo que hay que buscar un monedero que permita operar con las cripto que se quieren comprar y vender.

Las wallet son un aspecto fundamental para las transacciones, sin ellas no se podría comprar ni vender ninguna criptomoneda.

Técnicamente, es un software o hardware que permite almacenar las transacciones de entrada y salida junto con un par de claves criptográficas, dicho de otra manera, es el instrumento que permite interactuar con la blockchain.

Hay varios tipos definidos, cada uno va a depender de la necesidad del usuario, la experiencia que busca obtener y la seguridad relativa que espera.

Para hacer una definición sencilla sobre las mismas, hay que mencionar tres tipos: las wallet por software, por hardware o las billeteras papel.

También se pueden clasificar como billeteras calientes o frías.

El primer caso a mencionar, ya que es uno de los más utilizados, son las software wallet. Pueden estar instaladas en un dispositivo del usuario (Pc, celular, etc.) o en un Exchange. Este último caso es uno de los más peligrosos, ya que se le confía a un tercero las claves públicas y privadas, por lo que pueden utilizar las criptomonedas o se puede ver comprometida la seguridad del Exchange y de esta manera, se pierden todos los ahorros, un caso muy resonante fue el deMt.Gox(“Mt. Gox,” 2019).

El segundo subtipo es el del software que se instala en los dispositivos del usuario. Este es más seguro que tenerlo dentro de un Exchange, siempre y cuando se tomen medidas de seguridad (pc libre de virus, malware y troyanos, copias de seguridad periódicas, encriptación de la billetera por una clave extra, etc). Hay que tener en cuenta que las criptomonedas son propiedad del usuario solo porque tiene acceso a su billetera, si pierde el acceso a la misma, por ejemplo se rompe el dispositivo y no tiene respaldo de las claves o una copia de la computadora, dichas monedas quedarían en una nebulosa y serían imposibles de recuperar sin las claves criptográficas propias de la dirección. A octubre del 2020,se estimaba

que había un 25% de Bitcoin perdidos (“Detectan cuántos bitcoins se pierden por día y los motivos de la desaparición,” n.d.).

Tanto el caso del Exchange como el del software se pueden considerar como billeteras calientes. La definición de caliente o fría está dada por si la billetera está conectada a internet continuamente o no. Lógicamente, cuan más conectada esté más susceptible es a ataques cibernéticos.

Las ColdWallet son las billeteras por hardware, dispositivos físicos que utilizan un sistema de generación aleatoria de números para la obtención de las claves públicas y privadas. A su vez, las mismas quedan guardadas en el dispositivo físico que está desconectado de internet, por lo que son considerados de los más seguros. Se recomienda este tipo de billeteras si la idea es guardar las criptomonedas a largo plazo.

El ultimo tipo mencionado son las billeteras papel, en sí no son ningún tipo de hardware ni software, básicamente es la impresión de las claves públicas y privadas en un papel. Es uno de los dispositivos más difíciles de hackear, ya que no tienen ningún tipo de conexión a internet ni software que se pueda vulnerar, pero es engorroso manipular su saldo de forma parcial por lo cual es el menos recomendado para las transacciones diarias(“Guía sobre Tipos de Criptomonederos,” n.d.).

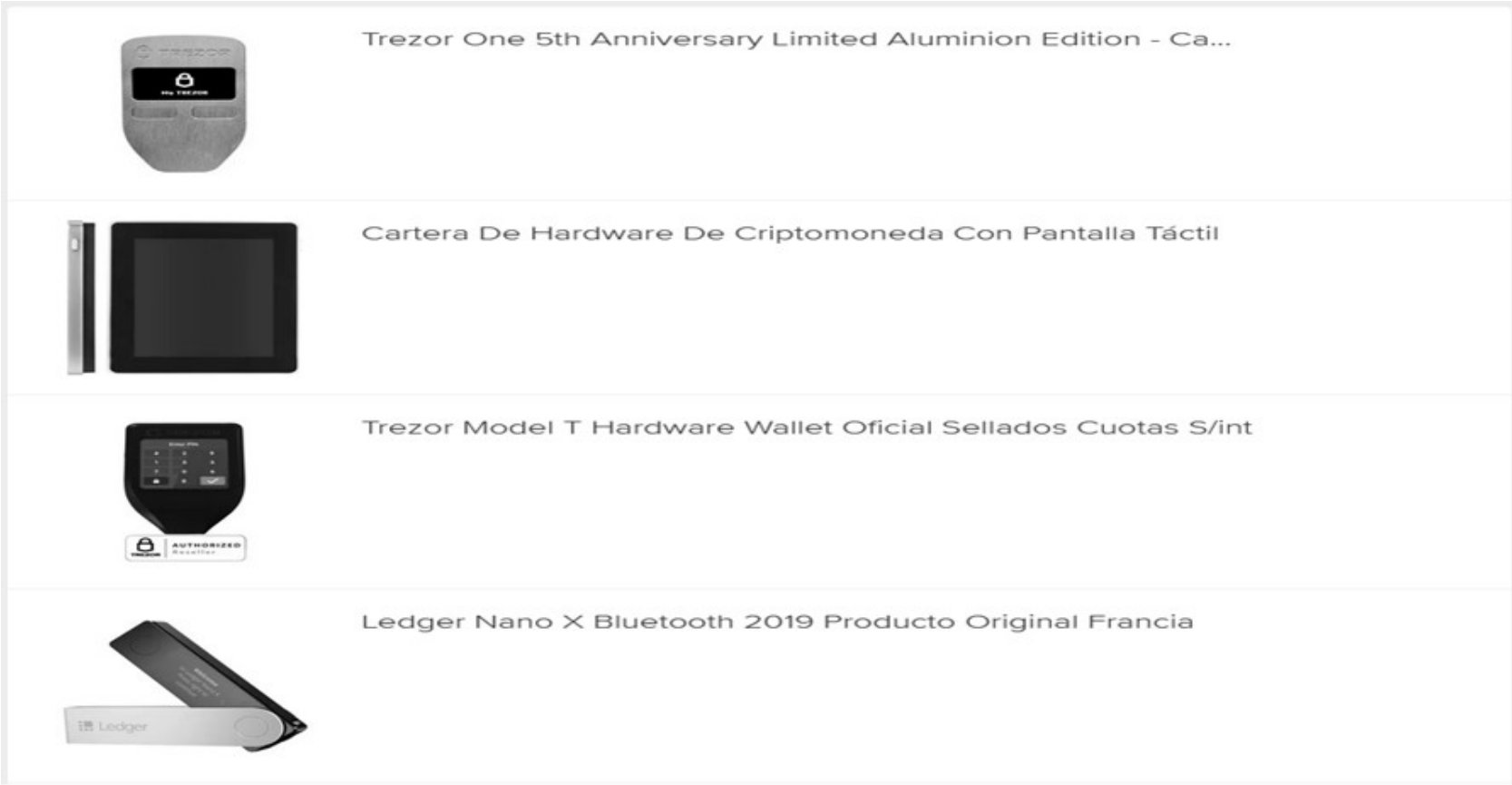

Imagen 12- Billeteras hardware vendidas en Argentina.

En la imagen anterior, podemos ver algunas de las HardWallet que se consiguen en Argentina(“Billeteras para Criptomonedas | MercadoLibre.com.ar,” n.d.).

2.4 Delitos

Cuando de delitos se trata hay que hacer foco en los relacionados con las criptomonedas, ya sea donde el fin es el robo de las mismas o son parte de lo perpetuado. Los principales casos conocidos son el robo de criptomonedas (sección 2.4.1), el robo o secuestro de información que lleva a un rescate pagado por criptomonedas (sección 2.4.2), la Sextorsion (sección 2.4.3), las transacciones ilegales (venta de armas, drogas, servicios ilegales, etc) (sección 2.4.4) y otros, como el cyberterrorismo (“Corea del Norte robó 300 millones de dólares en criptomonedas para financiarse,” n.d.).

2.4.1 Robo de criptomonedas

El robo de criptomonedas es algo que sucede cada vez con más frecuencia. Como se menciona anteriormente, la tecnología que soporta a las cripto, blockchain, es casi imposible de vulnerar por lo que el robo en sí se suele lograr atacando a las billeteras privadas de los usuarios(sección 2.4.1.1) o a los Exchange (sección 2.4.1.2).

2.4.1.1 Billeteras privadas

Dentro de este punto hay varios delitos o fraudes que se realizan en la actualidad.

Hay muchas maneras en las cuales el delincuente se queda con los Bitcoin de otra persona. Una muy eficaz es la de obtener la clave pública y privada del dueño de la billetera. Hay varios casos conocidos en donde esto sucede, siendo el principal blanco de ataque las billeteras del tipo caliente instaladas en un dispositivo.

Uno es el de Monty Munford que compró en el 2017 Ether, los cuales dejaron de estar disponibles con el paso del tiempo. Al investigar sobre el hecho, descubrieron que los atacantes habían accedido a su billetera, ya que él tenía guardada su clave privada en su propia casilla de Gmail (“Cómo me robaron US$30.000 en criptomonedas,” n.d.)

Otra forma muy común de robo, es infectar el dispositivo con un malware o un keyloger para encontrar información relevante de la billetera o capturar las pulsaciones del teclado.

Hay muchos casos de robo de billeteras entre personas conocidas, es muy frecuente en casos de divorcios conflictivos en donde una de las partes involucradas se transfiere los saldos de la billetera del otro y, como en principio, no hay un tercero de confianza que garantice la propiedad, cuesta mucho que la justicia actúe.

Otro caso muy común indirectamente a las billeteras privadas son los fraudes, si bien no se pierde acceso a la misma, el atacante engaña al poseedor para que este le transfiera parte de sus criptomonedas. Al ser una red P2P, sin intermediarios, cuando alguien por ejemplo

quiere comprar Bitcoin por fuera de un Exchange queda a la suerte de que la persona que le tiene que transferir los mismos lo haga efectivamente. Actualmente, en Argentina sucede mucho en los grupos de Facebook o foros similares donde personas ofrecen “vender” Bitcoin u otras criptomonedas sin las comisiones de ningún Exchange y terminan estafando a las personas, ya que nunca transfieren las monedas o en el caso inverso, el dinero.

En los últimos años, se han visto casos de robo a mano armada a personas con la excusa de comprar o vender criptomonedas. Hay casos reportados y de público conocimiento en Dubái, New York, Moscú, etc. (*Detienen a una pandilla en Dubái por robar $2 millones a compradores de bitcoin*, 2018; *Robo a mano armada de $1,8 millones en ethers es denunciado en Nueva York*, 2017).

A nivel nacional, hay un posible caso de estafa en curso, es sobre un sitio llamado “Ganancias Deportivas” donde el servicio ofrece ganancia de entre 20% al 240%. Toda la plata que ingresa el afiliado se convierte a Bitcoin. El servicio propone la entrega de ganancias mensuales a sus afiliados, las mismas se originan supuestamente al llevar la plata a las apuestas deportivas, pero se está investigando si no es una estafa piramidal donde los nuevos les pagan la ganancia a los miembros más viejos. (“Argentina investiga a la red ‘Ganancias Deportivas’ por presunta estafa con bitcoin,” 2021).

2.4.1.2 Exchange

Un Exchange funciona de manera similar al Exchange de dinero físico. Son plataformas para el comercio pero entre criptomonedas. Estas páginas no están dedicadas solamente a la venta y compra sino que ofrecen variados servicios desde billeteras virtuales hasta sistemas de inversión, estadísticas y predicciones.

Como se expuso al principio del punto 2, unas de las formas más comunes en donde se vulneran las billeteras de los propietarios y se pierden millones de dólares en criptomonedas son con los Exchange; es más fácil para un delincuente, o mejor dicho, tiene más posibilidades de encontrar una vulnerabilidad en el sistema que usan o en alguna de las personas que participa de la compañía que lograr obtener las credenciales de una sola persona. Lógicamente, el monto que pueden robar es mucho más grande en un Exchange que de una sola persona.

Hay muchos casos conocidos de robo a los Exchange, dentro de los más conocidos tenemos el caso de Mt. Gox que sufrió en dos oportunidades el robo de criptomonedas (“Mt. Gox,” 2019), el robo a Bitfinex(“Roban más de 65 millones de dólares en bitcoin a BitFinex,” 2016), BitFloor que se vio afectado en el 2012 por el robo de 24000 Btc, luego de esto nunca pudo recuperarse la empresa (Academy, 2018), y muchos otros casos de robos perpetuados a distintos exchanges.

2.4.2 Robo de información

Cuando se habla de robo de información, se hace referencia a un secuestro de información a cambio de dinero. Esto sucedió desde siempre, pero con la llegada de la tecnología y de las criptomonedas este tipo de delito tuvo un crecimiento exponencial.

Hay que tener en cuenta que, en la actualidad, el 99% de la información con la que trabajan las empresas, los gobiernos y todo tipo de organización está digitalizada, esto trae enormes beneficios como el orden, la velocidad de acceso e incluso la posibilidad de analizar y actuar preventivamente. Esta ventaja de la digitalización conlleva el gran problema de que cada vez se está más expuesto tanto a nivel organizacional como personal. En los últimos cinco años, se vieron muchos ataques a nivel mundial donde los delincuentes secuestraban la información (se encriptaban los directorios de trabajo específicos) y se solicitaba un rescate para obtener la clave y lograr desencriptar los archivos. El caso más resonante de la última década fue el ataque de WannaCry perpetrado en el año 2017 donde se vieron afectadas cerca de 230 mil computadoras en 150 países distintos. Los más perjudicados fueron Rusia, Ucrania, India, Gran Bretaña, donde se vio comprometido el servicio nacional de salud; España, por el ataque a Telefónica, y Alemania, donde la empresa ferroviaria alemana Deutsche Bahn AG fue el principal blanco.

Los atacantes lograron recaudar 140000 dólares en Bitcoin. Si bien parece un número elevado, es ridículamente bajo para un ataque de tal magnitud, esto se debe a que nunca se recomienda pagar cuando sucede esto, ya que nadie puede asegurar que los delincuentes entreguen las claves de cifrado y por otro lado, si se abona el rescate, se está promoviendo este tipo de actividades (“Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia,” n.d.)

Otro caso resonante fue el ataque a la lotería nacional de México. Si bien la ente estatal desmintió la notica el grupo que perpetuo el ataque mostro documentos internos de la empresa y exigió un pago en criptomonedas cercano a los 5 millones de dólares para liberar la información (Clarín.com, 2021a).

Siguiendo con México el grupo Anonymous ataco la petrolera Pemex pidiendo un rescate cercano a los 4,9 millones, luego en Julio del 2020 llevaron a cabo un ataque contra los servicios de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros pero este ultimo sin solicitar recate, fue en protesta por no atender las quejas de las victimas de estafas de los bancos (Clarín.com, 2021a).

2.4.3 Sextorsión

La Sextorsión, o extorsión sexual, consiste en la amenaza de revelar información íntima sobre una víctima a no ser que esta pague al delincuente. Este tipo de amenaza existe desde hace muchísimos años, pero con las tecnologías actuales se profundizó.

Abordando el tema, la Sextorsion viene dada cuando un atacante logra obtener información privada de la víctima y luego pide un rescate en criptomonedas para “borrar” esa información. Es cierto que hay varios casos que son reales, donde el delincuente efectivamente logra comprometer una red social, el teléfono celular o por ejemplo la casilla de mail de la víctima y a cambio pidió un pago en Btc por ejemplo, pero en la mayoría , los atacantes salen a “pescar” distraídos haciéndoles creer que obtuvieron acceso, lo cual no es cierto. En los últimos dos años, circuló fuertemente una campaña de Spam donde se enviaban millones de mail diarios; los mismos parecían salir de la cuenta de correo de la víctima y, para darle credibilidad, solían poner una contraseña real utilizada por la persona. En estos mails, los delincuentes mencionaban que tenían fotos o videos comprometedores y que si no se abonaba un rescate, este material iba a ser enviado a todos sus contactos.

Este caso mencionado es un mezcla de técnicas, por un lado el phising (suplantación de identidad) al utilizar supuestamente la misma cuenta de la persona, lo que daba la sensación de que tenían acceso a esta, por otro, la utilización de datos filtrados en hackeos anteriores como contraseñas reales de las víctimas(“La web que te dice si te robaron las contraseñas de Dropbox, LinkedIn, MySpace y otras cuentas (y cómo protegerte),” n.d.),(País, 2013) etc.

Un ejemplo de los mencionados mails de Sextorsión que se hicieron masivos se ven en las siguientes imágenes (“‘Sextorsión’, la nueva estafa por mail que revela tu contraseña y fotos privadas - Infotechnology.com,” n.d.)**:**

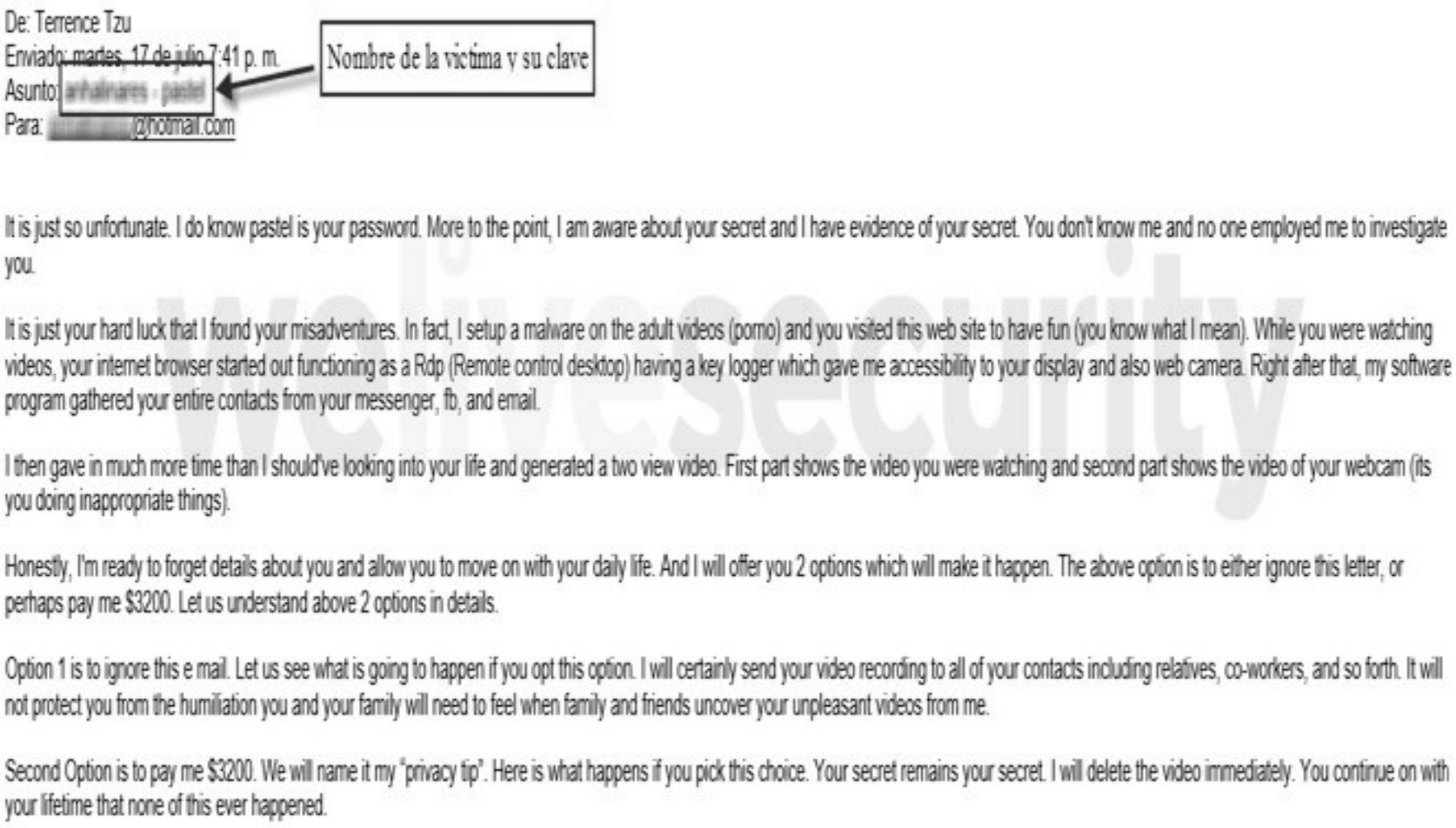

Imagen 13- Email ejemplo de un ataque de phising de Sextorsion.

En la siguiente imagen podremos ver otro ejemplo de mail(“Nueva ola de correos spam incluyen contraseñas de usuarios en el asunto,” 2020).

From: Rebekah Mckinney <kmsamuelay@outlook.com>
Sent: Friday, April 10, 2020 9:26:56 AM
To: [redacted]
Subject: [redacted] camif[redacted]

Your password is camif[redacted] I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which proided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. The first part recorded the video you were viewing (you'e got an exceptional taste haha), and the next part recorded your webcam (Yep! t's you \doing nasty things!).

What should you do?

Well, I believe, $4900 is a fair price for our little secret. You'll make the payment via bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

bitcoin Address:

bc1qls8wknrwhvxlf36m[redacted]cdekscjlpfry
(It is cAsE sensitive, so copy and paste it)

Important:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth.Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Rebekah Mckinney

welivesecurity

Imagen 14- Email ejemplo de un ataque de phising de Sextorsion.

En Argentina se está dando una modalidad de Sextorsion en donde los delincuentes captan a sus víctimas en aplicaciones de citas haciéndose pasar por otras personas, entablan una relación virtual logrando engañarlos para tener charlas sexuales e incluso que les envíen fotografías.

Luego de que la victima caiga en la trampa comienzan a recibir llamadas, supuestamente de la policía o de agencias de seguridad, alertándolos de que dichas conversaciones fueron con un menor de edad y tratando de "ayudarlos" a que no llegue la causa a la justicia a cambio de una suma de dinero (Clarín.com, 2021b).

Si bien los casos más conocidos en argentina siguen utilizando transferencias electrónicas de dinero convencional es una caso testigo de lo que se puede hacer mediante una criptomonedas minimizando el riesgo para los delincuentes.

2.4.4 Ventas ilegales

Un gran problema para las fuerzas de seguridad, y al contrario, un gran beneficio para la comunidad delictiva, es la creación de las criptomonedas. Claramente, cuando se adquiere un bien ilícito el mismo no se debe abonar mediante una trasferencia electrónica común, ya que esto deja rastros de la transacción como de las personas tratantes. La anonimidad, característica principal de las criptomonedas, es fundamental para este tipo de comercio, ya que si se efectúa correctamente la transacción, no queda registro de la misma ni de los participantes.

La web está constituida por 2 grandes grupos, la web abierta (5% del total) y la deep Web o web profunda (95%); dentro de la deep web se encuentra la "DARK WEB" (0.1% del total).

Muchos de las ventas ilegales se llevan a cabo en la "DARK WEB", la dark web es un conjunto de páginas y sitios alojados en internet los cuales no están indexados y pueden ser accedidos mediante un navegador especial como por Ejemplo TOR. ("¿Qué es la Deep Web y la Dark Web?," 2021).

En esta parte de la web se puede comerciar armas, drogas, datos de personas y muchas cosas más que no se podrían ofrecer en la web abierta (BBVA, 2019).

Un caso muy conocido y que tuvo a las fuerzas de seguridad de Estados Unidos en alerta, fue el de la ruta de la seda (pauta, n.d.). Skill Road fue una web creada, supuestamente, por Ross Ulbricht; operó abiertamente entre el año 2011 y 2013. En la web, se podían comprar drogas de todo tipo y eran abonadas con Btc.

Hay muchos casos más de ventas ilegales donde las criptomonedas son protagonistas, dada su privacidad tanto para el comprador como para el vendedor

2.5 Marco de trabajo para el análisis forense

En las siguientes secciones, se explica el concepto de un marco de trabajo (sección 2.5.1) y se mencionan los marcos asociados a los delitos cibernéticos que existen y se utilizan actualmente para la investigación forense (sección 2.5.2).

2.5.1 Concepto

Un marco de trabajo es una guía de referencia, un conjunto estandarizado de conceptos, prácticas y criterios para enfocar al ejecutante hacia un horizonte.

Este concepto es general y aplica desde un Frameworks para desarrollo de software hasta el marco para aplicar y/o revisar la calidad de un producto o proceso.

2.5.2 Marco asociado a los cyberdelitos

Cuando de tecnología se trata, y sobre todo de análisis forense, hay que poner en foco el estándar desarrollado porla ISO (“ISO/IEC 27037:2012(en), Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence,” n.d.); este vino a actualizar lasdirectrices definidas en guía “RFC 3227” (“Directrices RFC 3227,” 2020) .

La ISO/IEC 27037:2012 está orientada a distintos tipos de dispositivos tales como dispositivos de almacenamiento (discos rígidos y demás medios de almacenamiento), dispositivos móviles (celulares, PDA, etc.), sistemas de GPS, cámaras de fotos y de video (incluyendo sistemas de video vigilancia), computadoras en red, redes basadas en TCP/IP y dispositivos con funcionalidades similares a los mencionados.

La normativa identifica cuatro etapas generales, las cuales son identificación, recolección, conservación y análisis (esta última, si bien está identificada, no se profundiza).

La identificación se entiende por el proceso de identificar y localizar la evidencia en sus dos principales estados, físico y lógico. Esto va a depender del caso a investigar.

La recolección se define como la recogida de todos los dispositivos y los documentos indispensables para el análisis forense que se va a realizar.

La conservación hace referencia a cómo hay que tratar a las pruebas recolectadas para que las mismas sean admisibles como prueba original e íntegra, por lo que se puede decir que esta etapa está directamente relacionada con la cadena de custodia, la integridad y la originalidad de las pruebas hacia un posible juicio.

Este estándar fue presentado en el 2012 y confirmado como estándar en julio del 2018.

Muchos modelos se desprenden de este o mismo del RFC 3227.

Un modelo que se utiliza para la realización de análisis forense en la actualidad es el “EDRM”(“EDRM Model | EDRM,” 2020), el cual cuenta con ocho etapas (identificación, preservación, recolección, procesamiento, revisión, análisis, producción y presentación). Este tipo de modelo trata de ser más abarcativo e integrador, pudiendo ser aplicado a muchos aspectos de las TIC desde un simple disco rígido o computadora de escritorio hasta sistemas en red e incluso podría ser aplicado en cierto punto a sistemas cloud.

3.Conclusiones

En este capítulo se elabora un resumen del trabajo de investigación realizado (sección 3.1) y se exponen las futuras líneas de investigación (sección 3.2)

3.1 Resumen del trabajo de investigación

En el presente trabajo de investigación, se realizó un análisis de la tecnología Blockchain, demostrando sus virtudes y sus fortalezas. Se vio que más allá de las criptomonedas también es posible utilizarla en otros sectores y su función puede ser fundamental en la evolución de tecnología actuales como en el desarrollo de nuevos mercados, en sistemas de votación, trazabilidad de alimentos o medicamentos, etc..

Por otro lado, se hizo foco en las criptomonedas, su funcionamiento y su uso en la actualidad, así como también los riesgos inherentes que, si bien no vienen dados por la tecnología, existen y cada vez se explotan con mayor recurrencia.

Resumen de investigación	
Tecnología	Blockchain: Las transacciones se envían a todos los nodos validadores, estos las incorporan en un bloque, cuando el mismo está completo se hace un cálculo de hash para cerrarlo, el nodo que sella el bloque envía el mismo a toda la red: la red valida el cálculo y se sigue con otro bloque.
Algoritmos	Los dos principales y más utilizados son: PoW (prueba de trabajo) y PoS (prueba de participación); existen otros derivados principalmente de estos 2pero no se utilizan en mayor medida
Usos de la Tecnología	Criptomonedas (Uso principal), Almacenamiento de archivos, perpetuidad y trazabilidad de documentos, sistemas de votación, trazabilidad de alimentos, etc.
Criptomonedas	Se estima que hay más de 10000 criptomonedas distintas al día de hoy pero las principales, y con mayor capitalización de mercado, son Bitcoin, Ethereum, Tether, Cardano, Solana, etc.
Billeteras Virtuales	Es donde se almacenan las criptomonedas, nos da titularidad sobre las mismas. Existen 3 tipos, Billetera por software, por hardware y billetera de papel
Delitos	Existen muchos tipos pero los principales son Robo de Criptomonedas, robo de información (con rescate en criptomonedas), extorsiones (con rescate en criptomonedas), transacciones ilegales, etc.

Luego de la investigación efectuada se entiende que, dado el crecimiento exponencial de los delitos relacionados, hay que desarrollar herramientas para que la justicia y las fuerzas de seguridad puedan investigar y ejecutar acciones para mitigar o prevenir los efectos de los mismos.

3.2 Futuras líneas de investigación

Luego de una investigación preliminar realizada para el presente, se resalta que las criptomonedas vinieron para quedarse. Cada vez son más las personas que se meten en este mundo sin tomar las medidas básicas de seguridad recomendadas para evitar perder sus inversiones.

Como en todo el mundo tecnológico, surgen nuevas y tentadoras tecnologías y es mayor el avance y la complejidad de los delitos relacionados.

En la actualidad, hay empresas que investigan los delitos mencionados e interactúan con las fuerzas de seguridad como también algunas herramientas desarrolladas para realizar análisis de manera más sencilla, pero no hay un esquema que ordene y guie las investigaciones.

Para el trabajo de tesis se plantea la búsqueda y el desarrollo teórico de un marco de trabajo para el análisis forense de los posibles delitos relacionados con las criptomonedas.

El primer paso de este trabajo será profundizar más en el entendimiento de la tecnología Blockchain, continuar investigando las principales criptomonedas del mercado, realizar un profundo análisis de cuales son y cómo se están realizando los delitos sobre las mismas para dar lugar al análisis minucioso de los marcos actuales de análisis forense relacionado a la tecnología y a las herramientas actualmente desarrolladas para el análisis de criptomonedas.

El aporte que se busca es el desarrollo de un marco de trabajo ,el cual sirva para poder guiar una investigación donde las criptomonedas sean parte o fin del delito. El marco mencionado tendrá origen en las directrices expuestas en el RFC 3227 (“Directrices RFC 3227,” 2020), en el estándar desarrollado por la ISO “ISO/IEC 27037:2012” (“ISO/IEC 27037:2012(en), Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence,” n.d.) y en el modelo EDRM (“EDRM Model | EDRM,” 2020).

El EDRM es desde donde se partirá, ya que se basa en los anteriores mencionados y proporciona ocho etapas muy bien definidas: identificación, preservación, recolección, procesamiento, revisión, análisis, producción y presentación. Además, es el marco más actualizado y el cual se está utilizando en las investigaciones actuales relacionadas a delitos, en donde la tecnología se presenta como el medio para efectuarlos.

El trabajo de tesis iniciará en las etapas mencionadas y en el análisis de las principales herramientas actuales para el análisis de delitos relacionados con lascriptomonedasChainalysis(“CryptocurrencyInvestigation Software - Chainalysis Reactor,” n.d.), EllipticForensics(London, n.d.), Scorechain(“Trust provider for crypto markets - AML Compliance Cryptocurrencies | Scorechain,” n.d.), CipherTrace(“CipherTrace - Blockchain Analytics & Cryptocurrency Intelligence Company,” n.d.), (Schüssler et al., 2018; Yang et al.,

2019), (Bartoletti et al., 2017), intentando adaptar las etapas de los marcos actuales (ejemplo EDRM) a la situación delictiva de las cripto y viendo cómo las herramientas actuales desarrolladas pueden alojarse en las distintas etapas, con el fin de guiar una investigación de manera correcta desde la solicitud de la misma hasta la presentación de la evidencia a la autoridad competente, teniendo siempre presente la anonimidad que plantean las criptomonedas y como, mediante el planteo de reglas claras, un sistema de pasos secuenciales y el uso correcto de la propia tecnología blockchain, se puede relacionar uno o varios movimientos a una persona o grupo delictivo.

Marcos de trabajo actuales asociados a los cyberdelitos	
Marcos de trabajo	RFC 3227; ISO/IEC 27037:2012; modelo EDRM.
El modelo EDRM	Es el más utilizado en la actualidad, proporciona 8 etapas, deriva de RFC 3227 y ISO/IEC 27037:2012, sus capas son identificación, preservación, recolección, procesamiento, revisión, análisis, producción y presentación.
Herramientas de análisis	Chainalysis; EllipticForensics; Scorechain; CipherTrace entre otras.

Dentro del desarrollo mencionado y de las herramientas de análisisactualmente involucradas, se buscará identificar cómo la inteligencia artificial puede ayudar en la identificaciónde datos sensibles tales como movimientos delictivos a través del análisis de billeteras virtuales, transacciones sospechosas e incluso intentos de bifurcaciones de cadenas con el fin de prevenir futuros delitos y con la intención de identificar actores maliciosos, tanto previamente a cometer el delito como posteriormente del mismo.

Esta tarea se llevará a cabo aplicando algoritmos deagrupaciónpara diferenciar grupos de transacciones e intentar crearobjetivos y jerarquías; algoritmos de regresión en búsquedade prevenir futuros delitos generando predicción,yalgoritmos de deep learning buscando identificar patrones que resultarán fundamentalespara el proceso de identificación.

El marco a desarrollar incorporarásiete etapas, las cuales son identificación, recolección, procesamiento, revisión, análisis, producción y presentación.No se incorporará una etapa de preservación, ya que la naturaleza de la tecnología que soporta a las cripto no nos permite modificar la información, con lo cual no sería necesaria una preservación de la prueba.

La función básica de cada etapa estaría dada de la siguiente manera:

Marco de trabajo propuesto	
Identificación	Esta etapa está relacionada con la identificación de la información. Va a estar enfocado a qué criptomoneda se va a investigar y por ende, con qué blockchain hay que conectarse.
Recolección	Aquí se definiría el alcance del análisis, con qué blockchain se trabajará, qué cripto está involucrada, desde y hasta donde abarcará el análisis, etc.
Procesamiento	En esta etapa es donde se reducirá la información con la que se trabajará al mínimo nivel para quedarse solo con el contenido inherente.
Revisión	Se evaluará si la información procesada es relevante para la causa, se define si no es necesario incorporar más información.
Análisis	Se realiza el análisis real de la información desde todos los enfoques.
Producción	Se prepara el resultado de la etapa anterior de forma que sea útil para los equipos que tienen que juzgar el hecho o mismo las fuerzas de seguridad que tienen que llevar a cabo sus tareas.
Presentación	Se presenta la información.

En el siguiente gráfico, se plantea el porcentaje de trabajo que demandará cada etapa del marco propuesto.

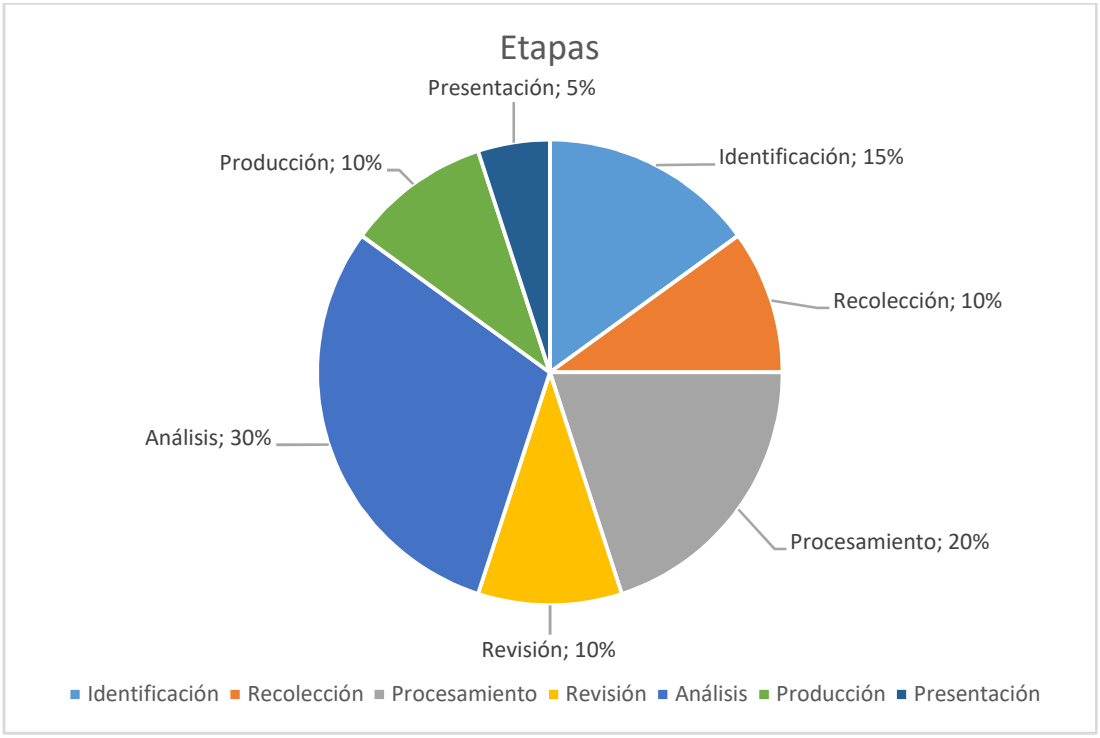

Gráfico 1- Porción de tiempo de cada etapa en el marco de trabajo.

Como se puede visualizar en el grafico 1 la etapa que más tiempo demandará en el Framework planteado es la etapa de Análisis dado que es donde se trabaja sobre toda la

información previamente recolectada y procesada; la etapa de Procesamiento es la segunda más duradera, dado que en ella es donde se trabaja en la reducciónde la información recolectada para trabajar solo con lo relevante al caso, seguida en tiempo por la Identificación, ya que es donde se define sobre qué criptomoneda y Blockchain se iniciará la investigación(fundamental esta etapa para la continuidad del caso).

4. Referencias

Academy, B., 2020. ¿Qué es una UTXO? [WWW Document]. Bit2Me Acad. URL https://academy.bit2me.com/que-es-una-utxo/ (accessed 3.8.21).

Academy, B., 2019. ¿Quién es Nick Szabo? [WWW Document]. Bit2Me Acad. URL https://academy.bit2me.com/quien-es-nick-szabo/ (accessed 2.14.21).

Academy, B., 2018. Mayores Robos de Bitcoin y Criptomonedas [WWW Document]. Bit2Me Acad. URL https://academy.bit2me.com/los-mayores-robos-de-bitcoin-y-criptomonedas-de-la-historia/ (accessed 3.10.21).

Academy, B., 2016. ¿Qué puedes comprar con Bitcoin? [WWW Document]. Bit2Me Acad. URL https://academy.bit2me.com/que-puedes-comprar-bitcoin/ (accessed 3.10.21).

Argentina investiga a la red “Ganancias Deportivas” por presunta estafa con bitcoin [WWW Document], 2021. . CriptoNoticias - Bitcoin Blockchains Criptomonedas. URL https://www.criptonoticias.com/judicial/argentina-investiga-red-ganancias-deportivas-presunta-estafa-bitcoin/ (accessed 3.10.21).

Ast, F., 2019. Breve Historia del Bitcoin [WWW Document]. Medium. URL https://medium.com/astec/breve-historia-del-bitcoin-3cd9942debef (accessed 3.9.21).

Back, A., 2002. Hashcash - A Denial of Service Counter-Measure.

Bartoletti, M., Lande, S., Pompianu, L., Bracciali, A., 2017. A general framework for blockchain analytics, in: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers - SERIAL ’17. Presented at the the 1st Workshop, ACM Press, Las Vegas, Nevada, pp. 1–6. https://doi.org/10.1145/3152824.3152831

Bayer, D., Haber, S., Stornetta, W., 1999. Improving the Efficiency and Reliability of Digital Time-Stamping. https://doi.org/10.1007/978-1-4613-9323-8_24

BBVA, 2019. ‘Deep web’: cinco datos curiosos que no conocías. BBVA Not. URL https://www.bbva.com/es/deep-web-cinco-datos-curiosos-que-no-conocias/ (accessed 3.10.21).

Billeteras para Criptomonedas | MercadoLibre.com.ar [WWW Document], n.d. URL https://listado.mercadolibre.com.ar/criptomonedas-billeteras/_OrderId_PRICE*DESC (accessed 3.10.21).

Bitcoin (BTC) price predictions [WWW Document], n.d. URL https://app.intotheblock.com/predictions/BTC/btcOb60mAvg60m (accessed 3.9.21).

Bitcoin Pizza Day [WWW Document], n.d. URL https://academy.bit2me.com/que-es-bitcoin-pizza-day/ (accessed 2.21.23).

Blockchain Voting: The End To End Process, n.d. . Follow My Vote. URL https://followmyvote.com/blockchain-voting-the-end-to-end-process/ (accessed 3.5.21).

Blockchain.com Explorer | BTC | ETH | BCH [WWW Document], n.d. URL https://www.blockchain.com/explorer (accessed 3.8.21).

Bloques y transacciones [WWW Document], n.d. . Blockchain Fed. Argent. URL http://bfa.ar/blockchain/bloques-y-transacciones (accessed 3.5.21).

Chaum, D., 1983. Blind Signatures for Untraceable Payments, in: Chaum, D., Rivest, R.L., Sherman, A.T. (Eds.), Advances in Cryptology. Springer US, Boston, MA, pp. 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18

CipherTrace - Blockchain Analytics & Cryptocurrency Intelligence Company, n.d. URL https://ciphertrace.com/ (accessed 6.21.21).

Clarín.com, 2021a. México: hackers atacan a la Lotería Nacional y exigen un millonario rescate para no hacer saltar el sistema [WWW Document]. Clarín. URL

https://www.clarin.com/internacional/mexico/mexico-hackers-atacan-loteria-nacional-exigen-millonario-rescate-hacer-saltar-sistema_0_iZwiCHFMt.html (accessed 2.21.23).

Clarín.com, 2021b. Contactaban a hombres por redes sociales haciéndose pasar por nenas y después los extorsionaban [WWW Document]. Clarín. URL https://www.clarin.com/policiales/contactaban-hombres-redes-sociales-haciendose-pasar-nenas-despues-extorsionaban_0_zAI7wB-PI.html (accessed 2.21.23).

Cómo me robaron US$30.000 en criptomonedas, n.d. . BBC News Mundo.

Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia [WWW Document], n.d. . infobae. URL /america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/ (accessed 3.10.21).

Corea del Norte robó 300 millones de dólares en criptomonedas para financiarse [WWW Document], n.d. URL https://www.telam.com.ar/notas/202102/544153-corea-del-norte-robo-300-millones-de-dolares-en-criptomonedas-para-financiarse.html (accessed 2.14.21).

Cryptocurrency Investigation Software - Chainalysis Reactor [WWW Document], n.d. . Chainalysis. URL https://www.chainalysis.com/chainalysis-reactor/ (accessed 6.21.21).

¿Cuán arriesgado es comprar un Tesla usando bitcoin?, 2021. . CNN. URL https://cnnespanol.cnn.com/2021/02/12/cuan-arriesgado-es-comprar-un-tesla-usando-bitcoin/ (accessed 3.10.21).

Decentralized Cloud Storage — Storj [WWW Document], n.d. . Decentralized Cloud Storage — Storj. URL https://storj.io (accessed 3.4.21).

Detectan cuántos bitcoins se pierden por día y los motivos de la desaparición [WWW Document], n.d. URL https://www.ambito.com/negocios/bitcoin/detectan-

cuantos-s-se-pierden-dia-y-los-motivos-la-desaparicion-n5135103 (accessed 3.10.21).

Detienen a una pandilla en Dubai por robar $2 millones a compradores de bitcoin [WWW Document], 2018. . CriptoNoticias - Bitcoin Blockchains Criptomonedas. URL https://www.criptonoticias.com/judicial/detienen-pandilla-dubai-robar-2-millones-compradores-bitcoin/ (accessed 3.10.21).

Diferencias entre criptomoneda, moneda virtual y dinero digital [WWW Document], n.d. URL https://www.cace.org.ar/noticias-diferencias-entre-criptomoneda-moneda-virtual-y-dinero-digital (accessed 3.9.21).

Dinero virtual, 2021. . Wikipedia Encicl. Libre.

Directrices RFC 3227, 2020. . Ciberforensic. URL https://www.ciberforensic.com/directrices-rfc-3227 (accessed 3.30.21).

EDRM Model | EDRM, 2020. URL https://edrm.net/edrm-model/ (accessed 3.30.21).

El análisis de Utxo revela mucho sobre bitcoin, litecoin, dash y otros criptoactivos [WWW Document], n.d. URL https://www.hebergementwebs.com/blockchain/el-analisis-de-utxo-revela-mucho-sobre-bitcoin-litecoin-dash-y-otros-criptoactivos (accessed 3.9.21).

Ethereum Whitepaper [WWW Document], n.d. . ethereum.org. URL https://ethereum.org (accessed 2.14.21).

Galinsky, P., 2018. El primer balneario del país en el que se puede alquilar carpa con bitcoins [WWW Document]. URL https://www.clarin.com/sociedad/primer-balneario-pais-puede-alquilar-carpa-bitcoins_0_r12Ky49VG.html (accessed 3.10.21).

Guía sobre Tipos de Criptomonederos [WWW Document], n.d. . Binance Acad. URL https://academy.binance.com/es/articles/crypto-wallet-types-explained (accessed 3.10.21).

Haber, S., Stornetta, W.S., 1991. How to time-stamp a digital document. J. Cryptol. 3, 99–111. https://doi.org/10.1007/BF00196791

Healthchain [WWW Document], 2020. . IBM Comun. URL https://www.ibm.com/blogs/ibm-comunica/module/healthchain/ (accessed 3.4.21).

ISO/IEC 27037:2012(en), Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence [WWW Document], n.d. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en (accessed 9.28.20).

King, S., Nadal, S., n.d. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake 6.

La web que te dice si te robaron las contraseñas de Dropbox, LinkedIn, MySpace y otras cuentas (y cómo protegerte), n.d. . BBC News Mundo.

Latifi, S., Zhang, Y., Cheng, L.-C., 2019. Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market, in: 2019 IEEE International Conference on Blockchain (Blockchain). Presented at the 2019 IEEE International Conference on Blockchain (Blockchain), pp. 528–535. https://doi.org/10.1109/Blockchain.2019.00002

London, n.d. Blockchain Analytics & Compliance Solutions | Elliptic [WWW Document]. URL https://www.elliptic.co (accessed 6.21.21).

Mercado Libre Argentina incorpora sección para compraventa de inmuebles con bitcoin [WWW Document], 2021. . CriptoNoticias - Bitcoin Blockchains Criptomonedas. URL https://www.criptonoticias.com/comunidad/adopcion/mercado-libre-argentina-incorpora-seccion-compraventa-inmuebles-bitcoin/ (accessed 5.25.21).

Mt. Gox: de la magia a la quiebra [WWW Document], 2019. . CriptoNoticias - Bitcoin Blockchains Criptomonedas. URL https://www.criptonoticias.com/seguridad-bitcoin/mt-gox-magia-quiebra/ (accessed 3.10.21).

Nakamoto, S., n.d. Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario 9.

Nieto, A., 2018. Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital [WWW Document]. Xataka. URL https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital (accessed 3.9.21).

Nueva ola de correos spam incluyen contraseñas de usuarios en el asunto [WWW Document], 2020. . WeLiveSecurity. URL https://www.welivesecurity.com/la-es/2020/04/14/sextorsion-nueva-ola-spam-incluyen-contrasenas-usuarios-asunto/ (accessed 3.10.21).

Nyaletey, E., Parizi, R.M., Zhang, Q., Choo, K.R., 2019. BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability, in: 2019 IEEE International Conference on Blockchain (Blockchain). Presented at the 2019 IEEE International Conference on Blockchain (Blockchain), pp. 18–25. https://doi.org/10.1109/Blockchain.2019.00012

País, E., 2013. 38 millones de cuentas de Adobe, hackeadas. El País.

pauta, n.d. La Ruta de la Seda, el mayor caso de narcotráfico en la historia de la web [WWW Document]. pauta. URL https://www.pauta.cl/ciencia-y-tecnologia/narcotrafico-online-la-historia-de-la-ruta-de-la-seda-virtual (accessed 2.14.21).

Proof of Existence [WWW Document], n.d. URL https://proofofexistence.com/ (accessed 3.4.21).

¿Qué es la Deep Web y la Dark Web? [WWW Document], 2021. . www.kaspersky.es. URL https://www.kaspersky.es/resource-center/threats/deep-web (accessed 2.21.23).

¿Quién es Hal Finney? [WWW Document], n.d. URL https://academy.bit2me.com/quien-es-hal-finney/ (accessed 2.21.23).

Roban más de 65 millones de dólares en bitcoin a BitFinex [WWW Document], 2016. . Hipertextual. URL http://hipertextual.com/2016/08/robo-bitcoin-bitfinex (accessed 3.10.21).

Robo a mano armada de $1,8 millones en ethers es denunciado en Nueva York [WWW Document], 2017. . CriptoNoticias - Bitcoin Blockchains Criptomonedas. URL https://www.criptonoticias.com/judicial/robo-mano-armada-1-millones-ethers-denunciado-nueva-york/ (accessed 3.10.21).

RPOW - Reusable Proofs of Work | Satoshi Nakamoto Institute [WWW Document], n.d. URL https://nakamotoinstitute.org/finney/rpow/ (accessed 3.4.21).

Schüssler, F., Nasirifard, P., Jacobsen, H.-A., 2018. Attack and Vulnerability Simulation Framework for Bitcoin-like Blockchain Technologies, in: Proceedings of the 19th International Middleware Conference on - Middleware '18. Presented at the the 19th International Middleware Conference, ACM Press, Rennes, France, pp. 5–6. https://doi.org/10.1145/3284014.3284017

"Sextorsión", la nueva estafa por mail que revela tu contraseña y fotos privadas - Infotechnology.com [WWW Document], n.d. URL https://www.infotechnology.com/online/Sextorsion-la-nueva-estafa-por-mail-que-revela-tu-contrasena-y-fotos-privadas-20180723-0001.html (accessed 3.10.21).

Shelling Out: The Origins of Money | Satoshi Nakamoto Institute [WWW Document], n.d. URL https://nakamotoinstitute.org/shelling-out/ (accessed 3.4.21).

Tecnología blockchain en el Sistema Informático de Trazabilidad Citrícola [WWW Document], 2019. . Argentina.gob.ar. URL https://www.argentina.gob.ar/noticias/tecnologia-blockchain-en-el-sistema-informatico-de-trazabilidad-citricola (accessed 3.5.21).

Trust provider for crypto markets - AML Compliance Cryptocurrencies | Scorechain [WWW Document], n.d. URL https://www.scorechain.com/#risk-aml-due-diligence (accessed 6.21.21).

Yang, X., Chen, Y., Chen, X., 2019. Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information, in: 2019 IEEE International Conference on Blockchain (Blockchain). Presented at the 2019 IEEE International Conference on Blockchain (Blockchain), pp. 261–265. https://doi.org/10.1109/Blockchain.2019.00041

Apéndice

Motivación	Las criptomonedas proponen un nuevo paradigma en el mundo económico, este nuevo paradigma conlleva nuevos delitos. El presente trabajo pretende avanzar con una investigación para entender las criptomonedas, los delitos asociados en pos de poder sentar la base teórica para el futuro desarrollo de un marco de forensia para las mismas.	
Objetivo	Obtener información de las criptomonedas, su funcionamiento, su tecnología y los delitos asociados.	
Preguntas De Investigación	**Q1**: ¿Que criptomonedas son las de mayor uso?	
	Q2: ¿Cuáles son las tecnologías primarias y cómo funcionan?	
	Q3: ¿Qué delitos asociados existen?	
	Q4: ¿Cuáles son los marcos de Forensia actuales?	
	Q5: ¿Cuál de esos marcos se acerca más a la tecnología utilizada en Criptomonedas?	
Búsqueda	**Cadenas y palabras claves**	**C1**: Bitcoin
		C2: Criptomonedas
		C3: Monedas virtuales
		C4: Blockchain
		C5: Billetera virtual
		C6: Delitos cibernéticos
		C7:PoW
		C8: Bloques
		C9: Ethereum
		C10: Framework seguridad
		C11: Criptomonedas + usos
		C12: Framework + criptomonedas
		C13: EDRM
	Período	2007-2021
	Fuentes y sitios	**FB1**: Google Scholar
		FB2: ACM Library
		FB3: IEEE Explore
		FB4: Elsevier
		FB5: SEDICI
		FB6: Sciencedirect
		FB7: Nakamoto Institute
		FB8: www.criptonoticias.com
		FB9: www.blockchain.com
		FB10: academy.bit2me.com
		FB11: ethereum.org
		FB12: ciphertrace.com
		FB13: medium.com