IMPLEMENTACIÓN DE LA COMPUTACIÓN CUÁNTICA COMO HERRAMIENTA PARA LA APERTURA DE MONEDEROS VIRTUALES, CUYA CLAVE FUE OLVIDADA

PRESENTADO POR:

LUIS FELIPE TRIVIÑO PAREDES
CÓDIGO: 20202099019



UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
ESPECIALIZACIÓN EN INGENIERÍA DE SOFTWARE
TRABAJO DE GRADO
BOGOTA D.C.
2021

IMPLEMENTACIÓN DE LA COMPUTACIÓN CUÁNTICA COMO HERRAMIENTA PARA LA APERTURA DE MONEDEROS VIRTUALES, CUYA CLAVE FUE OLVIDADA

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE:

ESPECIALISTA EN INGENIERÍA DE SOFTWARE

DIRECTORA:
ING. ALEXANDRA ABUCHAR PORRAS

REVISORA:
ING. SANDRA MILENA CORTES MUÑOZ



UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
ESPECIALIZACIÓN EN INGENIERÍA DE SOFTWARE
TRABAJO DE GRADO
BOGOTA D.C.
2021

Tabla de Contenido

INTRODUCCIÓN 7
PARTE I. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 8
CAPÍTULO 1. DESCRIPCION DE LA INVESTIGACIÓN 8
1.1 TÍTULO Y DEFINICIÓN DEL TEMA DE LA INVESTIGACIÓN 8
1.2 ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN 8
1.2.1 Planteamiento del problema 8
1.2.2 Formulación del problema 9
1.2.3 Sistematización del problema 9
1.3 OBJETIVOS DE LA INVESTIGACIÓN 9
1.3.1 Objetivo general 9
1.3.2 Objetivos específicos 9
1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN 10
1.4.1 Justificación práctica 10
1.5 MARCO REFERENCIAL 10
1.5.1 Marco teórico 10
1.5.2 Marco conceptual 18
1.6 HIPÓTESIS CONCEPTUAL 19
1.7 ASPECTOS METODOLÓGICOS 20
1.7.1 Tipo de estudio 20
1.7.2 Método de investigación 20
1.7.3 Fuentes y técnicas para la recolección de la información 20
1.7.4 Tratamiento de la información 20
1.8 CRONOGRAMA 20
PARTE 2. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 21
CAPÍTULO 2. DESARROLLO DE LA INVESTIGACIÓN 21
2.1 MONEDERO VIRTUAL 21
2.1.1 ¿Qué es? 21
2.1.2 ¿Cómo funciona? 21
2.1.3 Tipos de monederos 22
2.1.4 Desarrollo de monederos 25
2.1.5 Semilla maestra 26
2.1.6 Formatos de billeteras 27
2.1.7 Servicios de monederos (Empresas) 28
2.2 ALGORITMOS DE ENCRIPTACIÓN 28
2.2.1 SHA-256 28

2.2.2 AES-256 30
2.3 PSICOLOGIA DE LAS CONTRASEÑAS 31
2.3.1 Escritura Leet 32
2.3.2 Personalidades detrás de las contraseñas 33
2.4 ESPECIFICACIÓN DE CONTRASEÑAS 34
2.5 TECNICAS 34
2.5.1 Permutaciones 34
2.5.2 Combinaciones 35
2.5.3 Diccionario de datos 35
2.5.4 TarGuess 36
2.6 HERRAMIENTAS DISPONIBLES PARA DESENCRIPTAR 37
2.6.1 My wallet backup decryption tool 37
2.6.2 Btcrecover 38
2.7 COMPUTACIÓN CUANTICA 39
2.7.1 Avances generales 39
2.7.2 Aplicaciones actuales 40
PARTE 3. CIERRE DE LA INVESTIGACIÓN 42
CAPÍTULO 3. RESULTADOS 42
3.1 ALCANCE IDENTIFICADO 42
3.2 MATRIZ DE TIEMPOS 42
3.2.1 Información relevante 43
3.2.2 Información moderada 49
3.2.3 Información insuficiente 55
CAPÍTULO 4. CONCLUSIONES 61
4.1 VERIFICACIÓN, CONTRASTE Y EVALUACIÓN DE LOS OBJETIVOS 61
4.2 APORTES ORIGINALES 62
4.3 TRABAJOS O PUBLICACIONES DERIVADAS 62
CAPÍTULO 5. PROSPECTIVA DEL TRABAJO DE GRADO 62
5.1 LINEAS DE INVESTIGACIÓN FUTURAS 62
5.2 TRABAJOS DE INVESTIGACIÓN FUTUROS 62
REFERENCIAS WEB 63

Tabla de Ilustraciones

Ilustración 1 - Cronograma general del proyecto **20**
Ilustración 2- Billetera o monedero virtual de papel **23**
Ilustración 3 - Billetera o monedero virtual Hardware **24**
Ilustración 4 - Cifrado SHA-256 ..... **29**
Ilustración 5- Ejemplo Leet **33**
Ilustración 6 - Especificación de contraseñas en las billeteras virtuales **34**
Ilustración 7 - Especificación de contraseñas en las billeteras virtuales **36**
Ilustración 8 - Arquitectura de TarGuess **37**
Ilustración 9 - Interfaz gráfica de My Wallet backup decryption tool **38**
Ilustración 10 - Estimación tiempos contraseña corta, numérica y con información relevante **43**
Ilustración 11 - Estimación tiempos contraseña corta, numérica, minúsculas y con información relevante **43**
Ilustración 12 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información relevante **44**
Ilustración 13 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante **44**
Ilustración 14 - Estimación tiempos contraseña estándar, numérica y con información relevante **45**
Ilustración 15 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información relevante **45**
Ilustración 16 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información relevante **46**
Ilustración 17 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante **46**
Ilustración 18 - Estimación tiempos contraseña compleja, numérica y con información relevante **47**
Ilustración 19 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información relevante **47**
Ilustración 20 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información relevante **48**
Ilustración 21 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante **48**
Ilustración 22 - Estimación tiempos contraseña corta, numérica y con información moderada **49**
Ilustración 23 - Estimación tiempos contraseña corta, numérica, minúsculas y con información moderada **49**
Ilustración 24 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información moderada **50**
Ilustración 25 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada **50**
Ilustración 26 - Estimación tiempos contraseña estándar, numérica y con información moderada **51**
Ilustración 27 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información moderada **51**
Ilustración 28 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información moderada **52**
Ilustración 29 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada **52**
Ilustración 30 - Estimación tiempos contraseña compleja, numérica y con información moderada **53**
Ilustración 31 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información moderada **53**
Ilustración 32 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información moderada **54**
Ilustración 33 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada **54**
Ilustración 34 - Estimación tiempos contraseña corta, numérica y con información insuficiente **55**

Ilustración 35 - Estimación tiempos contraseña corta, numérica, minúsculas y con información insuficiente 55
Ilustración 36 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información insuficiente..... 56
Ilustración 37 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente 56
Ilustración 38 - Estimación tiempos contraseña estándar, numérica y con información insuficiente 57
Ilustración 39 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información insuficiente 57
Ilustración 40 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información insuficiente..... 58
Ilustración 41 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente 58
Ilustración 42 - Estimación tiempos contraseña compleja, numérica y con información insuficiente.... 59
Ilustración 43 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información insuficiente 59
Ilustración 44 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información insuficiente..... 60
Ilustración 45 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente..... 60

INTRODUCCIÓN

El auge de las criptomonedas ha atraído a diversos tipos de personas en todo el mundo que buscan poder realizar transacciones rápidas reduciendo los costos de transacción o simplemente buscando invertir, con la esperanza de que dichos activos aumenten su valor.
La base de esta moneda digital es la criptografía cuya implementación provee de seguridad las transacciones, controla la creación de nuevas unidades y resguarda el acceso a tan preciados activos.
Gran parte de quien ha adquirido algunas unidades de criptomonedas en sus inicios con muy poca inversión, han sido personas curiosas que buscaban entender este nuevo mercado y ver sus ventajas frente al sector financiero tradicional, pero quedó en eso, simple curiosidad.

Con el transcurrir de los años y al ver el crecimiento exponencial y acelerado que ha tenido el valor de estos cripto activos, muchos de estos curiosos e inexpertos se han dado cuenta que sus pequeñas inversiones de hace algunos años, ahora son una fortuna y al intentar acceder a estos recursos, se han encontrado con la sorpresa de que sus credenciales de acceso son inválidas debido al olvido de su contraseña principal; es aquí donde parte esta investigación que se desarrollará durante todo el documento con el apoyo del nuevo paradigma de la computación cuántica y buscará guiar y ayudar a miles de personas por descuido hoy no tienen acceso a sus recursos.

PARTE I. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

CAPÍTULO 1. DESCRIPCION DE LA INVESTIGACIÓN

1.1 TÍTULO Y DEFINICIÓN DEL TEMA DE LA INVESTIGACIÓN

Título: Implementación de la computación cuántica como herramienta para la apertura de monederos virtuales, cuya clave fue olvidada.

Tema de investigación:
Aplicación de la computación cuántica en la criptografía tradicional.

1.2 ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN

1.2.1 Planteamiento del problema

Los monederos virtuales donde se almacenan las criptomonedas tienen como característica principal la encriptación de la información mediante una contraseña principal que solo el dueño de dicho monedero debe tener acceso, es decir que ninguna plataforma ni empresa guarda esta información por seguridad ya que si son hackeados los recursos de sus clientes no se van a ver afectados. Otra opción para acceder a los recursos es la combinación de 12 palabras generadas aleatoriamente que sirven como contingencia en caso de que la contraseña principal haya sido olvidada.
Hoy, muchas personas tienen grandes recursos almacenados en estos monederos, sin embargo, no recuerdan su contraseña principal ni las 12 palabras de recuperación, causando la pérdida temporal del acceso a estos activos y por supuesto la oportunidad de poder invertir o vender sus criptomonedas.
La proyección teórica en el valor de estos cripto activos tiende a aumentar con el transcurrir de los años, sin embargo, las criptomonedas son muy sensibles a temas legales y de reputación entre la comunidad de inversionistas y muchas veces su valor es muy volátil permitiendo no solo aumentar las ganancias sino también perder todo repentinamente.

Con base a lo anterior, es muy importante poder prever y controlar estas situaciones, accediendo a los fondos de estos monederos rápidamente mediante la implementación de la computación cuántica que teóricamente será una gran herramienta en esta labor.

1.2.2 Formulación del problema

¿Cuáles son las herramientas que el paradigma de la computación cuántica puede ofrecer para acceder a los fondos de un monedero virtual, cuya clave principal fue olvidada?

1.2.3 Sistematización del problema

- ¿Qué relación tiene la computación cuántica y la criptografía?
- ¿Qué métodos criptográficos utilizan los monederos virtuales?
- ¿Qué alternativas existen para acceder o recuperar los fondos de un monedero virtual?
- ¿Por qué la computación cuántica puede convertirse en una herramienta para acceder a criptomonedas olvidadas?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo general

- Identificar alternativas criptográficas mediante los avances y resultados que la computación cuántica ha obtenido en esta área y así poder acceder a los fondos de cualquier monedero virtual cuya clave principal fue olvidada.

1.3.2 Objetivos específicos

- Enumerar las técnicas criptográficas utilizadas en el almacenamiento de las criptomonedas basado en la información pública de empresas que prestan este servicio para tener un contexto real y cuantitativo de estas técnicas.
- Especificar los avances de la computación cuántica en el área de la criptografía apoyado en documentación científica para ver su posible implementación en los monederos virtuales.
- Definir teóricamente los tiempos estimados para la apertura de un monedero virtual mediante el análisis de casos de éxito obtenidos en la práctica de la computación cuántica sobre la criptografía.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1 Justificación práctica

El resultado de esta investigación ayudará a muchas personas que tienen dificultades para acceder a los fondos de su monedero virtual, porque brindará las herramientas y presentará alternativas basadas en teorías comprobables que estarán enfocadas en la solución del problema planteado.

1.5 MARCO REFERENCIAL

1.5.1 Marco teórico

Criptografía[1]:

La criptografía es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo. Hoy en día, en pleno auge de las comunicaciones digitales, funciona como la base para cualquier proceso de seguridad informática.

Esta disciplina nació en la Antigua Grecia con el objetivo de evitar que se difundan secretos militares. Los mensajes se encriptan con métodos sencillos como, por ejemplo, alternando las letras del abecedario. Con el correr de los siglos esas técnicas se fueron complejizando considerablemente y actualmente atraviesan gran parte de nuestra vida cotidiana: garantizan la seguridad de nuestras transacciones mediante banca online, por ejemplo. También van ganando protagonismo en la comunicación entre usuarios: aplicaciones de mensajería como Signal o Telegram desde hace años nos permiten enviar mensajes encriptados de “punta a punta”, desde el origen hasta el destino. Así, ni siquiera accediendo a sus servidores se podría leer el contenido de los chats. WhatsApp se integró a la tendencia en 2016 y Skype recién a principios de 2018, confirmando un rumbo claro hacia plataformas de comunicación más seguras.

Pero ¿cómo funcionan hoy en día estos métodos de encriptación? Cuando convertimos un mensaje que puede ser leído a uno que es ilegible, es decir que a un mensaje lo transformamos en caracteres que no construyen sentido, estamos realizando lo que denominamos un proceso de cifrado. Y si queremos que, nuevamente, ese mensaje sea legible, hacemos el proceso inverso, al que denominamos descifrado. Por

[1] "¿Qué es criptografía? | NIC Argentina." http://nic.ar/es/enterate/novedades/que-es-criptografia. Marzo. 2018.

lo general estos mecanismos, que conforman la base de la criptografía, se realizan mediante algoritmos y claves.

En la actualidad existen diversos tipos de criptografía:

Criptografía simétrica

Solo utiliza una clave para cifrar y descifrar. Ésta debe ser previamente conocida por todas las partes involucradas.

Podemos imaginar este sistema como algo similar a la seguridad de nuestra casa. Tenemos una llave para cerrar la puerta y estamos tranquilos que solo las personas con esa misma llave la van a poder abrir. Tenemos la ventaja que podemos compartirla con cualquier persona de confianza, pero también existe la posibilidad de que se extravíe, o de que alguien la robe. Esa es la principal desventaja de la criptografía simétrica.

Criptografía asimétrica o criptografía de clave pública

Esta metodología tiene como base la utilización de dos claves diferentes, pero vinculadas matemáticamente entre sí, utilizadas para cifrar y descifrar el mensaje. Una de ellas debe ser pública, propia de cada participante, pero puesta a disposición de cualquier usuario, sea participante en el intercambio de información o no. La otra es una clave privada, también propia de cada uno de ellos, pero que debe permanecer en secreto y nunca ser revelada. Al requerir que cada usuario posea un par de claves, y que una de ellas no se comunique nunca a nadie, todo el proceso se vuelve más seguro.

Una característica importante de este sistema es que nos permite garantizar la privacidad de un mensaje. El emisor puede cifrar con la clave pública del destinatario (que, como vimos, tiene a su disposición) y con esto se asegura que solo ese destinatario podrá descifrarlo con su clave privada.

Criptomonedas[2]:

Una criptomoneda es una moneda digital diseñada para funcionar como medio de intercambio. Utiliza la criptografía para asegurar y verificar transacciones, así como para controlar la creación de nuevas unidades de una criptomoneda particular. Esencialmente, las criptomonedas son entradas limitadas en una base de datos que nadie puede cambiar a menos que se cumplan condiciones específicas. Existen miles de criptomonedas, la más popular es Bitcoin, pero aquí vamos a contarte acerca de qué son las criptomonedas en general y cómo funcionan. Sigue

[2] "¿Qué es criptomoneda? - Cointelegraph." https://es.cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies.

leyendo para aprender más sobre el dinero digital del futuro y cómo entender su funcionamiento para que de esta manera puedas utilizarlas de una mejor manera y puedas aprender a invertir en criptomonedas sabiamente.

Las criptomonedas más comunes:

Bitcoin — La primera criptomoneda que comenzó todo.

Ethereum — una moneda Turing completa programable que permite a los desarrolladores crear diferentes aplicaciones distribuidas y tecnologías que no funcionan con Bitcoin.

Ripple — A diferencia de la mayoría de las criptomonedas, no utiliza una Blockchain para alcanzar un consenso en toda la red para las transacciones. En cambio, se implementa un proceso iterativo de consenso, que lo hace más rápido que Bitcoin, pero también lo hace vulnerable a los ataques de hackers.

Bitcoin Cash — Una bifurcación de Bitcoin respaldada por la mayor empresa minera de Bitcoin y fabricante de chips ASIC para minería de Bitcoin. Solo ha existido durante un par de meses, pero ya se ha disparado a las cinco principales criptomonedas en términos de capitalización de mercado.

NEM — A diferencia de la mayoría de las otras criptomonedas que utilizan un algoritmo de Prueba de trabajo, usa Prueba de importancia, que requiere que los usuarios ya posean ciertas cantidades de monedas para poder obtener otras nuevas. Alienta a los usuarios a gastar sus fondos y realizar un seguimiento de las transacciones para determinar qué tan importante es un usuario en particular para la red NEM en general.

Litecoin — Una criptomoneda que se creó con la intención de ser la 'plata digital' en comparación con el 'oro digital' qué es Bitcoin. También es una bifurcación de Bitcoin, pero a diferencia de su predecesor, puede generar bloques cuatro veces más rápido y tener cuatro veces la cantidad máxima de monedas en 84 millones.

IOTA — La avanzada tecnología de contabilidad de esta criptomoneda se llama 'Enredo' y requiere que el remitente en una transacción realice una Prueba de trabajo que aprueba dos transacciones. Por lo tanto, IOTA ha eliminado a los mineros dedicados del proceso.

NEO — Es una red de contratos inteligentes que permite desarrollar todo tipo de contratos financieros y aplicaciones distribuidas de terceros. Tiene muchos de los mismos objetivos que Ethereum, pero se desarrolló en

China, lo que puede darle algunas ventajas debido a una mejor relación con los reguladores chinos y las empresas locales.

Dash — Es una red de dos niveles. El primer nivel son los mineros que aseguran la red y registran las transacciones, mientras que el segundo consiste en "nodos maestros" que transmiten transacciones y habilitan el tipo de transacción InstantSend y PrivateSend. El primero es significativamente más rápido que Bitcoin, mientras que el segundo es completamente anónimo.

Qtum — Es una fusión de las tecnologías de Bitcoin y Ethereum dirigidas a aplicaciones comerciales. La red cuenta con la confiabilidad de Bitcoin, al tiempo que permite el uso de contratos inteligentes y aplicaciones distribuidas, funciona parecido a la red Ethereum.

Monero — Una criptomoneda con capacidades de transacciones privadas y una de las comunidades más activas, que se debe a sus ideales abiertos y centrados en la privacidad.

Ethereum Classic — Una versión original de Ethereum. La división ocurrió después de que una organización autónoma descentralizada construida sobre el Ethereum original fuera pirateada.

Monedero virtual[3]:

Las wallets o monederos de criptomonedas, son el puente que nos permiten administrar nuestras criptomonedas. Una pieza de software o de hardware con los que realizar las operaciones de recepción y envío a través de la red blockchain de cada criptomoneda.

Uno de los elementos más importantes en mundo criptográfico y de la tecnología blockchain son las wallets o monederos. El uso de estas herramientas es indispensable a la hora de gestionar nuestras criptomonedas. Es por ello, que elegir una adecuada y que cumpla con nuestras necesidades es tan importante como disponer de una. Por esta razón, en este artículo te compartiremos la información más importante y fundamental que debes conocer para comprender qué son las wallets y cómo funcionan.

El término wallet hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de nuestras criptomonedas.

---

[3] "Qué es una wallet o monedero de criptomonedas | Bit2Me ...." 1 Jun. 2020, https://academy.bit2me.com/wallet-monederos-criptomonedas/.

¿Cómo funcionan los monederos o wallet de criptomonedas?

Como ya mencionamos, wallet o monederos de criptomonedas son uno de los elementos más importantes e indispensables a la hora de operar con estas. Esto debido a que son las que nos permiten enviar o recibir pagos en criptoactivos.

A diferencia del sistema financiero tradicional, Bitcoin y otras criptomonedas son monedas totalmente digitales que no existen en el mundo físico y que funcionan basándose en criptografía. Por ello, el diseño de las wallets es de vital importancia para poder operar y gestionar nuestros fondos. Y aunque, el término monedero nos parezca similar al que usamos para guardar nuestro dinero físico, lo cierto es que, en criptomonedas, lo que realmente se almacena en las wallets son las claves públicas y privadas.

Las criptomonedas como tal, no existen como monedas, sino más bien como registros de transacciones contenidos dentro de una blockchain que es operada por nodos interconectados entre sí alrededor de todo el mundo. Entonces, las claves públicas y, sobre todo, las claves privadas dentro de una wallet son las que nos dan la propiedad y derecho sobre las criptomonedas transferidas a una dirección en particular. Veamos esto con más detalle:

La clave pública es similar a un número de cuenta bancaria. Podemos entregarla a cualquier persona para que nos envíe dinero, sin el riesgo de que pueda extraer nuestros fondos. A través de la clave pública se generan direcciones para recibir, consultar y ver el estado de nuestros fondos.

La clave privada funciona como una especie de llave, un PIN o contraseña que no debemos revelar a nadie, ya que nos otorga el derecho de gastar las criptomonedas contenidas en una dirección. Así, el propietario de la clave privada será el propietario de los fondos y tendrá total control sobre ellos.

Seguridad de los monederos:

Las wallets o monederos utilizan avanzadas técnicas de cifrado de las blockchain para otorgar y garantizar seguridad total a los usuarios. De esta forma la wallet puede guardar, enviar y recibir criptomonedas sin mayor riesgo.

En el momento de configurar una wallet, lo primero es crear una clave privada mediante un algoritmo seguro. Por ejemplo, a través del algoritmo ECDSA usando la curva elíptica secp256k1. O también puede usarse el algoritmo EdDSA. En cualquiera de los casos el objetivo es proporcionar

un alto nivel de seguridad. Esto gracias a que ambos métodos permiten la creación de combinaciones casi infinitas y con un alto grado de dificultad. Esto hace que sean prácticamente imposibles de adivinar o ser atacadas por la fuerza.

Luego de la generación de la clave privada, se procede a la creación de la clave pública, la cual está relacionada matemáticamente con la primera. Y a partir de la clave pública se generan las direcciones donde podemos recibir criptomonedas. No obstante, es importante señalar que, aunque la clave pública se genere y esté relacionada con la clave privada, no se puede hacer el proceso inverso. Es decir, no podemos deducir la clave privada partiendo de la clave pública, ya que el algoritmo usado para la creación es unidireccional.

Así mismo, existen wallets deterministas (wallets HD) que, al momento de configurarlas por primera vez, generan una seed o semilla. A partir de la cual son generadas todas las claves y direcciones. Posteriormente nos servirá para restaurar, recuperar el monedero y nuestros fondos en caso de daño o pérdida de los equipos. Estas semillas son una especie de código que está representado por palabras mnemotécnicas generalmente en inglés. Con el fin de brindar una mayor facilidad al momento de realizar copias de seguridad.

Como dato curioso es importante señalar que las claves tanto públicas como privadas generadas en una wallet no están relacionadas con el protocolo de la criptomoneda. Si no más bien, resguardarse dentro del hardware que las opera y nunca abandonan el dispositivo. No obstante, el nivel de seguridad proporcionado por una wallet dependerá del tipo que se esté empleando, sea un hardware wallet, paper wallet, light wallets, software para desktop, tablet o smartphone, u online.

Computación cuántica[4]:

La computación cuántica es uno de esos conceptos que resuena cada vez más en medios generalistas haciéndose eco de un avance científico notorio en cuanto a un nuevo paradigma de computación. Cuáles son sus ventajas, limitaciones, inconvenientes y avances reales es lo que intentaremos abordar brevemente en este post.

De manera simplificada, la computación cuántica supone un cambio de paradigma con respecto a la computación clásica, funcionando con qubits o bits cuánticos (habitualmente denominados “qubits”), permitiendo una enorme capacidad de cómputo utilizando las propiedades de la mecánica

[4] "La computación cuántica y el “futuro de la criptografía”: 15 Enero 2020, https://www.bbvanexttechnologies.com/la-computacion-cuantica-y-el-futuro-de-la-criptografia-la-criptografia-post-cuantica/.

cuántica y la superposición de estados. En computación clásica un bit puede tener los valores 0 o 1, en computación cuántica el valor 0 y 1 a la vez, o mejor dicho probabilidades de ambos valores a la vez (superposición cuántica de estados).

Este hecho que podría ser “anecdótico” presenta una gran utilidad al desarrollarse algoritmos teóricos específicos, que aprovechan esa superposición, para tratar problemas computacionalmente complejos de resolver con ordenadores clásicos. Y si en papel es posible desarrollar algoritmos con gran capacidad para resolver problemas computacionalmente intratables, el reto recae en construir ordenadores que los puedan ejecutar de manera adecuada. Este es el motivo del interés y avance en la computación cuántica.

En 1998, se consiguió por primera vez probar un algoritmo cuántico usando 2 qubits en la Universidad de Oxford. En 2000, se consiguieron ordenadores con 4, 5 y 7 qubits. En 2006, 12 qubits en un ordenador cuántico del Institute for Quantum Computing, Perimeter Institute for Theoretical Physics y MIT. La disponibilidad e interés para acceder a este tipo de ordenadores ha ido en aumentando hasta nuestros días. Empresas como IBM permiten programar tus propios algoritmos cuánticos y poder probarlos tanto en simuladores como ordenadores cuánticos reales a través de su plataforma IBM Q o utilizar su primer ordenador cuántico comercial el IBM Q System One con 20 qubits. Otras empresas como AWS también permiten probar algoritmos cuánticos a través de su servicio Amazon Quantum Solutions Lab, pudiéndose probar en distintos tipos de ordenadores cuánticos como D-Wave, Rigetti o IonQ. Por ejemplo, BBVA ha firmado un acuerdo con el CSIC para investigar el potencial de la computación cuántica en el sector financiero.

La supremacía cuántica

En los últimos meses ha tenido una gran repercusión que Google haya logrado la supremacía cuántica, esto es, un problema que los ordenadores cuánticos pueden resolver pero que los ordenadores clásicos no en un tiempo “razonable”. En el artículo publicado por Google en la revista Nature, los autores reclaman que han logrado la supremacía cuántica al lograr resolver un problema en un ordenador cuántico infinitamente más rápido que haciéndolo en un ordenador clásico. El procesador desarrollado por Google, de nombre Sycamore, tiene 54 qubits, resolviendo el problema en sólo 200 segundos. Los autores estiman que resolver este problema en un superordenador clásico hubiera tardado 10000 años, logrando así la supremacía cuántica.

¿Qué consecuencias tendrá la computación cuántica en la seguridad informática?

A día de hoy nadie sabe exactamente cuándo existirá un ordenador cuántico con la suficiente capacidad (diseño y qubits) para anular procedimientos que facilitan mecanismos de seguridad en las comunicaciones y redes digitales, típicamente mediante el uso de criptografía. El rango de fechas es muy holgado desde unos pocos años, para los muy optimistas, hasta varias décadas. Lo que está claro es que difícilmente dispondremos de estos ordenadores a nivel particular en las próximas décadas con lo que es un asunto que quedará restringido a grandes países con capacidad económica y científica para llevar este complejo proyecto adelante. Este asunto no es baladí ya que es importante para una correcta gestión de expectativas, contramedidas y gestión del riesgo. Una de las estimaciones a menudo referenciadas postula un ordenador con estas características aproximadamente para el 2030 con un coste de 1000 millones de euros y una planta nuclear (PQCrypto 2014, Matteo Mariantoni).

En el caso de existir un ordenador cuántico con la suficiente potencia se podrían ejecutar algoritmos cuánticos conocidos con impacto en la protección de datos y comunicaciones digitales como por ejemplo el algoritmo de Grover y el algoritmo de Shor.

El algoritmo de Grover, publicado en 1996, permite realizar una búsqueda en una secuencia no ordenada de datos con N elementos en un tiempo $O(\sqrt{N})$, mientras que el mismo problema con un ordenador clásico, la búsqueda se realizaría en un tiempo O(N). Por ejemplificar, si buscáramos en un conjunto de datos (no ordenados) de 1 millón de elementos con un algoritmo clásico se requeriría 1 millón de operaciones, mientras que, utilizando el algoritmo de Grover en un ordenador cuántico, sólo se requerirían 1000 operaciones, bastante más rápido que los algoritmos clásicos de búsqueda.

El algoritmo de Shor, publicado en 1994, permite factorizar un número N en tiempo O ((log N)3) en un ordenador cuántico, sustancialmente más rápido que usando la criba general del cuerpo de números (GNFS, por sus siglas en inglés) que tiene una complejidad subexponencial, y es el algoritmo más rápido conocido hasta la fecha para este tipo de problema.

¿Qué consecuencias tendrán estos algoritmos a la criptografía que hoy conocemos?

El algoritmo de Grover afectará a la criptografía simétrica (algoritmos de cifrado simétrico como AES y funciones hash) ya que reducirá su nivel de seguridad a la mitad. La solución será aumentar el tamaño de las claves o la salida de las funciones hash al doble del tamaño actual (actualmente

se están estudiando más restricciones adicionalmente el aumento del tamaño de bloque o clave). Así, por ejemplo, si en la actualidad tenemos una clave AES de 128 bits, la seguridad en bits de la clave con la presencia de un ordenador cuántico que ejecute el algoritmo de Grover sería de 64 bits, por lo que incrementando el tamaño de clave a 256 bits se obtendría una seguridad de 128 bits, igual a la actual sin la presencia de un adversario cuántico.

Esto no sucede así con el algoritmo de Shor, que tiene unas consecuencias devastadoras en la criptografía asimétrica que conocemos a día de hoy: todos los algoritmos serían rotos con la presencia de un adversario cuántico que ejecutara el algoritmo de Shor. Así pues, algoritmos como RSA, la criptografía de curva elíptica, los criptosistemas basados en el problema del logaritmo discreto como Diffie-Hellman o DSA quedarían obsoletos y no serían seguros. La estimación actual, por ejemplo, para romper un RSA-2048 bits recae en unos pocos miles de qubits "de calidad" (algo muy alejado todavía de los ordenadores cuánticos actuales) y unos cientos de millones de puertas lógicas en la construcción del ordenador.

1.5.2 Marco conceptual

Monedero virtual[5]:

Para almacenar toda ciptomoneda se necesita de una clave privada a la cual se asocia una cantidad determinada de dicha moneda. Pues bien, para este tipo de almacenaje se usa un software o dispositivo específico al que llamamos monedero o cartera (wallet).

Este monedero te permite almacenar y operar con esas monedas de manera que se pueda transferir a otras personas, recibir de otras personas o almacenarlas.

Criptomoneda[6]:

Las criptomonedas son un tipo de moneda digital, que son aquellas que no existen de forma física, pero que sirven como moneda de intercambio, permitiendo transacciones instantáneas a través de Internet y sin importar las fronteras.

[5] "¿Qué es un monedero o cartera virtual?" Diciembre 29, 2017 http://www.blockchainservices.es/novedades/que-es-un-monedero-o-cartera-virtual/
[6] "Criptomoneda" https://economipedia.com/definiciones/criptomoneda.html

Computación cuántica[7]:

es un paradigma de computación distinto al de la informática clásica o computación clásica. Se basa en el uso de cúbits, una especial combinación de unos y ceros. Los bits de la computación clásica pueden estar en 1 o en 0, pero solo un estado a la vez; en tanto el cúbits puede tener los dos estados simultáneos también. Esto da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.

Criptografía[8]:

Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

Blockchain[9]:

La cadena de bloques, más conocida por el término en inglés blockchain, es un registro único, consensuado y distribuido en varios nodos de una red. En el caso de las criptomonedas, podemos pensarlo como el libro contable donde se registra cada una de las transacciones.

1.6 HIPÓTESIS CONCEPTUAL

La implementación del paradigma de la computación y supremacía cuántica asegura teóricamente, que se puede acceder a un monedero virtual en segundos, utilizando las técnicas de criptografía tradicionales y la estadística.

[7] "Computación cuántica: qué es, de dónde viene y qué ha conseguido" 1 marzo 2019, https://economipedia.com/definiciones/criptomoneda.html

[8] "¿Qué es la Criptografía?" 10 de febrero de 2020, https://www.tecnologia-informatica.com/que-es-la-criptografia/

[9] "

Blockchain: qué es, cómo funciona y cómo se está usando en el mercado" 4 Sep. 2018, https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

1.7 ASPECTOS METODOLÓGICOS

1.7.1 Tipo de estudio

Nivel de profundidad: Descriptivo.

1.7.2 Método de investigación

El método que se va a utilizar para realizar la investigación es el método de análisis.

1.7.3 Fuentes y técnicas para la recolección de la información

El proyecto analizará información basada en documentación, noticias y artículos de fuentes como grupos de investigación, empresas de tecnología, expertos y prensa, que se recopilaran mediante técnicas físicas como periódicos, revistas, libros y técnicas virtuales como el internet.

1.7.4 Tratamiento de la información

La información será clasificada y presentada mediante tablas, diagramas, graficas, etiquetas, referencias y será de acceso público.

1.8 CRONOGRAMA

Se propone para el desarrollo del proyecto 24 semanas en las cuales se realizarán las actividades mencionadas a continuación y su duración:

			Semanas																								
Tarea	Inicio	Fin	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Recopilación y clasificación de información	30/11/2020	27/12/2020																								
Analisis de información	28/12/2020	24/01/2021																								
Selección de metodos criptograficos	25/01/2021	14/02/2021																								
Selección de tecnicas estadisticas	15/02/2021	07/03/2021																								
Identificación de avances cuanticos en la criptografia seleccionada.	08/03/2021	22/03/2021																								
Analisis de la estrucutura de un monedero virtual.	23/03/2021	04/04/2021																								
Identificación de herramientas a utilizar.	05/04/2021	25/04/2021																								
Proyección de resultados con la implementacion de la herramienta seleccionada.	26/04/2020	17/05/2021																								
Conclusiones y verificación de la hipotesis.	18/05/2020	24/05/2021																								

Ilustración 1 - Cronograma general del proyecto

PARTE 2. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

CAPÍTULO 2. DESARROLLO DE LA INVESTIGACIÓN

2.1 MONEDERO VIRTUAL

2.1.1 ¿Qué es?

> El término wallet hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de nuestras criptomonedas. [10]

Permite enviar y recibir criptomonedas a través de la red Blockchain, almacenar las que quieras y controlar siempre que quieras tu saldo.

2.1.2 ¿Cómo funciona? [11]

Las criptomonedas son registros de transacciones contenidos dentro de una blockchain que es operada por nodos interconectados entre sí alrededor de todo el mundo. Entonces, las claves públicas y, sobre todo, las claves privadas dentro de una wallet son las que nos dan la propiedad y derecho sobre las criptomonedas transferidas a una dirección en particular. [12]

- ✓ La clave pública es similar a un número de cuenta bancaria. Podemos entregarla a cualquier persona para que nos envíe dinero, sin el riesgo de que pueda extraer nuestros fondos. A través de la clave pública se generan direcciones para recibir, consultar y ver el estado de nuestros fondos.

- ✓ La clave privada funciona como una especie de llave, un PIN o contraseña que no debemos revelar a nadie, ya que nos otorga el derecho de gastar las criptomonedas contenidas en una dirección. Así, el propietario de la clave privada será el propietario de los fondos y tendrá total control sobre ellos.

Cuando alguien envía por ejemplo un Bitcoin, está enviado un valor en forma de transacción, transfiriendo una propiedad al destinatario. Para que la wallet registre el ingreso y el destinatario pueda usar su Bitcoin, las

---

[10] Bit2Me, ¿Qué es una wallet o monedero de criptomonedas? [En línea]. Disponible en: https://academy.bit2me.com/wallet-monederos-criptomonedas/ [Accedido: 18–Enero-2021]

[11] Bitcobie, Qué es una Wallet y cómo se crea [En línea]. Disponible en: https://www.bitcobie.com/wallet/ [Accedido: 20–Enero-2021]

claves privadas deben de coincidir con la dirección a la que se envió la moneda.

La propiedad y la conservación de tus claves privadas te otorga un control absoluto sobre los fondos que estén asociados a tus claves públicas.

2.1.3 Tipos de monederos

Cold Wallets

Son monederos o carteras digitales donde puedes almacenar y gestionar tu dinero en este caso, criptomonedas. Así las cold wallets, son aquellas que utilizan claves generadas por una fuente que no está conectada a la blockchain y, por tanto, tampoco a Internet. Por lo que se denominan monederos en frío.

Este tipo de wallet ofrece una enorme ventaja sobre las demás, ya que hacen el rol de una cuenta bancaria de ahorros. Donde podemos guardar dinero que no utilizaremos durante algún tiempo. Son las más empleadas por los usuarios para depositar y resguardar grandes cantidades de criptomonedas y, ofrecen un nivel de seguridad insuperable.

Las cold wallets al no estar en conexión constante con Internet no son propensas a sufrir de ataques de hackeo o robo de claves como el caso de las hot wallets. No obstante, sí existe el riesgo de perder el dinero si se extravía el hardware o papel que las contiene[13].

Paper Wallet[14]

Se trata de un monedero impreso en papel que contiene las claves privadas y direcciones para gestionar las criptomonedas. Fueron muy populares durante el 2011 con el auge de Bitcoin, ya que ofrecen un nivel de seguridad off-line y almacenamiento en frío. Por lo que no son propensas al robo cibernético; y de forma obvia, tampoco son propensas a ataques de virus y malware pues se trata de un papel.

Las paper wallets son ideales para el almacenamiento y resguardo de fondos que no van a ser utilizados o movidos en mucho tiempo. Así, pueden emplearse como resguardo de valor y ahorro. No obstante, se debe conocer detalladamente

[13] Bit2Me, ¿Qué son las Cold Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-cold-wallets/ [Accedido: 4–Febrero-2021]
[14] Bit2Me, ¿Qué son las paper wallets o monederos de papel? [En línea]. Disponible en: https://academy.bit2me.com/monedero-papel-bitcoin-paper-wallet/ [Accedido: 6–Febrero-2021]

cómo funcionan y cómo gestionarlas para no cometer errores que puedan afectar la integridad de nuestros fondos.

Este tipo de monederos son muy fáciles de crear. Se debe acceder a un generador de paper wallet y generar una clave privada. Una vez esto, se elige la opción de imprimir paper wallet y cuántas copias de seguridad desee. Es importante mencionar que estas wallets pueden ser cifradas antes de ser impresas, lo que le proporciona una mayor protección.

Pero también es importante aclarar que, el concepto “paper wallet” puede ser extrapolado a otros materiales, no sólo papel. Por ejemplo, se puede generar la semilla con las medidas de seguridad anteriormente explicadas y, en vez de imprimirla en papel, grabarla en una placa de metal de larga duración.



Ilustración 2- Billetera o monedero virtual de papel[15]

Hardware Wallets[16]

Son dispositivos físicos que operan como monederos sin conexión a Internet y mantienen las claves privadas almacenadas de forma segura dentro de ellos. Esto es lo que se conoce como Hardware Wallets, que también forman parte de las Cold Wallets por su condición de almacenamiento en frío, al no permanecer conectadas a la blockchain o al internet.

Se tratan de dispositivos diseñados especialmente para este objetivo, pequeñas unidades HSM (Módulos Hardware de Seguridad, en inglés) con seguridad de grado militar que

[15] Bit2Me, Billetera de papel [En línea]. Disponible en: https://academy.bit2me.com/wp-content/uploads/2019/12/bitcoin-armory-paper-wallet-steel.webp [Accedido: 23–Febrero-2021]
[16] Bit2Me, ¿Qué son las Hardware Wallets? [En línea]. Disponible en: https://academy.bit2me.com/hardware-wallets/ [Accedido: 25–Febrero-2021]

permiten generar claves privadas y que estas nunca salgan del dispositivo. Además, si el dispositivo intenta ser manipulado físicamente con el objetivo de acceder a sus claves privadas, este se “suicida” eliminando por completo las claves.

Estas representan una de las opciones más seguras y cómodas del mercado a la hora de almacenar en frío grandes cantidades de criptomonedas. Esto por el hecho de que protegen la seguridad de las claves privadas dentro de sí, pero permiten ser utilizados cómodamente, normalmente vía USB. La mayoría de ellas emplea una especie de chip de seguridad donde se retienen las claves y no se pueden transferir jamás fuera del dispositivo.



Ilustración 3 - Billetera o monedero virtual Hardware[17]

Hot Wallets[18]

Almacenan las claves privadas en lugares que siempre están conectados a Internet.

Es un tipo de wallet muy común, ampliamente utilizado para el almacenamiento y gestión de las criptomonedas. Su principal utilidad es que ofrece un rápido y cómodo acceso a los fondos debido a su constante conexión a internet. Sin embargo, esto representa también un mayor riesgo comparadas con otros tipos de wallets. Por ejemplo, un ciberdelincuente podría traspasar la seguridad del dispositivo donde se utiliza la wallet y robar las claves privadas, con ello los

[17] Bit2Me, Billetera de hardware [En línea]. Disponible en: https://academy.bit2me.com/wp-content/uploads/2019/12/hadware-wallets-y-sus-distintos-modelos-y-marcas.webp [Accedido: 1–Marzo-2021]
[18] Bit2Me, ¿Qué son las Hot Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-hot-wallets/ [Accedido: 3–Marzo-2021]

fondos. Es por esta razón, que no se recomienda manejar grandes cantidades de dinero digital en Hot Wallets.

Pese a esto, las hot wallets son una muy buena opción, debido a su comodidad de uso, para manejar criptomonedas en el día a día para cantidades relativamente pequeñas.

- **Desktop (de escritorio)**

  Software descargados e instalados en ordenadores. Están diseñados para recibir y gestionar criptomonedas ofreciendo mayores niveles de seguridad en comparación con otras hot wallets. Aunque si por algún motivo el ordenador es hackeado se corre el riesgo de perder todos los activos.

- **Smartphone (teléfonos móviles)**

  Las wallets móviles son aplicaciones instaladas en los teléfonos inteligentes. Aunque disponen de un espacio mucho más limitado que las de ordenador. Estas nos permiten una mayor facilidad de uso debido a que pueden ser empleadas desde cualquier lugar, por lo que son ideales para realizar operaciones del día a día.

- **Online (en línea)**

  Estas wallets son servicios que ofrecen las webs sin necesidad de descargar ni instalar ninguna aplicación. Funcionan directamente en línea como su nombre lo indica. Su mayor ventaja es que facilita realizar una operación desde cualquier parte del mundo que cuente con internet. Sin embargo, para operarlas en su mayoría, es necesario ceder las claves privadas a un tercero, lo que implica confiar los fondos a otra persona. En temas de seguridad no es recomendable.

2.1.4 Desarrollo de monederos[19]

El diseño de una billetera o monedero virtual debe tener los siguientes elementos:

- Registro
- Perfil

[19] SPRO, How to Develop a Bitcoin Wallet App? [En línea]. Disponible en: https://s-pro.io/blog/how-to-develop-a-bitcoin-wallet-app [Accedido: 15–Marzo-2021]

- Escáner de código QR
- Tasa de cambio en el mercado
- Servicio de compra y venta de criptomonedas
- Generación de direcciones
- Seguimiento de pagos en tiempo real
- Notificaciones
- Seguridad

La seguridad es el factor en el cual se debe contemplar mayor detalle, se sugiere cifrar la billetera con una contraseña, al igual que crear copias y guardarla en lugares seguros.

Actualmente existen las siguientes librerías para poder desarrollar una billetera o monedero virtual:

Blockchain Bitcoin wallet:

Debido a un conjunto completo de API gratuita, la billetera Blockchain Bitcoin está de moda entre los desarrolladores. Es compatible con muchas plataformas, incluye muchos lenguajes de programación y es gratuito.
Tiene una excelente documentación, por lo que los desarrolladores pueden crear rápidamente sus billeteras pasando por todas las etapas de construcción de su funcionalidad.

Coinbase SDK

Es una librería Java multiplataforma, que admite plataformas como Android e iOS y funciona con Ruby, Java, Python y otros lenguajes de programación. Está diseñado no solo para Bitcoin sino también para las monedas Ethereum y Litecoin.

BitcoinJ SDK

Es una librería de Bitcoin multiplataforma, que admite plataformas Android y Windows y se puede usar desde cualquier lenguaje compatible con JVM como C ++, JavaScript, Python, etc.

2.1.5 Semilla maestra[20]

Las Hierarchical Deterministic Wallets o como se conocen comúnmente HD Wallets, son monederos de criptomonedas que emplean una única semilla de 12, 18 o 24 palabras claves, con la que pueden generar un número ilimitado de direcciones. Esto se realiza de forma automática,

[20] Bit2Me, ¿Qué son las HD Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-las-hd-wallets/ [Accedido: 27–Marzo-2021]

jerárquica y secuencial. No obstante, recordar la semilla es un tanto complicado ya que se trata de una cadena de caracteres alfanuméricos ilegibles, por ello, se usan los códigos mnemotécnicos. Que convierten esta semilla en palabras entendibles para nosotros, por lo que realizar una copia de seguridad es mucho más fácil y práctico.

Así, la implementación de este tipo de wallets resuelve la problemática presentada al inicio de tener que realizar tantas copias de seguridad y generar direcciones manualmente. Ahora con las HD Wallets solo es necesario que se haga un respaldo de la semilla, que está basada en un Protocolo de Mejora de Bitcoin (BIP), conocido como el BIP 32.
https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

Matemáticamente, el BIP 32 le permite a la wallet generar, a partir de la semilla, una estructura jerárquica de claves privadas en forma de árbol. Así, cuando un dispositivo se pierda o dañe, es posible restaurar la wallet con todas las claves privadas del árbol, y por supuesto con todos los fondos, con la copia de seguridad de la semilla.

2.1.6 Formatos de billeteras[21]

Wallet.dat:

El archivo wallet.dat contiene las claves privadas, claves públicas, scripts (que corresponden a direcciones), metadatos clave (por ejemplo, etiquetas) y las transacciones relacionadas con su billetera. Si tiene una billetera HD, también incluye la semilla HD y las rutas de derivación para cada clave privada.

Contiene:

Pares de claves para cada una de sus direcciones
Transacciones realizadas desde / hacia sus direcciones
Preferencias del usuario
Llave predeterminada
Llaves reservadas
Cuentas
Un número de versión
Grupo de claves
Información sobre la mejor cadena actual, para poder volver a escanear automáticamente al restaurar desde una copia de seguridad.

[21] Bitcoin, Wallet [En línea]. Disponible en: https://en.bitcoin.it/wiki/Wallet [Accedido: 1–Abril-2021]

2.1.7 Servicios de monederos (Empresas)

Paper wallets:
- BitAddress
- Bitcoin.com
- Walletgenerator.net
- Generatepaperwallet

Hardware wallets:
- Trezor
- Ledger
- KeepKey
- Blockchain Lockbox
- Archos

Desktop (de escritorio):
- Electrum
- Exodus
- Bitcoin Core

Smartphone (teléfonos móviles):
- Electrum
- Mycelium
- Coinomi
- Trust Wallet

Online (En linea):
- BitGo
- Blockchain.com
- Bit2Me Wallet

2.2 ALGORITMOS DE ENCRIPTACIÓN

2.2.1 SHA-256[22]

Las siglas SHA-256 hacen mención a la función hash que ha sido elegida para el funcionamiento de muchas criptomonedas pues ofrece un alto nivel de seguridad, lo que la hace perfecta para la tarea de proteger y codificar de forma segura la información de las mismas.

Este es un algoritmo de hash que es usado por Bitcoin para garantizar la integridad de la información almacenada en un bloque, entre otras cosas.

[22] Bit2Me, Criptografia SHA-256 [En línea]. Disponible en: https://academy.bit2me.com/wp-content/uploads/2019/10/Criptography_SHA_256_es.pdf [Accedido: 3–Abril-2021]

Como casi todos los avances en materia de criptografía, los gobiernos del mundo han tenido un papel fundamental debido a las guerras. El algoritmo SHA o Secure Hash Algorithm (Algoritmo de Hash Seguro), es uno de estos avances. Este algoritmo criptográfico fue desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y el National Institute of Standards and Technology (NIST). Su objetivo es generar hashes o códigos únicos en base a un estándar con el que se pudieran asegurar documentos o datos informáticos frente a cualquier agente externo que desee modificarlos. Este algoritmo fue y es un gran avance en el camino a garantizar la privacidad del contenido en el procesamiento de información.

Características:

- ✓ Funciona en una sola dirección: esto quiere decir que de cualquier contenido podemos generar su hash (su "huella dáctilar digital") pero de un hash no hay forma de generar el contenido asociado a él.

- ✓ Es uno de los más usados por su equilibrio entre seguridad y coste computacional de generación.

- ✓ La longitud del hash resultante es siempre igual, no importa lo extenso que sea el contenido que uses para generar el hash.

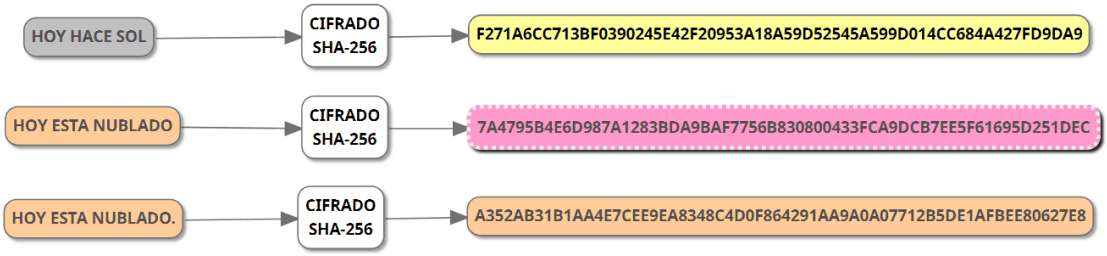


Ilustración 4 - Cifrado SHA-256[23]

Mensaje M o datos de entrada:

Es la información que procesará la función SHA-256 para calcular el digest o hash correspondiente. M puede tener longitud variable1, puede ser un archivo, una cadena de texto como" Hola mundo" e incluso una cadena vacía, obteniendo como resultado una cadena ω de 256 bits de longitud expresada en 64 caracteres hexadecimales o base 16.

[23] Bit2Me, Hash criptográfico [En línea]. Disponible en: https://academy.bit2me.com/wp-content/uploads/2018/08/hash-criptografico.webp [Accedido: 15–Abril-2021]

¿Se puede descifrar la clave del SHA-256?[24]

Romper un algoritmo SHA, implica, por definición encontrar dos mensajes m1 y m2, diferentes, de tal manera que sus funciones hash sean idénticas, de esta manera:

sha-256(m1) = sha-256(m2)

Entonces si es teóricamente posible, asumiendo que tienes suficiente tiempo, suficiente dinero y por tanto suficientes recursos de cómputo.

2.2.2 AES-256[25]

Actualmente hay tres tipos de cifrado AES: 128 bits, 192 bits y 256 bits, donde este último es el más seguro. Esto se diseñó en base a la Ley de Moore, ya que las primeras pruebas demostraron que, en un tiempo relativamente corto, la potencia de los procesadores podría romper el cifrado más débil en periodos de tiempo cada vez menores.

Por ello, aunque se empezó con 56 bits, rápidamente se cambió a los tres tipos nombrados para hacerlo más seguro. Advanced Encryption Standard o AES tiene una ventaja bastante clara frente a otros competidores: tiene una naturaleza abierta, lo cual significa que se puede usar tanto en lo público como en lo privado, sea para fines comerciales o no.

Además, es un sistema de clave simétrica, lo cual le otorga una mayor seguridad, ya que la clave usada debe ser conocida para el cifrado como para el descifrado y tanto emisor como receptor necesitan una copia de la llave correspondiente. Esto tiene una importante ventaja en el rendimiento de un sistema de cifrado, ya que como se obliga a remitente y destinatario a saber la clave, se requiere menos potencia computacional para hacer viajar la información puesto que siempre va segura.

Todo se basa en bloques, concretamente bloques de 128 bits los cuales se dividen en una matriz de cuatro por cuatro con 16 bytes. Ocho bits por byte nos dan los 128 bits mencionados y por ello al cifrar la información no se altera el tamaño de la misma gracias a las matrices. AES es un sistema de sustitución y permutación, por lo que es altamente seguro gracias a que la clave inicial sirve para generar unas claves nuevas.

---

[24] Quiora, ¿Es posible romper una SHA-256? [En línea]. Disponible en: https://es.quora.com/Es-posible-romper-una-SHA-256 [Accedido: 18–Enero-2021]

[25] Hardzone, Así funciona el sistema de cifrado AES-256 bits, ¿es realmente seguro? [En línea]. Disponible en: https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/ [Accedido: 10–Abril-2021]

Cada byte de datos se sustituye por otro mediante una tabla predeterminada para a continuación coger cada matriz 4×4 y moverla de la siguiente manera: los bytes de la segunda fila se mueven un espacio a la izquierda, los bytes en la tercera fila se mueven dos espacios y los bytes de la cuarta se mueven tres para finalmente mezclar las columnas y añadir la clave inicial al conjunto y vuelta a empezar.

Esto genera un texto cifrado que nada tiene que ver con el original y que para descifrarlo se requiere hacer los pasos inversos conociendo previamente dicha clave. Entre los tres tipos de cifrados AES la única diferencia es precisamente la longitud de la clave, por lo que si comparamos 128 bits con 256 bits tendremos una clave el doble de larga en este último.

¿Se puede romper el AES-256?

El cifrado de 256 bits hasta donde sabemos sigue inexpugnable y aunque ha habido intentos con AES-128 bits, intentar romper una clave 256 bits requiere **2128 veces más potencia de cómputo por fuerza bruta**, ya que estamos hablando de pasar de $\mathbf{2^{128}}$ posibles valores a $\mathbf{2^{256}}$ **posibles valores.**

El tiempo para descifrar una sola clave sería **más del doble de la edad total del universo.**

2.3 PSICOLOGIA DE LAS CONTRASEÑAS[26]

Hacemos las cosas por alguna razón: elegir coche, destino de vacaciones, carrera universitaria, incluso la contraseña. Detrás de cada combinación más o menos aleatoria de letras, números y caracteres hay una historia que merece la pena contar.

Detrás hay todo tipo de anécdotas, centradas en un mismo objetivo: **el recuerdo**.

Ejemplos:

“**asdfghASDFGH**”
Sencilla pero fácil de recordar.
Cuanto más se complique la clave para contrarrestar ataques informáticos, más difícil será memorizarla.

“**JamonConQueso**”

[26] El Diario, Dime tu contraseña y te diré quién eres: hay una historia fascinante en cada clave [En línea]. Disponible en: https://www.eldiario.es/hojaderouter/seguridad/contrasenas-seguridad-psicologia-historias_1_4271346.html [Accedido: 12–Abril-2021]

Uso de mayúsculas de forma intercalada con un significado en particular. El uso de múltiples contraseñas en distintos sitios hace que las personas tarden hasta 3 o 4 intentos en recordar, generando bloqueos en los sitios.

Historias de amor y desamor:
"**Carlitos**"
Nombre de la persona que le gustaba.
"**frances**"
Nacionalidad de la persona que le gustaba.
"**Jorgibiris**"
Apodo del hermano menor quien se llama Jorge.

Las personas suelen variar sus contraseñas si el sitio solicita mayúsculas, caracteres numéricos y demás, pero **siempre** sobre la misma base.

Se suelen utilizar temáticas como:

- Matrículas de vehículos
- Pensamientos oscuros
- Lugares
- Fechas importantes
- Momentos especiales
- Direcciones
- Etc.

2.3.1 Escritura Leet[27]

Intercambio de letras por números (Leet):

O por 0
A por 4
I por 1
E por 3
G por 6
S por 5
Etc.
Ejemplo: "**C0l0mb14**"

Se estima que tardamos unos 150-200 milisegundos en identificar una palabra completa entre los miles de patrones que tenemos almacenados, y en este proceso nuestro sistema cognitivo normaliza la información sensorial, de manera que puede identificar rápidamente un número que se parece a una letra. De esta forma, cuando vemos una palabra como M4T3R14L inmediatamente se activa el significado de MATERIAL.

[27] Magnet, Poder leer P4L4BR4S con NÚM3R05 no es tan difícil como creías, todo está en tu cerebro [En línea]. Disponible en: https://magnet.xataka.com/un-mundo-fascinante/poder-leer-p4l4br4s-con-num3r05-no-es-tan-dificil-como-creias-todo-esta-en-tu-cerebro [Accedido: 12–Abril-2021]

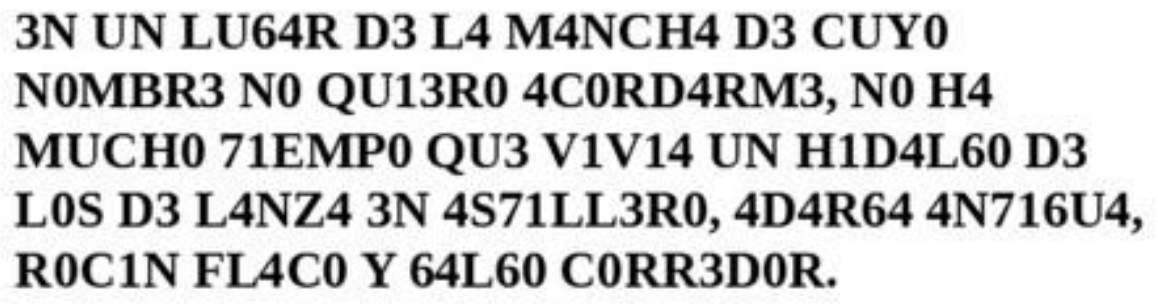


Ilustración 5- Ejemplo Leet[28]

¿Qué nos puede llevar a utilizar una u otra contraseña?

Según el psicólogo social Guillermo Fouce, estudiando las contraseñas antiguas o nuevas "se pueden obtener algunos de **los hábitos o de los gustos** o algunas de las **fechas que son importantes** para esa persona. Se puede también saber si repite siempre la misma o si va modificando distintas contraseñas en función del tipo de tema "
La mayoría de contraseñas están relacionadas con momentos felices o neutros de la vida, pero ¿**es posible asociar recuerdos negativos a las contraseñas?**

Fouce menciona que es habitual hallar el **nombre de mascotas que fallecieron** en la secuencia de caracteres.
¿Esto nos hace bien? "Depende de cada caso", matiza. "En el caso de los duelos, de que alguien haya fallecido, **la cuestión está en que eso no marque tu vida**. Si es una cuestión de mero recuerdo, no debería ser un problema ni es patológico".

2.3.2 Personalidades detrás de las contraseñas

La psicóloga **Helen Petrie**[29], de la Universidad de Londres, realizó una investigación con 1.200 personas para intentar descubrir qué personalidades había detrás de las contraseñas. Identificó cuatro grupos:

- ✓ **Orientados a la familia:** Aquellos cuya contraseña se basaba en su propio nombre o apodo, en el de la mascota o en una fecha de nacimiento (es decir, "con valor emotivo").

[28] Escritura Leet [En línea]. Disponible en: https://i.blogs.es/aac1f5/captura-de-pantalla-321-/1366_2000.jpg [Accedido: 17–Abril-2021]
[29] Psychology Today, Passwords reveal your personality [En línea]. Disponible en: https://www.psychologytoday.com/intl/articles/200201/passwords-reveal-your-personality [Accedido: 18–Abril-2021]

- ✓ **Fans:** Contraseñas con nombres de atletas, cantantes, equipos de fútbol… Son jóvenes y se quieren identificar con el estilo de vida de estas celebridades.
- ✓ **Fantaseadores:** Se imaginan que son más atractivos o altos de lo que son en realidad: 'sexy', 'semental'...
- ✓ **Crípticos:** Contraseñas verdaderamente difíciles de reconocer.

2.4 ESPECIFICACIÓN DE CONTRASEÑAS

Es indispensable conocer las características referentes a las contraseñas que son solicitadas por cada uno de los sistemas o hardware mencionados anterior mente, para esto se realizó una investigación en las páginas oficiales y se pudo determinar lo siguiente:

			¿Caracteres obligatorios?			
Billetera	Tipo de billetera	Longitud Minima	Numeros	Mayusculas	Minusculas	Especiales
BitAdress	Papel	15	No	No	No	No
Walletgenerator.net	Papel	15	No	No	No	No
Trezor	Hardware	6	Si	No	No	No
Ledger	Hardware	4	Si	No	No	No
KeepKey	Hardware	4	Si	No	No	No
Electrum	Escritorio - Movil	8	Si	Si	Si	No
Exodus	Escritorio	6	Si	Si	Si	No
Bitcoin Core	Escritorio	4	Si	Si	Si	Si
Mycelium	Movil	4	Si	Si	Si	Si
Coinomi	Movil	5	Si	Si	Si	Si
Trust Wallet	Movil	8	Si	Si	Si	Si
BitGo	Online	8	Si	Si	Si	Si
Blockchain.com	Online	8	Si	Si	Si	Si
Bit2Me Wallet	Online	8	Si	Si	Si	Si

Ilustración 6 - Especificación de contraseñas en las billeteras virtuales

2.5 TECNICAS

2.5.1 Permutaciones[30]

La permutación es una técnica de conteo que permite calcular las posibles ordenaciones de los elementos de un conjunto o número de elementos del espacio muestral de un experimento aleatorio. En esta técnica de conteo se considera que existe el orden en la muestra, pero no es posible repetir ningún elemento de la población en su conformación.

[30] La Arena, Pemrutaciones [En línea]. Disponible en: https://danacaweb.com/permutaciones.html [Accedido: 30–Abril-2021]

Dado un experimento aleatorio con una población N y una muestra n, si en la muestra existe orden, pero no repetición, el número de elementos del espacio muestral corresponde a la permutación de n en N, la cual se simboliza N^{P_n} y se define como:

$$N^{P_n} = \frac{N!}{(N-n)!}$$

Donde, n! = n x (n - 1) x (n - 2) x ... x 2 x 1, y 0!=1

2.5.2 Combinaciones[31]

Una combinación es un arreglo donde el orden NO es importante. La notación para las combinaciones es C(n,r) que es la cantidad de combinaciones de “n” elementos seleccionados, “r” a la vez. Es igual a la cantidad de permutaciones de “n” elementos tomados “r” a la vez dividido por “r” factorial. Esto sería P(n,r)/r! en notación matemática.

Ejemplo: Si se seleccionan cinco cartas de un grupo de nueve, ¿cuantas combinaciones de cinco cartas habría?

La cantidad de combinaciones posibles sería: P(9,5)/5! = (9*8*7*6*5)/(5*4*3*2*1) = 126 combinaciones posibles.

2.5.3 Diccionario de datos[32]

Un diccionario de datos corresponde a fuentes de información en diferentes tipos de formatos ya sean texto, bases de datos, archivos, etc. que contiene una seria de claves o contraseñas precargadas consideradas débiles o de fácil predicción que pueden servir como insumo inicial.

Estos diccionarios de datos son utilizados por empresas de seguridad informática con el objetivo de verificar que tan seguras son las contraseñas que utilizan las personas o empleados de una empresa.

A continuación, se puede observar un ranking de las 25 contraseñas más comunes en el mundo por año:

[31] AAA Math, Combinaciones [En línea]. Disponible en: https://www.aaamatematicas.com/sta-combin.htm [Accedido: 1–Mayo-2021]
[32] GitHub, Diccionarios de: usuarios, passwords, xss, dorks [En línea]. Disponible en: https://github.com/hackingyseguridad/diccionarios [Accedido: 1–Mayo-2021]

Rank	2011	2012	2013	2014	2015	2016	2017	2018
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

Ilustración 7 - Especificación de contraseñas en las billeteras virtuales[33]

2.5.4 TarGuess[34]

Investigadores de las universidades Lancaster, Peking y la Fujian Normal University han trabajado de forma coordinada para dar con un sistema que es capaz de acertar las contraseñas con un 73% de posibilidades de éxito.

Investiga la actividad en la red, cómo se llaman sus familiares, su mascota, dónde ha pasado sus vacaciones, combinando estos datos comienza el juego de las combinaciones y con él se elevan las posibilidades de acertar.

El equipo ha replicado esta sistemática empleando modelos matemáticos con los que se ponen cifras a su eficacia: 73% de éxito en contraseñas convencionales, y un llamativo 32% en aquellos casos en los que el usuario se ha esforzado por lograr una contraseña sofisticada. El gran reto al que se enfrentó el equipo fue lograr dar con las combinaciones

[33] GitHub, Top contraseñas [En línea]. Disponible en: https://github.com/hackingyseguridad/diccionarios/blob/master/25pass.png [Accedido: 03–Mayo-2021]
[34] El Pais, Este sistema adivina las contraseñas (y casi no falla) [En línea]. Disponible en: https://elpais.com/tecnologia/2016/11/09/actualidad/1478694955_288239.html [Accedido: 05–Mayo-2021]

adecuadas antes de que el servidor bloquee la cuenta (como medida de seguridad ante los ataques por fuerza bruta). Pero es aquí donde entran en juego los algoritmos de TarGuess.

La principal conclusión de este proyecto por parte del equipo es que los sistemas de seguridad empleados en la actualidad no son suficientes ante un ataque organizado basado en algoritmos y esperan concienciar a los usuarios acerca de la importancia de escoger contraseñas sofisticadas.

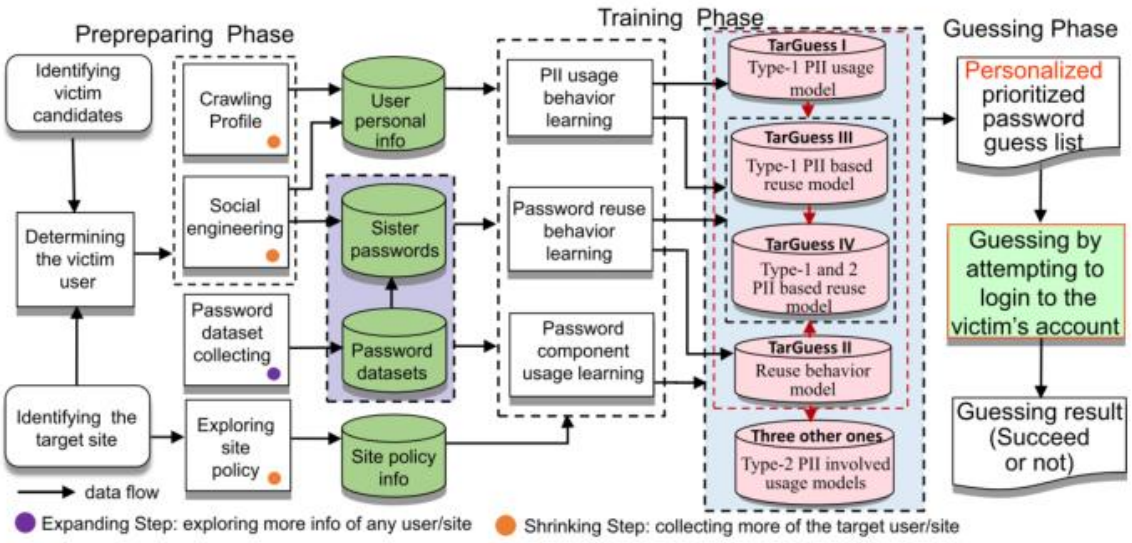


Ilustración 8 - Arquitectura de TarGuess[35]

2.6 HERRAMIENTAS DISPONIBLES PARA DESENCRIPTAR

2.6.1 My wallet backup decryption tool

Es una herramienta desarrollada por Blockchain.com y tiene como objetivo poder des encriptar una billetera virtual.

Los parámetros de entrada son:

- ✓ Archivo wallet encriptado.
- ✓ Contraseña principal.

Respuesta:

- ✓ Mensaje de éxito o fallo
- ✓ En caso de éxito, visualizar en claro la billetera virtual.

Desarrollado en lenguaje **JavaScript**, no requiere conexión a internet, no tiene límite de intentos y es de código abierto.

[35] AdictTec, Arquitectura Terguess [En línea]. Disponible en: https://adictec.com/wp-content/uploads/2016/11/TarGuess.png [Accedido: 09–Mayo-2021]

La herramienta puede ser descargada de la siguiente dirección, allí se detallan los pre requisitos, la forma de instalación y uso.:

https://github.com/blockchain/my-wallet-backup-decryption-tool

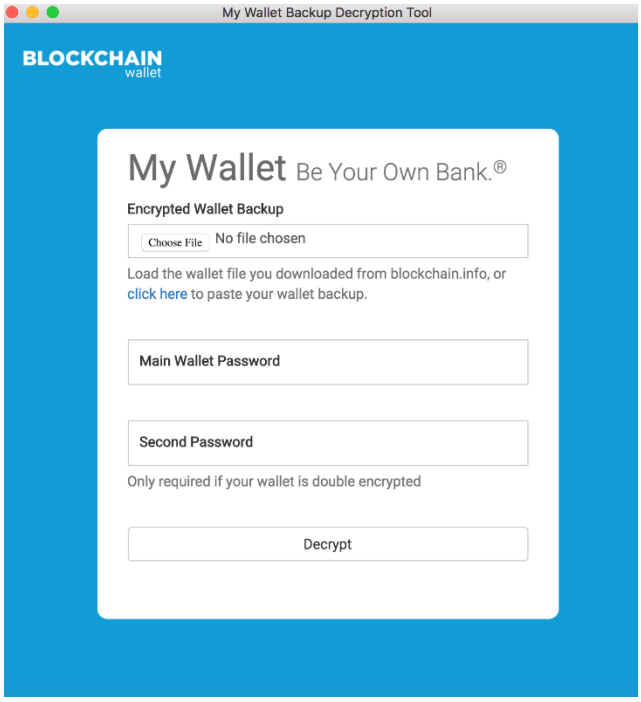


Ilustración 9 - Interfaz gráfica de My Wallet backup decryption tool[36]

2.6.2 Btcrecover[37]

Es una herramienta de recuperación de semillas y contraseña de billetera de código abierto.

Para la recuperación basada en semillas, esto es principalmente útil en situaciones en las que ha perdido/olvidadas partes de su mnemónico o ha cometido un error al transcribirlo. (Recibe un error de que su semilla no es válida)

Para recuperar la contraseña de la billetera o la frase de contraseña, es principalmente útil si tiene una idea razonable sobre cuál podría ser su contraseña.

---

[36] BTCRecover, Getting Started [En línea]. Disponible en: https://user-images.githubusercontent.com/16043809/31572618-431d2002-b0a2-11e7-8e23-7ca58a5598cb.png [Accedido: 9–Mayo-2021]

[37] BTCRecover, Getting Started [En línea]. Disponible en: https://btcrecover.readthedocs.io/en/latest/ [Accedido: 6–Mayo-2021]

Esta herramienta se encuentra desarrollada en lenguaje Python.

La herramienta puede ser descargada e instalada desde la siguiente dirección:

https://btcrecover.readthedocs.io/en/latest/INSTALL/

2.7 COMPUTACIÓN CUANTICA[38]

2.7.1 Avances generales

Principios de la teoría cuántica:

El origen de la teoría cuántica data del periodo comprendido entre 1900 y 1905, teniendo como protagonistas a Max Planck y Albert Einstein, los cuales continuaron la línea de pensamiento que Ludwig Boltzmann abrió en 1877, acerca de la entropía y la probabilidad como elementos clave en sus descubrimientos. El eje principal de sus investigaciones era resolver el problema planteado por la radiación del cuerpo negro. En diciembre de 1900, Planck introdujo el concepto de cuanto de energía dentro de sus investigaciones, para describir las propiedades espectrales de la radiación, mediante un proceso de distancias discretas o cuantización (electrones que giran alrededor del núcleo a ciertas distancias específicas) aplicado a la materia. Las teorías y los descubrimientos de Max Planck, fueron el motor que con el paso del tiempo introdujeron al mundo en la era cuántica, la era del láser, el CD, el ordenador, el transistor y los artilugios de comunicación personal.

Inicios de revolución cuántica:

En 1923 Niels Bohr comenzó a complementar el modelo cuántico explicando la estructura del átomo, por medio de ecuaciones sencillas, explicó las propiedades de los átomos mediante la mecánica cuántica (cuantización).

El físico francés Louis de Broglie demostró que las orbitas atómicas pueden explicarse asumiendo que los electrones también pueden comportarse como ondas.

Erwin Schrödinger en 1925 formuló la ecuación que lleva su nombre, sentando las bases de una teoría completa de la mecánica cuántica, dando a los científicos una receta universal para entender todos los fenómenos cuánticos anteriores, y les proporcionó una forma sistemática de explorar el mundo atómico para obtener nuevos e inexplorados efectos

[38] Reyez Álvarez, M. (2016). Evolución de la computación cuántica y los retos para la seguridad de la información. Cuaderno Activa, 8, 49-63

cuánticos, siendo la teoría cuántica la más precisa y con más fuerza jamás concebida por la humanidad, la cual fue tremendamente útil como herramienta científica e hizo posible muchas de las tecnologías actuales.

Revolución cuántica moderna:

La segunda revolución cuántica cuenta con dos características principales 1. Capacidad de controlar la rareza del mundo cuántico incluidas la superposición y el entrelazamiento, 2. Es el auge de la era de la información, ahí llega la información cuántica o IQ.

En 1985 un artículo del físico americano Richard Feynman, hablaba de la posibilidad de que los ordenadores funcionaran por principios cuánticos. Introdujo la teoría de los patrones, hipotéticas partículas localizadas en el núcleo atómico, que daría pie más tarde a la introducción del moderno concepto de quark. Su aportación a la física teórica ha quedado recogida en títulos tales como, Quantum.

La tecnología actual se está aproximando a los límites de la información cuántica, y nuestros transistores se acercan al tamaño de un bit cuántico, o qubit, a lo cual en un principio se le llamó ley de Moore (se trata de una regla por la cual establece que el número de transistores en un chip microprocesador se duplicará cada dos años más o menos) en honor al fundador de Intel que lo predijo hace veinte años, y por tanto se esperaba que en los siguientes veinte años los transistores que son el corazón de los dispositivos informáticos se acerquen al tamaño de un único átomo. Pero como era de esperarse, la evolución de la tecnología ha cambiado mucho, y ya la ley de Moore ha ido quedando como una anécdota más, pero que da lugar para comprender la gran evolución tecnológica comparando un ordenador de los años setenta con los sofisticados aparatos de los noventa, que dieron origen a la popularización de internet.

2.7.2 Aplicaciones actuales

- La criptografía cuántica, ya se ha utilizado a alto nivel, para asegurar los resultados electorales en Suiza, allí se desarrolló la tecnología básica para la criptografía cuántica, lo que se aseguraba mediante la criptografía cuántica es el vínculo de fibra óptica que une el lugar donde se cuentan las papeletas, con el lugar donde están los ordenadores del Estado, y esa fue la primera aplicación publica de la información cuántica en el mundo real.

- La tele transportación cuántica no tiene nada que ver con lo que se ve en ciencia ficción, porque no se traslada ninguna materia de un punto A un punto B, es la información cuántica lo que se traslada de A hacia B. La tele transportación cuántica es posible

por el entrelazamiento de dos fotones para transmitirle información del uno al otro.

- La simulación de sistemas cuánticos, por ejemplo, un simulador de vuelo.

- Ayudar a diseñar nuevos súper conductores para dirigir trenes de levitación magnética

- Podría simular los átomos de un fármaco para indicar cómo prepararlo, y cómo interactuará con otras sustancias químicas, la química de los átomos, el comportamiento de los materiales, todo depende de la mecánica cuántica, y un ordenador cuántico es magnífico para simularlo.

- Identificar el mercurio en el pescado.

- Buscar el plomo en los juguetes.

- Detectar bombas.

- Hacer sensores más sólidos, más precisos, más sensibles, y si se pueden compactar se podrán usar ampliamente en el entorno medioambiental.

- Fayer Wayer afirma que el ordenador cuántico podrá encontrar la mejor forma para codificar secretos, usando diferentes técnicas de cifrado a través de la factorización de números, lo que a su vez dejará obsoletos los métodos de cifra actuales, y se abrirán nuevos paradigmas para la seguridad de la información.

PARTE 3. CIERRE DE LA INVESTIGACIÓN

CAPÍTULO 3. RESULTADOS

3.1 ALCANCE IDENTIFICADO

Durante la investigación se pudo observar que el tipo de **billetera hardware** no puede llegar a implementar esta solución al problema planteado, ya que este tipo de billeteras o monederos tienen un número limitado de intentos antes de que sean formateadas de forma automática, esto quiere decir que no se puede utilizar distintos tipos de contraseñas candidatas para poder realizar la apertura de la billetera porque puede llegarse a perder los fondos de forma definitiva.

Para los demás tipos de billeteras como son las de papel, escritorio, móvil y en línea pueden llegar a implementar las soluciones propuestas.

3.2 MATRIZ DE TIEMPOS

Con base a la investigación realizada se logró generar una relación entre los tipos de billeteras, los algoritmos de encriptación, características de la contraseña, las técnicas para generar posibles contraseñas, las herramientas y el potencial cuántico.

El resultado de esta relación es una matriz que expresa los tiempos teóricos en los cuales se estima la apertura de un monedero virtual.

En la estimación se tuvo en cuenta 3 factores correspondientes a la información que el dueño de la billetera virtual recuerda, en información Relevante, información Moderada e información insuficiente.
Lo anterior corresponde a que tantos caracteres de utilizan en la generación de contraseñas, entre mayor sea la información recordada más probabilidad existe de poder recuperar los recursos.

3.2.1 Información relevante

Longitud corta – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
10	Permutaciones	1.048.576	MWB Decryption tool	150 GFLOP	6,13E-18	23 Qubit	1,06E-28
				14 TFLOP	6,57E-20	42 Qubit	2,02E-34
				200 PFLOPS	4,60E-24	54 Qubit	4,93E-38
			BtcRecover	150 GFLOP	5,58E-18	23 Qubit	9,63E-29
				14 TFLOP	5,98E-20	42 Qubit	1,84E-34
				200 PFLOPS	4,18E-24	54 Qubit	4,48E-38
	Combinaciones	980.419	MWB Decryption tool	150 GFLOP	5,73E-18	23 Qubit	9,89E-29
				14 TFLOP	6,14E-20	42 Qubit	1,89E-34
				200 PFLOPS	4,30E-24	54 Qubit	4,61E-38
			BtcRecover	150 GFLOP	5,22E-18	23 Qubit	9,00E-29
				14 TFLOP	5,59E-20	42 Qubit	1,72E-34
				200 PFLOPS	3,91E-24	54 Qubit	4,19E-38
	Diccionario	606.077	MWB Decryption tool	150 GFLOP	3,54E-18	23 Qubit	6,12E-29
				14 TFLOP	3,80E-20	42 Qubit	1,17E-34
				200 PFLOPS	2,66E-24	54 Qubit	2,85E-38
			BtcRecover	150 GFLOP	3,22E-18	23 Qubit	5,57E-29
				14 TFLOP	3,46E-20	42 Qubit	1,06E-34
				200 PFLOPS	2,42E-24	54 Qubit	2,59E-38
	Targuess	141.558	MWB Decryption tool	150 GFLOP	8,28E-19	23 Qubit	1,43E-29
				14 TFLOP	8,87E-21	42 Qubit	2,72E-35
				200 PFLOPS	6,21E-25	54 Qubit	6,65E-39
			BtcRecover	150 GFLOP	7,53E-19	23 Qubit	1,30E-29
				14 TFLOP	8,07E-21	42 Qubit	2,48E-35
				200 PFLOPS	5,65E-25	54 Qubit	6,05E-39

Ilustración 10 - Estimación tiempos contraseña corta, numérica y con información relevante

Longitud corta – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
10	Permutaciones	2,89E+11	MWB Decryption tool	150 GFLOP	1,69E-12	23 Qubit	2,92E-23
				14 TFLOP	1,81E-14	42 Qubit	5,57E-29
				200 PFLOPS	1,27E-18	54 Qubit	1,36E-32
			BtcRecover	150 GFLOP	1,54E-12	23 Qubit	2,66E-23
				14 TFLOP	1,65E-14	42 Qubit	5,07E-29
				200 PFLOPS	1,15E-18	54 Qubit	1,24E-32
	Combinaciones	2,70E+11	MWB Decryption tool	150 GFLOP	1,58E-12	23 Qubit	2,73E-23
				14 TFLOP	1,69E-14	42 Qubit	5,21E-29
				200 PFLOPS	1,19E-18	54 Qubit	1,27E-32
			BtcRecover	150 GFLOP	1,44E-12	23 Qubit	2,48E-23
				14 TFLOP	1,54E-14	42 Qubit	4,74E-29
				200 PFLOPS	1,08E-18	54 Qubit	1,16E-32
	Diccionario	1,67E+11	MWB Decryption tool	150 GFLOP	9,78E-13	23 Qubit	1,69E-23
				14 TFLOP	1,05E-14	42 Qubit	3,22E-29
				200 PFLOPS	7,33E-19	54 Qubit	7,86E-33
			BtcRecover	150 GFLOP	8,90E-13	23 Qubit	1,54E-23
				14 TFLOP	9,53E-15	42 Qubit	2,93E-29
				200 PFLOPS	6,67E-19	54 Qubit	7,15E-33
	Targuess	3,90E+10	MWB Decryption tool	150 GFLOP	2,28E-13	23 Qubit	3,94E-24
				14 TFLOP	2,45E-15	42 Qubit	7,52E-30
				200 PFLOPS	1,71E-19	54 Qubit	1,84E-33
			BtcRecover	150 GFLOP	2,08E-13	23 Qubit	3,59E-24
				14 TFLOP	2,23E-15	42 Qubit	6,84E-30
				200 PFLOPS	1,56E-19	54 Qubit	1,67E-33

Ilustración 11 - Estimación tiempos contraseña corta, numérica, minúsculas y con información relevante

Longitud corta – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
10	Permutaciones	6,34E+13	MWB Decryption tool	150 GFLOP	3,71E-10	23 Qubit	6,40E-21
				14 TFLOP	3,97E-12	42 Qubit	1,22E-26
				200 PFLOPS	2,78E-16	54 Qubit	2,98E-30
			BtcRecover	150 GFLOP	3,37E-10	23 Qubit	5,82E-21
				14 TFLOP	3,61E-12	42 Qubit	1,11E-26
				200 PFLOPS	2,53E-16	54 Qubit	2,71E-30
	Combinaciones	5,93E+13	MWB Decryption tool	150 GFLOP	3,47E-10	23 Qubit	5,98E-21
				14 TFLOP	3,71E-12	42 Qubit	1,14E-26
				200 PFLOPS	2,60E-16	54 Qubit	2,79E-30
			BtcRecover	150 GFLOP	3,15E-10	23 Qubit	5,44E-21
				14 TFLOP	3,38E-12	42 Qubit	1,04E-26
				200 PFLOPS	2,37E-16	54 Qubit	2,54E-30
	Diccionario	3,66E+13	MWB Decryption tool	150 GFLOP	2,14E-10	23 Qubit	3,70E-21
				14 TFLOP	2,30E-12	42 Qubit	7,05E-27
				200 PFLOPS	1,61E-16	54 Qubit	1,72E-30
			BtcRecover	150 GFLOP	1,95E-10	23 Qubit	3,37E-21
				14 TFLOP	2,09E-12	42 Qubit	6,42E-27
				200 PFLOPS	1,46E-16	54 Qubit	1,57E-30
	Targuess	8,56E+12	MWB Decryption tool	150 GFLOP	5,00E-11	23 Qubit	8,64E-22
				14 TFLOP	5,36E-13	42 Qubit	1,65E-27
				200 PFLOPS	3,75E-17	54 Qubit	4,02E-31
			BtcRecover	150 GFLOP	4,55E-11	23 Qubit	7,86E-22
				14 TFLOP	4,88E-13	42 Qubit	1,50E-27
				200 PFLOPS	3,42E-17	54 Qubit	3,66E-31

Ilustración 12 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información relevante

Longitud corta – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
10	Permutaciones	1,41E+14	MWB Decryption tool	150 GFLOP	8,25E-10	23 Qubit	1,42E-20
				14 TFLOP	8,84E-12	42 Qubit	2,72E-26
				200 PFLOPS	6,19E-16	54 Qubit	6,63E-30
			BtcRecover	150 GFLOP	7,51E-10	23 Qubit	1,30E-20
				14 TFLOP	8,05E-12	42 Qubit	2,47E-26
				200 PFLOPS	5,63E-16	54 Qubit	6,04E-30
	Combinaciones	1,32E+14	MWB Decryption tool	150 GFLOP	7,72E-10	23 Qubit	1,33E-20
				14 TFLOP	8,27E-12	42 Qubit	2,54E-26
				200 PFLOPS	5,79E-16	54 Qubit	6,20E-30
			BtcRecover	150 GFLOP	7,02E-10	23 Qubit	1,21E-20
				14 TFLOP	7,52E-12	42 Qubit	2,31E-26
				200 PFLOPS	5,27E-16	54 Qubit	5,64E-30
	Diccionario	8,16E+13	MWB Decryption tool	150 GFLOP	4,77E-10	23 Qubit	8,23E-21
				14 TFLOP	5,11E-12	42 Qubit	1,57E-26
				200 PFLOPS	3,58E-16	54 Qubit	3,83E-30
			BtcRecover	150 GFLOP	4,34E-10	23 Qubit	7,49E-21
				14 TFLOP	4,65E-12	42 Qubit	1,43E-26
				200 PFLOPS	3,26E-16	54 Qubit	3,49E-30
	Targuess	1,91E+13	MWB Decryption tool	150 GFLOP	1,11E-10	23 Qubit	1,92E-21
				14 TFLOP	1,19E-12	42 Qubit	3,67E-27
				200 PFLOPS	8,36E-17	54 Qubit	8,96E-31
			BtcRecover	150 GFLOP	1,01E-10	23 Qubit	1,75E-21
				14 TFLOP	1,09E-12	42 Qubit	3,34E-27
				200 PFLOPS	7,61E-17	54 Qubit	8,15E-31

Ilustración 13 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante

Longitud estándar – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
15	Permutaciones	1,07E+09	MWB Decryption tool	150 GFLOP	6,28E-15	23 Qubit	1,08E-25
				14 TFLOP	6,73E-17	42 Qubit	2,07E-31
				200 PFLOPS	4,71E-21	54 Qubit	5,05E-35
			BtcRecover	150 GFLOP	5,71E-15	23 Qubit	9,86E-26
				14 TFLOP	6,12E-17	42 Qubit	1,88E-31
				200 PFLOPS	4,28E-21	54 Qubit	4,59E-35
	Combinaciones	1,00E+09	MWB Decryption tool	150 GFLOP	5,87E-15	23 Qubit	1,01E-25
				14 TFLOP	6,29E-17	42 Qubit	1,93E-31
				200 PFLOPS	4,40E-21	54 Qubit	4,72E-35
			BtcRecover	150 GFLOP	5,34E-15	23 Qubit	9,22E-26
				14 TFLOP	5,72E-17	42 Qubit	1,76E-31
				200 PFLOPS	4,01E-21	54 Qubit	4,29E-35
	Diccionario	6,21E+08	MWB Decryption tool	150 GFLOP	3,63E-15	23 Qubit	6,26E-26
				14 TFLOP	3,89E-17	42 Qubit	1,19E-31
				200 PFLOPS	2,72E-21	54 Qubit	2,92E-35
			BtcRecover	150 GFLOP	3,30E-15	23 Qubit	5,70E-26
				14 TFLOP	3,54E-17	42 Qubit	1,09E-31
				200 PFLOPS	2,48E-21	54 Qubit	2,65E-35
	Targuess	1,45E+08	MWB Decryption tool	150 GFLOP	8,48E-16	23 Qubit	1,46E-26
				14 TFLOP	9,08E-18	42 Qubit	2,79E-32
				200 PFLOPS	6,36E-22	54 Qubit	6,81E-36
			BtcRecover	150 GFLOP	7,71E-16	23 Qubit	1,33E-26
				14 TFLOP	8,26E-18	42 Qubit	2,54E-32
				200 PFLOPS	5,78E-22	54 Qubit	6,20E-36

Ilustración 14 - Estimación tiempos contraseña estándar, numérica y con información relevante

Longitud estándar – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
15	Permutaciones	1,56E+17	MWB Decryption tool	150 GFLOP	9,10E-07	23 Qubit	1,57E-17
				14 TFLOP	9,75E-09	42 Qubit	2,99E-23
				200 PFLOPS	6,82E-13	54 Qubit	7,31E-27
			BtcRecover	150 GFLOP	8,28E-07	23 Qubit	1,43E-17
				14 TFLOP	8,87E-09	42 Qubit	2,73E-23
				200 PFLOPS	6,21E-13	54 Qubit	6,65E-27
	Combinaciones	1,45E+17	MWB Decryption tool	150 GFLOP	8,50E-07	23 Qubit	1,47E-17
				14 TFLOP	9,11E-09	42 Qubit	2,80E-23
				200 PFLOPS	6,38E-13	54 Qubit	6,84E-27
			BtcRecover	150 GFLOP	7,74E-07	23 Qubit	1,34E-17
				14 TFLOP	8,29E-09	42 Qubit	2,55E-23
				200 PFLOPS	5,80E-13	54 Qubit	6,22E-27
	Diccionario	8,99E+16	MWB Decryption tool	150 GFLOP	5,26E-07	23 Qubit	9,07E-18
				14 TFLOP	5,63E-09	42 Qubit	1,73E-23
				200 PFLOPS	3,94E-13	54 Qubit	4,23E-27
			BtcRecover	150 GFLOP	4,78E-07	23 Qubit	8,26E-18
				14 TFLOP	5,13E-09	42 Qubit	1,58E-23
				200 PFLOPS	3,59E-13	54 Qubit	3,85E-27
	Targuess	2,10E+16	MWB Decryption tool	150 GFLOP	1,23E-07	23 Qubit	2,12E-18
				14 TFLOP	1,32E-09	42 Qubit	4,04E-24
				200 PFLOPS	9,21E-14	54 Qubit	9,87E-28
			BtcRecover	150 GFLOP	1,12E-07	23 Qubit	1,93E-18
				14 TFLOP	1,20E-09	42 Qubit	3,68E-24
				200 PFLOPS	8,38E-14	54 Qubit	8,98E-28

Ilustración 15 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información relevante

Longitud estándar – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
15	Permutaciones	5,05E+20	MWB Decryption tool	150 GFLOP	2,95E-03	23 Qubit	5,10E-14
				14 TFLOP	3,16E-05	42 Qubit	9,72E-20
				200 PFLOPS	2,21E-09	54 Qubit	2,37E-23
			BtcRecover	150 GFLOP	2,69E-03	23 Qubit	4,64E-14
				14 TFLOP	2,88E-05	42 Qubit	8,84E-20
				200 PFLOPS	2,01E-09	54 Qubit	2,16E-23
	Combinaciones	4,72E+20	MWB Decryption tool	150 GFLOP	2,76E-03	23 Qubit	4,76E-14
				14 TFLOP	2,96E-05	42 Qubit	9,09E-20
				200 PFLOPS	2,07E-09	54 Qubit	2,22E-23
			BtcRecover	150 GFLOP	2,51E-03	23 Qubit	4,34E-14
				14 TFLOP	2,69E-05	42 Qubit	8,27E-20
				200 PFLOPS	1,88E-09	54 Qubit	2,02E-23
	Diccionario	2,92E+20	MWB Decryption tool	150 GFLOP	1,71E-03	23 Qubit	2,94E-14
				14 TFLOP	1,83E-05	42 Qubit	5,62E-20
				200 PFLOPS	1,28E-09	54 Qubit	1,37E-23
			BtcRecover	150 GFLOP	1,55E-03	23 Qubit	2,68E-14
				14 TFLOP	1,66E-05	42 Qubit	5,11E-20
				200 PFLOPS	1,16E-09	54 Qubit	1,25E-23
	Targuess	6,82E+19	MWB Decryption tool	150 GFLOP	3,99E-04	23 Qubit	6,88E-15
				14 TFLOP	4,27E-06	42 Qubit	1,31E-20
				200 PFLOPS	2,99E-10	54 Qubit	3,20E-24
			BtcRecover	150 GFLOP	3,63E-04	23 Qubit	6,26E-15
				14 TFLOP	3,89E-06	42 Qubit	1,19E-20
				200 PFLOPS	2,72E-10	54 Qubit	2,91E-24

Ilustración 16 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información relevante

Longitud estándar – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
15	Permutaciones	1,68E+21	MWB Decryption tool	150 GFLOP	9,81E-03	23 Qubit	1,69E-13
				14 TFLOP	1,05E-04	42 Qubit	3,23E-19
				200 PFLOPS	7,35E-09	54 Qubit	7,88E-23
			BtcRecover	150 GFLOP	8,92E-03	23 Qubit	1,54E-13
				14 TFLOP	9,56E-05	42 Qubit	2,94E-19
				200 PFLOPS	6,69E-09	54 Qubit	7,17E-23
	Combinaciones	1,57E+21	MWB Decryption tool	150 GFLOP	9,17E-03	23 Qubit	1,58E-13
				14 TFLOP	9,82E-05	42 Qubit	3,02E-19
				200 PFLOPS	6,88E-09	54 Qubit	7,37E-23
			BtcRecover	150 GFLOP	8,34E-03	23 Qubit	1,44E-13
				14 TFLOP	8,94E-05	42 Qubit	2,75E-19
				200 PFLOPS	6,26E-09	54 Qubit	6,71E-23
	Diccionario	9,69E+20	MWB Decryption tool	150 GFLOP	5,67E-03	23 Qubit	9,78E-14
				14 TFLOP	6,07E-05	42 Qubit	1,87E-19
				200 PFLOPS	4,25E-09	54 Qubit	4,56E-23
			BtcRecover	150 GFLOP	5,16E-03	23 Qubit	8,90E-14
				14 TFLOP	5,53E-05	42 Qubit	1,70E-19
				200 PFLOPS	3,87E-09	54 Qubit	4,15E-23
	Targuess	2,26E+20	MWB Decryption tool	150 GFLOP	1,32E-03	23 Qubit	2,29E-14
				14 TFLOP	1,42E-05	42 Qubit	4,36E-20
				200 PFLOPS	9,93E-10	54 Qubit	1,06E-23
			BtcRecover	150 GFLOP	1,20E-03	23 Qubit	2,08E-14
				14 TFLOP	1,29E-05	42 Qubit	3,97E-20
				200 PFLOPS	9,04E-10	54 Qubit	9,68E-24

Ilustración 17 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante

Longitud compleja – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
20	Permutaciones	1,10E+12	MWB Decryption tool	150 GFLOP	6,43E-12	23 Qubit	1,11E-22
				14 TFLOP	6,89E-14	42 Qubit	2,12E-28
				200 PFLOPS	4,82E-18	54 Qubit	5,17E-32
			BtcRecover	150 GFLOP	5,85E-12	23 Qubit	1,01E-22
				14 TFLOP	6,27E-14	42 Qubit	1,93E-28
				200 PFLOPS	4,39E-18	54 Qubit	4,70E-32
	Combinaciones	1,03E+12	MWB Decryption tool	150 GFLOP	6,01E-12	23 Qubit	1,04E-22
				14 TFLOP	6,44E-14	42 Qubit	1,98E-28
				200 PFLOPS	4,51E-18	54 Qubit	4,83E-32
			BtcRecover	150 GFLOP	5,47E-12	23 Qubit	9,44E-23
				14 TFLOP	5,86E-14	42 Qubit	1,80E-28
				200 PFLOPS	4,10E-18	54 Qubit	4,40E-32
	Diccionario	6,36E+11	MWB Decryption tool	150 GFLOP	3,72E-12	23 Qubit	6,41E-23
				14 TFLOP	3,98E-14	42 Qubit	1,22E-28
				200 PFLOPS	2,79E-18	54 Qubit	2,99E-32
			BtcRecover	150 GFLOP	3,38E-12	23 Qubit	5,84E-23
				14 TFLOP	3,62E-14	42 Qubit	1,11E-28
				200 PFLOPS	2,54E-18	54 Qubit	2,72E-32
	Targuess	1,48E+11	MWB Decryption tool	150 GFLOP	8,68E-13	23 Qubit	1,50E-23
				14 TFLOP	9,30E-15	42 Qubit	2,86E-29
				200 PFLOPS	6,51E-19	54 Qubit	6,98E-33
			BtcRecover	150 GFLOP	7,90E-13	23 Qubit	1,36E-23
				14 TFLOP	8,46E-15	42 Qubit	2,60E-29
				200 PFLOPS	5,92E-19	54 Qubit	6,35E-33

Ilustración 18 - Estimación tiempos contraseña compleja, numérica y con información relevante

Longitud compleja – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
20	Permutaciones	8,37E+22	MWB Decryption tool	150 GFLOP	4,89E-01	23 Qubit	8,44E-12
				14 TFLOP	5,24E-03	42 Qubit	1,61E-17
				200 PFLOPS	3,67E-07	54 Qubit	3,93E-21
			BtcRecover	150 GFLOP	4,45E-01	23 Qubit	7,68E-12
				14 TFLOP	4,77E-03	42 Qubit	1,47E-17
				200 PFLOPS	3,34E-07	54 Qubit	3,58E-21
	Combinaciones	7,82E+22	MWB Decryption tool	150 GFLOP	4,57E-01	23 Qubit	7,90E-12
				14 TFLOP	4,90E-03	42 Qubit	1,51E-17
				200 PFLOPS	3,43E-07	54 Qubit	3,68E-21
			BtcRecover	150 GFLOP	4,16E-01	23 Qubit	7,18E-12
				14 TFLOP	4,46E-03	42 Qubit	1,37E-17
				200 PFLOPS	3,12E-07	54 Qubit	3,35E-21
	Diccionario	4,84E+22	MWB Decryption tool	150 GFLOP	2,83E-01	23 Qubit	4,88E-12
				14 TFLOP	3,03E-03	42 Qubit	9,31E-18
				200 PFLOPS	2,12E-07	54 Qubit	2,27E-21
			BtcRecover	150 GFLOP	2,57E-01	23 Qubit	4,44E-12
				14 TFLOP	2,76E-03	42 Qubit	8,47E-18
				200 PFLOPS	1,93E-07	54 Qubit	2,07E-21
	Targuess	1,13E+22	MWB Decryption tool	150 GFLOP	6,60E-02	23 Qubit	1,14E-12
				14 TFLOP	7,08E-04	42 Qubit	2,17E-18
				200 PFLOPS	4,95E-08	54 Qubit	5,31E-22
			BtcRecover	150 GFLOP	6,01E-02	23 Qubit	1,04E-12
				14 TFLOP	6,44E-04	42 Qubit	1,98E-18
				200 PFLOPS	4,51E-08	54 Qubit	4,83E-22

Ilustración 19 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información relevante

Longitud compleja – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
20	Permutaciones	4,02E+27	MWB Decryption tool	150 GFLOP	2,35E+04	23 Qubit	4,06E-07
				14 TFLOP	2,52E+02	42 Qubit	7,74E-13
				200 PFLOPS	1,76E-02	54 Qubit	1,89E-16
			BtcRecover	150 GFLOP	2,14E+04	23 Qubit	3,69E-07
				14 TFLOP	2,29E+02	42 Qubit	7,04E-13
				200 PFLOPS	1,60E-02	54 Qubit	1,72E-16
	Combinaciones	3,76E+27	MWB Decryption tool	150 GFLOP	2,20E+04	23 Qubit	3,79E-07
				14 TFLOP	2,35E+02	42 Qubit	7,24E-13
				200 PFLOPS	1,65E-02	54 Qubit	1,77E-16
			BtcRecover	150 GFLOP	2,00E+04	23 Qubit	3,45E-07
				14 TFLOP	2,14E+02	42 Qubit	6,58E-13
				200 PFLOPS	1,50E-02	54 Qubit	1,61E-16
	Diccionario	2,32E+27	MWB Decryption tool	150 GFLOP	1,36E+04	23 Qubit	2,34E-07
				14 TFLOP	1,46E+02	42 Qubit	4,47E-13
				200 PFLOPS	1,02E-02	54 Qubit	1,09E-16
			BtcRecover	150 GFLOP	1,24E+04	23 Qubit	2,13E-07
				14 TFLOP	1,32E+02	42 Qubit	4,07E-13
				200 PFLOPS	9,27E-03	54 Qubit	9,94E-17
	Targuess	5,43E+26	MWB Decryption tool	150 GFLOP	3,17E+03	23 Qubit	5,48E-08
				14 TFLOP	3,40E+01	42 Qubit	1,04E-13
				200 PFLOPS	2,38E-03	54 Qubit	2,55E-17
			BtcRecover	150 GFLOP	2,89E+03	23 Qubit	4,98E-08
				14 TFLOP	3,09E+01	42 Qubit	9,51E-14
				200 PFLOPS	2,17E-03	54 Qubit	2,32E-17

Ilustración 20 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información relevante

Longitud compleja – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
20	Permutaciones	1,99E+28	MWB Decryption tool	150 GFLOP	1,17E+05	23 Qubit	2,01E-06
				14 TFLOP	1,25E+03	42 Qubit	3,84E-12
				200 PFLOPS	8,74E-02	54 Qubit	9,37E-16
			BtcRecover	150 GFLOP	1,06E+05	23 Qubit	1,83E-06
				14 TFLOP	1,14E+03	42 Qubit	3,49E-12
				200 PFLOPS	7,95E-02	54 Qubit	8,52E-16
	Combinaciones	1,86E+28	MWB Decryption tool	150 GFLOP	1,09E+05	23 Qubit	1,88E-06
				14 TFLOP	1,17E+03	42 Qubit	3,59E-12
				200 PFLOPS	8,17E-02	54 Qubit	8,76E-16
			BtcRecover	150 GFLOP	9,91E+04	23 Qubit	1,71E-06
				14 TFLOP	1,06E+03	42 Qubit	3,26E-12
				200 PFLOPS	7,44E-02	54 Qubit	7,97E-16
	Diccionario	1,15E+28	MWB Decryption tool	150 GFLOP	6,73E+04	23 Qubit	1,16E-06
				14 TFLOP	7,22E+02	42 Qubit	2,22E-12
				200 PFLOPS	5,05E-02	54 Qubit	5,41E-16
			BtcRecover	150 GFLOP	6,13E+04	23 Qubit	1,06E-06
				14 TFLOP	6,57E+02	42 Qubit	2,02E-12
				200 PFLOPS	4,60E-02	54 Qubit	4,93E-16
	Targuess	2,69E+27	MWB Decryption tool	150 GFLOP	1,57E+04	23 Qubit	2,72E-07
				14 TFLOP	1,69E+02	42 Qubit	5,18E-13
				200 PFLOPS	1,18E-02	54 Qubit	1,26E-16
			BtcRecover	150 GFLOP	1,43E+04	23 Qubit	2,47E-07
				14 TFLOP	1,53E+02	42 Qubit	4,71E-13
				200 PFLOPS	1,07E-02	54 Qubit	1,15E-16

Ilustración 21 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información relevante

3.2.2 Información moderada

Longitud corta – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs3
10	Permutaciones	6,05E+07	MWB Decryption tool	150 GFLOP	3,54E-16	23 Qubit	6,10E-27
				14 TFLOP	3,79E-18	42 Qubit	1,16E-32
				200 PFLOPS	2,65E-22	54 Qubit	2,84E-36
			BtcRecover	150 GFLOP	3,22E-16	23 Qubit	5,55E-27
				14 TFLOP	3,45E-18	42 Qubit	1,06E-32
				200 PFLOPS	2,41E-22	54 Qubit	2,59E-36
	Combinaciones	5,65E+07	MWB Decryption tool	150 GFLOP	3,31E-16	23 Qubit	5,71E-27
				14 TFLOP	3,54E-18	42 Qubit	1,09E-32
				200 PFLOPS	2,48E-22	54 Qubit	2,66E-36
			BtcRecover	150 GFLOP	3,01E-16	23 Qubit	5,19E-27
				14 TFLOP	3,22E-18	42 Qubit	9,90E-33
				200 PFLOPS	2,26E-22	54 Qubit	2,42E-36
	Diccionario	3,49E+07	MWB Decryption tool	150 GFLOP	2,04E-16	23 Qubit	3,53E-27
				14 TFLOP	2,19E-18	42 Qubit	6,73E-33
				200 PFLOPS	1,53E-22	54 Qubit	1,64E-36
			BtcRecover	150 GFLOP	1,86E-16	23 Qubit	3,21E-27
				14 TFLOP	1,99E-18	42 Qubit	6,12E-33
				200 PFLOPS	1,39E-22	54 Qubit	1,49E-36
	Targuess	8,16E+06	MWB Decryption tool	150 GFLOP	4,77E-17	23 Qubit	8,24E-28
				14 TFLOP	5,11E-19	42 Qubit	1,57E-33
				200 PFLOPS	3,58E-23	54 Qubit	3,84E-37
			BtcRecover	150 GFLOP	4,34E-17	23 Qubit	7,50E-28
				14 TFLOP	4,65E-19	42 Qubit	1,43E-33
				200 PFLOPS	3,26E-23	54 Qubit	3,49E-37

Ilustración 22 - Estimación tiempos contraseña corta, numérica y con información moderada

Longitud corta – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	1,67E+13	MWB Decryption tool	150 GFLOP	9,75E-11	23 Qubit	1,68E-21
				14 TFLOP	1,04E-12	42 Qubit	3,21E-27
				200 PFLOPS	7,31E-17	54 Qubit	7,84E-31
			BtcRecover	150 GFLOP	8,87E-11	23 Qubit	1,53E-21
				14 TFLOP	9,51E-13	42 Qubit	2,92E-27
				200 PFLOPS	6,66E-17	54 Qubit	7,13E-31
	Combinaciones	1,56E+13	MWB Decryption tool	150 GFLOP	9,12E-11	23 Qubit	1,57E-21
				14 TFLOP	9,77E-13	42 Qubit	3,00E-27
				200 PFLOPS	6,84E-17	54 Qubit	7,33E-31
			BtcRecover	150 GFLOP	8,30E-11	23 Qubit	1,43E-21
				14 TFLOP	8,89E-13	42 Qubit	2,73E-27
				200 PFLOPS	6,22E-17	54 Qubit	6,67E-31
	Diccionario	9,64E+12	MWB Decryption tool	150 GFLOP	5,64E-11	23 Qubit	9,73E-22
				14 TFLOP	6,04E-13	42 Qubit	1,86E-27
				200 PFLOPS	4,23E-17	54 Qubit	4,53E-31
			BtcRecover	150 GFLOP	5,13E-11	23 Qubit	8,85E-22
				14 TFLOP	5,50E-13	42 Qubit	1,69E-27
				200 PFLOPS	3,85E-17	54 Qubit	4,12E-31
	Targuess	2,25E+12	MWB Decryption tool	150 GFLOP	1,32E-11	23 Qubit	2,27E-22
				14 TFLOP	1,41E-13	42 Qubit	4,33E-28
				200 PFLOPS	9,87E-18	54 Qubit	1,06E-31
			BtcRecover	150 GFLOP	1,20E-11	23 Qubit	2,07E-22
				14 TFLOP	1,28E-13	42 Qubit	3,94E-28
				200 PFLOPS	8,99E-18	54 Qubit	9,63E-32

Ilustración 23 - Estimación tiempos contraseña corta, numérica, minúsculas y con información moderada

Longitud corta – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	3,66E+15	MWB Decryption tool	150 GFLOP	2,14E-08	23 Qubit	3,69E-19
				14 TFLOP	2,29E-10	42 Qubit	7,04E-25
				200 PFLOPS	1,60E-14	54 Qubit	1,72E-28
			BtcRecover	150 GFLOP	1,95E-08	23 Qubit	3,36E-19
				14 TFLOP	2,08E-10	42 Qubit	6,40E-25
				200 PFLOPS	1,46E-14	54 Qubit	1,56E-28
	Combinaciones	3,42E+15	MWB Decryption tool	150 GFLOP	2,00E-08	23 Qubit	3,45E-19
				14 TFLOP	2,14E-10	42 Qubit	6,58E-25
				200 PFLOPS	1,50E-14	54 Qubit	1,61E-28
			BtcRecover	150 GFLOP	1,82E-08	23 Qubit	3,14E-19
				14 TFLOP	1,95E-10	42 Qubit	5,99E-25
				200 PFLOPS	1,36E-14	54 Qubit	1,46E-28
	Diccionario	2,11E+15	MWB Decryption tool	150 GFLOP	1,24E-08	23 Qubit	2,13E-19
				14 TFLOP	1,32E-10	42 Qubit	4,07E-25
				200 PFLOPS	9,27E-15	54 Qubit	9,93E-29
			BtcRecover	150 GFLOP	1,12E-08	23 Qubit	1,94E-19
				14 TFLOP	1,20E-10	42 Qubit	3,70E-25
				200 PFLOPS	8,43E-15	54 Qubit	9,04E-29
	Targuess	4,94E+14	MWB Decryption tool	150 GFLOP	2,89E-09	23 Qubit	4,98E-20
				14 TFLOP	3,09E-11	42 Qubit	9,50E-26
				200 PFLOPS	2,16E-15	54 Qubit	2,32E-29
			BtcRecover	150 GFLOP	2,63E-09	23 Qubit	4,53E-20
				14 TFLOP	2,81E-11	42 Qubit	8,65E-26
				200 PFLOPS	1,97E-15	54 Qubit	2,11E-29

Ilustración 24 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información moderada

Longitud corta – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	1,34E+16	MWB Decryption tool	150 GFLOP	7,85E-08	23 Qubit	1,35E-18
				14 TFLOP	8,41E-10	42 Qubit	2,58E-24
				200 PFLOPS	5,89E-14	54 Qubit	6,31E-28
			BtcRecover	150 GFLOP	7,14E-08	23 Qubit	1,23E-18
				14 TFLOP	7,65E-10	42 Qubit	2,35E-24
				200 PFLOPS	5,36E-14	54 Qubit	5,74E-28
	Combinaciones	1,26E+16	MWB Decryption tool	150 GFLOP	7,34E-08	23 Qubit	1,27E-18
				14 TFLOP	7,86E-10	42 Qubit	2,42E-24
				200 PFLOPS	5,50E-14	54 Qubit	5,90E-28
			BtcRecover	150 GFLOP	6,68E-08	23 Qubit	1,15E-18
				14 TFLOP	7,15E-10	42 Qubit	2,20E-24
				200 PFLOPS	5,01E-14	54 Qubit	5,37E-28
	Diccionario	7,76E+15	MWB Decryption tool	150 GFLOP	4,54E-08	23 Qubit	7,83E-19
				14 TFLOP	4,86E-10	42 Qubit	1,49E-24
				200 PFLOPS	3,40E-14	54 Qubit	3,65E-28
			BtcRecover	150 GFLOP	4,13E-08	23 Qubit	7,13E-19
				14 TFLOP	4,42E-10	42 Qubit	1,36E-24
				200 PFLOPS	3,10E-14	54 Qubit	3,32E-28
	Targuess	1,81E+15	MWB Decryption tool	150 GFLOP	1,06E-08	23 Qubit	1,83E-19
				14 TFLOP	1,14E-10	42 Qubit	3,49E-25
				200 PFLOPS	7,95E-15	54 Qubit	8,52E-29
			BtcRecover	150 GFLOP	9,64E-09	23 Qubit	1,66E-19
				14 TFLOP	1,03E-10	42 Qubit	3,17E-25
				200 PFLOPS	7,23E-15	54 Qubit	7,75E-29

Ilustración 25 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada

Longitud estándar – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	4,70E+11	MWB Decryption tool	150 GFLOP	2,75E-12	23 Qubit	4,75E-23
				14 TFLOP	2,95E-14	42 Qubit	9,05E-29
				200 PFLOPS	2,06E-18	54 Qubit	2,21E-32
			BtcRecover	150 GFLOP	2,50E-12	23 Qubit	4,32E-23
				14 TFLOP	2,68E-14	42 Qubit	8,24E-29
				200 PFLOPS	1,88E-18	54 Qubit	2,01E-32
	Combinaciones	4,40E+11	MWB Decryption tool	150 GFLOP	2,57E-12	23 Qubit	4,44E-23
				14 TFLOP	2,75E-14	42 Qubit	8,46E-29
				200 PFLOPS	1,93E-18	54 Qubit	2,07E-32
			BtcRecover	150 GFLOP	2,34E-12	23 Qubit	4,04E-23
				14 TFLOP	2,51E-14	42 Qubit	7,70E-29
				200 PFLOPS	1,75E-18	54 Qubit	1,88E-32
	Diccionario	2,72E+11	MWB Decryption tool	150 GFLOP	1,59E-12	23 Qubit	2,74E-23
				14 TFLOP	1,70E-14	42 Qubit	5,23E-29
				200 PFLOPS	1,19E-18	54 Qubit	1,28E-32
			BtcRecover	150 GFLOP	1,45E-12	23 Qubit	2,50E-23
				14 TFLOP	1,55E-14	42 Qubit	4,76E-29
				200 PFLOPS	1,08E-18	54 Qubit	1,16E-32
	Targuess	6,35E+10	MWB Decryption tool	150 GFLOP	3,71E-13	23 Qubit	6,41E-24
				14 TFLOP	3,98E-15	42 Qubit	1,22E-29
				200 PFLOPS	2,78E-19	54 Qubit	2,98E-33
			BtcRecover	150 GFLOP	3,38E-13	23 Qubit	5,83E-24
				14 TFLOP	3,62E-15	42 Qubit	1,11E-29
				200 PFLOPS	2,53E-19	54 Qubit	2,71E-33

Ilustración 26 - Estimación tiempos contraseña estándar, numérica y con información moderada

Longitud estándar – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	6,81E+19	MWB Decryption tool	150 GFLOP	3,98E-04	23 Qubit	6,88E-15
				14 TFLOP	4,27E-06	42 Qubit	1,31E-20
				200 PFLOPS	2,99E-10	54 Qubit	3,20E-24
			BtcRecover	150 GFLOP	3,62E-04	23 Qubit	6,26E-15
				14 TFLOP	3,88E-06	42 Qubit	1,19E-20
				200 PFLOPS	2,72E-10	54 Qubit	2,91E-24
	Combinaciones	6,37E+19	MWB Decryption tool	150 GFLOP	3,72E-04	23 Qubit	6,43E-15
				14 TFLOP	3,99E-06	42 Qubit	1,23E-20
				200 PFLOPS	2,79E-10	54 Qubit	2,99E-24
			BtcRecover	150 GFLOP	3,39E-04	23 Qubit	5,85E-15
				14 TFLOP	3,63E-06	42 Qubit	1,12E-20
				200 PFLOPS	2,54E-10	54 Qubit	2,72E-24
	Diccionario	3,94E+19	MWB Decryption tool	150 GFLOP	2,30E-04	23 Qubit	3,97E-15
				14 TFLOP	2,47E-06	42 Qubit	7,58E-21
				200 PFLOPS	1,73E-10	54 Qubit	1,85E-24
			BtcRecover	150 GFLOP	2,10E-04	23 Qubit	3,62E-15
				14 TFLOP	2,24E-06	42 Qubit	6,90E-21
				200 PFLOPS	1,57E-10	54 Qubit	1,68E-24
	Targuess	9,20E+18	MWB Decryption tool	150 GFLOP	5,38E-05	23 Qubit	9,28E-16
				14 TFLOP	5,76E-07	42 Qubit	1,77E-21
				200 PFLOPS	4,03E-11	54 Qubit	4,32E-25
			BtcRecover	150 GFLOP	4,89E-05	23 Qubit	8,45E-16
				14 TFLOP	5,24E-07	42 Qubit	1,61E-21
				200 PFLOPS	3,67E-11	54 Qubit	3,93E-25

Ilustración 27 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información moderada

Longitud estándar – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	2,21E+23	MWB Decryption tool	150 GFLOP	1,29E+00	23 Qubit	2,23E-11
				14 TFLOP	1,38E-02	42 Qubit	4,26E-17
				200 PFLOPS	9,69E-07	54 Qubit	1,04E-20
			BtcRecover	150 GFLOP	1,18E+00	23 Qubit	2,03E-11
				14 TFLOP	1,26E-02	42 Qubit	3,87E-17
				200 PFLOPS	8,82E-07	54 Qubit	9,45E-21
	Combinaciones	2,07E+23	MWB Decryption tool	150 GFLOP	1,21E+00	23 Qubit	2,09E-11
				14 TFLOP	1,29E-02	42 Qubit	3,98E-17
				200 PFLOPS	9,06E-07	54 Qubit	9,71E-21
			BtcRecover	150 GFLOP	1,10E+00	23 Qubit	1,90E-11
				14 TFLOP	1,18E-02	42 Qubit	3,62E-17
				200 PFLOPS	8,25E-07	54 Qubit	8,84E-21
	Diccionario	1,28E+23	MWB Decryption tool	150 GFLOP	7,47E-01	23 Qubit	1,29E-11
				14 TFLOP	8,00E-03	42 Qubit	2,46E-17
				200 PFLOPS	5,60E-07	54 Qubit	6,00E-21
			BtcRecover	150 GFLOP	6,80E-01	23 Qubit	1,17E-11
				14 TFLOP	7,28E-03	42 Qubit	2,24E-17
				200 PFLOPS	5,10E-07	54 Qubit	5,46E-21
	Targuess	2,98E+22	MWB Decryption tool	150 GFLOP	1,74E-01	23 Qubit	3,01E-12
				14 TFLOP	1,87E-03	42 Qubit	5,74E-18
				200 PFLOPS	1,31E-07	54 Qubit	1,40E-21
			BtcRecover	150 GFLOP	1,59E-01	23 Qubit	2,74E-12
				14 TFLOP	1,70E-03	42 Qubit	5,23E-18
				200 PFLOPS	1,19E-07	54 Qubit	1,28E-21

Ilustración 28 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información moderada

Longitud estándar – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	1,56E+24	MWB Decryption tool	150 GFLOP	9,09E+00	23 Qubit	1,57E-10
				14 TFLOP	9,74E-02	42 Qubit	2,99E-16
				200 PFLOPS	6,82E-06	54 Qubit	7,31E-20
			BtcRecover	150 GFLOP	8,27E+00	23 Qubit	1,43E-10
				14 TFLOP	8,86E-02	42 Qubit	2,72E-16
				200 PFLOPS	6,21E-06	54 Qubit	6,65E-20
	Combinaciones	1,45E+24	MWB Decryption tool	150 GFLOP	8,50E+00	23 Qubit	1,47E-10
				14 TFLOP	9,11E-02	42 Qubit	2,80E-16
				200 PFLOPS	6,38E-06	54 Qubit	6,83E-20
			BtcRecover	150 GFLOP	7,74E+00	23 Qubit	1,34E-10
				14 TFLOP	8,29E-02	42 Qubit	2,55E-16
				200 PFLOPS	5,80E-06	54 Qubit	6,22E-20
	Diccionario	8,99E+23	MWB Decryption tool	150 GFLOP	5,26E+00	23 Qubit	9,07E-11
				14 TFLOP	5,63E-02	42 Qubit	1,73E-16
				200 PFLOPS	3,94E-06	54 Qubit	4,22E-20
			BtcRecover	150 GFLOP	4,78E+00	23 Qubit	8,25E-11
				14 TFLOP	5,12E-02	42 Qubit	1,57E-16
				200 PFLOPS	3,59E-06	54 Qubit	3,84E-20
	Targuess	2,10E+23	MWB Decryption tool	150 GFLOP	1,23E+00	23 Qubit	2,12E-11
				14 TFLOP	1,32E-02	42 Qubit	4,04E-17
				200 PFLOPS	9,21E-07	54 Qubit	9,87E-21
			BtcRecover	150 GFLOP	1,12E+00	23 Qubit	1,93E-11
				14 TFLOP	1,20E-02	42 Qubit	3,68E-17
				200 PFLOPS	8,38E-07	54 Qubit	8,98E-21

Ilustración 29 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada

Longitud compleja – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	3,66E+15	MWB Decryption tool	150 GFLOP	2,14E-08	23 Qubit	3,69E-19
				14 TFLOP	2,29E-10	42 Qubit	7,04E-25
				200 PFLOPS	1,60E-14	54 Qubit	1,72E-28
			BtcRecover	150 GFLOP	1,95E-08	23 Qubit	3,36E-19
				14 TFLOP	2,08E-10	42 Qubit	6,40E-25
				200 PFLOPS	1,46E-14	54 Qubit	1,56E-28
	Combinaciones	3,42E+15	MWB Decryption tool	150 GFLOP	2,00E-08	23 Qubit	3,45E-19
				14 TFLOP	2,14E-10	42 Qubit	6,58E-25
				200 PFLOPS	1,50E-14	54 Qubit	1,61E-28
			BtcRecover	150 GFLOP	1,82E-08	23 Qubit	3,14E-19
				14 TFLOP	1,95E-10	42 Qubit	5,99E-25
				200 PFLOPS	1,36E-14	54 Qubit	1,46E-28
	Diccionario	2,11E+15	MWB Decryption tool	150 GFLOP	1,24E-08	23 Qubit	2,13E-19
				14 TFLOP	1,32E-10	42 Qubit	4,07E-25
				200 PFLOPS	9,27E-15	54 Qubit	9,93E-29
			BtcRecover	150 GFLOP	1,12E-08	23 Qubit	1,94E-19
				14 TFLOP	1,20E-10	42 Qubit	3,70E-25
				200 PFLOPS	8,43E-15	54 Qubit	9,04E-29
	Targuess	4,94E+14	MWB Decryption tool	150 GFLOP	2,89E-09	23 Qubit	4,98E-20
				14 TFLOP	3,09E-11	42 Qubit	9,50E-26
				200 PFLOPS	2,16E-15	54 Qubit	2,32E-29
			BtcRecover	150 GFLOP	2,63E-09	23 Qubit	4,53E-20
				14 TFLOP	2,81E-11	42 Qubit	8,65E-26
				200 PFLOPS	1,97E-15	54 Qubit	2,11E-29

Ilustración 30 - Estimación tiempos contraseña compleja, numérica y con información moderada

Longitud compleja – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	2,78E+26	MWB Decryption tool	150 GFLOP	1,63E+03	23 Qubit	2,81E-08
				14 TFLOP	1,74E+01	42 Qubit	5,36E-14
				200 PFLOPS	1,22E-03	54 Qubit	1,31E-17
			BtcRecover	150 GFLOP	1,48E+03	23 Qubit	2,56E-08
				14 TFLOP	1,59E+01	42 Qubit	4,87E-14
				200 PFLOPS	1,11E-03	54 Qubit	1,19E-17
	Combinaciones	2,60E+26	MWB Decryption tool	150 GFLOP	1,52E+03	23 Qubit	2,63E-08
				14 TFLOP	1,63E+01	42 Qubit	5,01E-14
				200 PFLOPS	1,14E-03	54 Qubit	1,22E-17
			BtcRecover	150 GFLOP	1,38E+03	23 Qubit	2,39E-08
				14 TFLOP	1,48E+01	42 Qubit	4,56E-14
				200 PFLOPS	1,04E-03	54 Qubit	1,11E-17
	Diccionario	1,61E+26	MWB Decryption tool	150 GFLOP	9,40E+02	23 Qubit	1,62E-08
				14 TFLOP	1,01E+01	42 Qubit	3,10E-14
				200 PFLOPS	7,05E-04	54 Qubit	7,56E-18
			BtcRecover	150 GFLOP	8,56E+02	23 Qubit	1,48E-08
				14 TFLOP	9,17E+00	42 Qubit	2,82E-14
				200 PFLOPS	6,42E-04	54 Qubit	6,88E-18
	Targuess	3,76E+25	MWB Decryption tool	150 GFLOP	2,20E+02	23 Qubit	3,79E-09
				14 TFLOP	2,35E+00	42 Qubit	7,23E-15
				200 PFLOPS	1,65E-04	54 Qubit	1,77E-18
			BtcRecover	150 GFLOP	2,00E+02	23 Qubit	3,45E-09
				14 TFLOP	2,14E+00	42 Qubit	6,58E-15
				200 PFLOPS	1,50E-04	54 Qubit	1,61E-18

Ilustración 31 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información moderada

Longitud compleja – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	1,34E+31	MWB Decryption tool	150 GFLOP	7,82E+07	23 Qubit	1,35E-03
				14 TFLOP	8,37E+05	42 Qubit	2,57E-09
				200 PFLOPS	5,86E+01	54 Qubit	6,28E-13
			BtcRecover	150 GFLOP	7,11E+07	23 Qubit	1,23E-03
				14 TFLOP	7,62E+05	42 Qubit	2,34E-09
				200 PFLOPS	5,33E+01	54 Qubit	5,72E-13
	Combinaciones	1,25E+31	MWB Decryption tool	150 GFLOP	7,31E+07	23 Qubit	1,26E-03
				14 TFLOP	7,83E+05	42 Qubit	2,41E-09
				200 PFLOPS	5,48E+01	54 Qubit	5,87E-13
			BtcRecover	150 GFLOP	6,65E+07	23 Qubit	1,15E-03
				14 TFLOP	7,12E+05	42 Qubit	2,19E-09
				200 PFLOPS	4,99E+01	54 Qubit	5,34E-13
	Diccionario	7,73E+30	MWB Decryption tool	150 GFLOP	4,52E+07	23 Qubit	7,80E-04
				14 TFLOP	4,84E+05	42 Qubit	1,49E-09
				200 PFLOPS	3,39E+01	54 Qubit	3,63E-13
			BtcRecover	150 GFLOP	4,11E+07	23 Qubit	7,10E-04
				14 TFLOP	4,40E+05	42 Qubit	1,35E-09
				200 PFLOPS	3,08E+01	54 Qubit	3,30E-13
	Targuess	1,80E+30	MWB Decryption tool	150 GFLOP	1,06E+07	23 Qubit	1,82E-04
				14 TFLOP	1,13E+05	42 Qubit	3,47E-10
				200 PFLOPS	7,91E+00	54 Qubit	8,48E-14
			BtcRecover	150 GFLOP	9,60E+06	23 Qubit	1,66E-04
				14 TFLOP	1,03E+05	42 Qubit	3,16E-10
				200 PFLOPS	7,20E+00	54 Qubit	7,72E-14

Ilustración 32 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información moderada

Longitud compleja – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	1,80E+32	MWB Decryption tool	150 GFLOP	1,05E+09	23 Qubit	1,82E-02
				14 TFLOP	1,13E+07	42 Qubit	3,47E-08
				200 PFLOPS	7,90E+02	54 Qubit	8,47E-12
			BtcRecover	150 GFLOP	9,59E+08	23 Qubit	1,65E-02
				14 TFLOP	1,03E+07	42 Qubit	3,16E-08
				200 PFLOPS	7,19E+02	54 Qubit	7,70E-12
	Combinaciones	1,68E+32	MWB Decryption tool	150 GFLOP	9,85E+08	23 Qubit	1,70E-02
				14 TFLOP	1,06E+07	42 Qubit	3,24E-08
				200 PFLOPS	7,39E+02	54 Qubit	7,92E-12
			BtcRecover	150 GFLOP	8,96E+08	23 Qubit	1,55E-02
				14 TFLOP	9,60E+06	42 Qubit	2,95E-08
				200 PFLOPS	6,72E+02	54 Qubit	7,20E-12
	Diccionario	1,04E+32	MWB Decryption tool	150 GFLOP	6,09E+08	23 Qubit	1,05E-02
				14 TFLOP	6,52E+06	42 Qubit	2,00E-08
				200 PFLOPS	4,57E+02	54 Qubit	4,89E-12
			BtcRecover	150 GFLOP	5,54E+08	23 Qubit	9,56E-03
				14 TFLOP	5,94E+06	42 Qubit	1,82E-08
				200 PFLOPS	4,16E+02	54 Qubit	4,45E-12
	Targuess	2,43E+31	MWB Decryption tool	150 GFLOP	1,42E+08	23 Qubit	2,45E-03
				14 TFLOP	1,52E+06	42 Qubit	4,68E-09
				200 PFLOPS	1,07E+02	54 Qubit	1,14E-12
			BtcRecover	150 GFLOP	1,29E+08	23 Qubit	2,23E-03
				14 TFLOP	1,39E+06	42 Qubit	4,26E-09
				200 PFLOPS	9,71E+01	54 Qubit	1,04E-12

Ilustración 33 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información moderada

3.2.3 Información insuficiente

Longitud corta – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	1,00E+10	MWB Decryption tool	150 GFLOP	5,85E-14	23 Qubit	1,01E-24
				14 TFLOP	6,26E-16	42 Qubit	1,92E-30
				200 PFLOPS	4,39E-20	54 Qubit	4,70E-34
			BtcRecover	150 GFLOP	5,32E-14	23 Qubit	9,18E-25
				14 TFLOP	5,70E-16	42 Qubit	1,75E-30
				200 PFLOPS	3,99E-20	54 Qubit	4,28E-34
	Combinaciones	9,35E+09	MWB Decryption tool	150 GFLOP	5,47E-14	23 Qubit	9,44E-25
				14 TFLOP	5,86E-16	42 Qubit	1,80E-30
				200 PFLOPS	4,10E-20	54 Qubit	4,39E-34
			BtcRecover	150 GFLOP	4,97E-14	23 Qubit	8,59E-25
				14 TFLOP	5,33E-16	42 Qubit	1,64E-30
				200 PFLOPS	3,73E-20	54 Qubit	4,00E-34
	Diccionario	5,78E+09	MWB Decryption tool	150 GFLOP	3,38E-14	23 Qubit	5,83E-25
				14 TFLOP	3,62E-16	42 Qubit	1,11E-30
				200 PFLOPS	2,53E-20	54 Qubit	2,72E-34
			BtcRecover	150 GFLOP	3,08E-14	23 Qubit	5,31E-25
				14 TFLOP	3,30E-16	42 Qubit	1,01E-30
				200 PFLOPS	2,31E-20	54 Qubit	2,47E-34
	Targuess	1,35E+09	MWB Decryption tool	150 GFLOP	7,89E-15	23 Qubit	1,36E-25
				14 TFLOP	8,46E-17	42 Qubit	2,60E-31
				200 PFLOPS	5,92E-21	54 Qubit	6,34E-35
			BtcRecover	150 GFLOP	7,18E-15	23 Qubit	1,24E-25
				14 TFLOP	7,70E-17	42 Qubit	2,36E-31
				200 PFLOPS	5,39E-21	54 Qubit	5,77E-35

Ilustración 34 - Estimación tiempos contraseña corta, numérica y con información insuficiente

Longitud corta – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	4,81E+15	MWB Decryption tool	150 GFLOP	2,81E-08	23 Qubit	4,85E-19
				14 TFLOP	3,01E-10	42 Qubit	9,26E-25
				200 PFLOPS	2,11E-14	54 Qubit	2,26E-28
			BtcRecover	150 GFLOP	2,56E-08	23 Qubit	4,42E-19
				14 TFLOP	2,74E-10	42 Qubit	8,42E-25
				200 PFLOPS	1,92E-14	54 Qubit	2,06E-28
	Combinaciones	4,50E+15	MWB Decryption tool	150 GFLOP	2,63E-08	23 Qubit	4,54E-19
				14 TFLOP	2,82E-10	42 Qubit	8,65E-25
				200 PFLOPS	1,97E-14	54 Qubit	2,11E-28
			BtcRecover	150 GFLOP	2,39E-08	23 Qubit	4,13E-19
				14 TFLOP	2,56E-10	42 Qubit	7,88E-25
				200 PFLOPS	1,79E-14	54 Qubit	1,92E-28
	Diccionario	2,78E+15	MWB Decryption tool	150 GFLOP	1,63E-08	23 Qubit	2,80E-19
				14 TFLOP	1,74E-10	42 Qubit	5,35E-25
				200 PFLOPS	1,22E-14	54 Qubit	1,31E-28
			BtcRecover	150 GFLOP	1,48E-08	23 Qubit	2,55E-19
				14 TFLOP	1,58E-10	42 Qubit	4,87E-25
				200 PFLOPS	1,11E-14	54 Qubit	1,19E-28
	Targuess	6,49E+14	MWB Decryption tool	150 GFLOP	3,80E-09	23 Qubit	6,55E-20
				14 TFLOP	4,07E-11	42 Qubit	1,25E-25
				200 PFLOPS	2,85E-15	54 Qubit	3,05E-29
			BtcRecover	150 GFLOP	3,45E-09	23 Qubit	5,96E-20
				14 TFLOP	3,70E-11	42 Qubit	1,14E-25
				200 PFLOPS	2,59E-15	54 Qubit	2,78E-29

Ilustración 35 - Estimación tiempos contraseña corta, numérica, minúsculas y con información insuficiente

Longitud corta – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	1,15E+18	MWB Decryption tool	150 GFLOP	6,74E-06	23 Qubit	1,16E-16
				14 TFLOP	7,22E-08	42 Qubit	2,22E-22
				200 PFLOPS	5,06E-12	54 Qubit	5,42E-26
			BtcRecover	150 GFLOP	6,13E-06	23 Qubit	1,06E-16
				14 TFLOP	6,57E-08	42 Qubit	2,02E-22
				200 PFLOPS	4,60E-12	54 Qubit	4,93E-26
	Combinaciones	1,08E+18	MWB Decryption tool	150 GFLOP	6,30E-06	23 Qubit	1,09E-16
				14 TFLOP	6,75E-08	42 Qubit	2,08E-22
				200 PFLOPS	4,73E-12	54 Qubit	5,07E-26
			BtcRecover	150 GFLOP	5,74E-06	23 Qubit	9,90E-17
				14 TFLOP	6,15E-08	42 Qubit	1,89E-22
				200 PFLOPS	4,30E-12	54 Qubit	4,61E-26
	Diccionario	6,66E+17	MWB Decryption tool	150 GFLOP	3,90E-06	23 Qubit	6,73E-17
				14 TFLOP	4,17E-08	42 Qubit	1,28E-22
				200 PFLOPS	2,92E-12	54 Qubit	3,13E-26
			BtcRecover	150 GFLOP	3,55E-06	23 Qubit	6,12E-17
				14 TFLOP	3,80E-08	42 Qubit	1,17E-22
				200 PFLOPS	2,66E-12	54 Qubit	2,85E-26
	Targuess	1,56E+17	MWB Decryption tool	150 GFLOP	9,10E-07	23 Qubit	1,57E-17
				14 TFLOP	9,75E-09	42 Qubit	3,00E-23
				200 PFLOPS	6,83E-13	54 Qubit	7,31E-27
			BtcRecover	150 GFLOP	8,28E-07	23 Qubit	1,43E-17
				14 TFLOP	8,87E-09	42 Qubit	2,73E-23
				200 PFLOPS	6,21E-13	54 Qubit	6,66E-27

Ilustración 36 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas y con información insuficiente

Longitud corta – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
10	Permutaciones	7,37E+19	MWB Decryption tool	150 GFLOP	4,31E-04	23 Qubit	7,44E-15
				14 TFLOP	4,62E-06	42 Qubit	1,42E-20
				200 PFLOPS	3,23E-10	54 Qubit	3,47E-24
			BtcRecover	150 GFLOP	3,92E-04	23 Qubit	6,77E-15
				14 TFLOP	4,20E-06	42 Qubit	1,29E-20
				200 PFLOPS	2,94E-10	54 Qubit	3,15E-24
	Combinaciones	6,89E+19	MWB Decryption tool	150 GFLOP	4,03E-04	23 Qubit	6,96E-15
				14 TFLOP	4,32E-06	42 Qubit	1,33E-20
				200 PFLOPS	3,02E-10	54 Qubit	3,24E-24
			BtcRecover	150 GFLOP	3,67E-04	23 Qubit	6,33E-15
				14 TFLOP	3,93E-06	42 Qubit	1,21E-20
				200 PFLOPS	2,75E-10	54 Qubit	2,95E-24
	Diccionario	4,26E+19	MWB Decryption tool	150 GFLOP	2,49E-04	23 Qubit	4,30E-15
				14 TFLOP	2,67E-06	42 Qubit	8,20E-21
				200 PFLOPS	1,87E-10	54 Qubit	2,00E-24
			BtcRecover	150 GFLOP	2,27E-04	23 Qubit	3,91E-15
				14 TFLOP	2,43E-06	42 Qubit	7,47E-21
				200 PFLOPS	1,70E-10	54 Qubit	1,82E-24
	Targuess	9,96E+18	MWB Decryption tool	150 GFLOP	5,82E-05	23 Qubit	1,00E-15
				14 TFLOP	6,24E-07	42 Qubit	1,92E-21
				200 PFLOPS	4,37E-11	54 Qubit	4,68E-25
			BtcRecover	150 GFLOP	5,30E-05	23 Qubit	9,14E-16
				14 TFLOP	5,68E-07	42 Qubit	1,74E-21
				200 PFLOPS	3,97E-11	54 Qubit	4,26E-25

Ilustración 37 - Estimación tiempos contraseña corta, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente

Longitud estándar – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	1,00E+15	MWB Decryption tool	150 GFLOP	5,85E-09	23 Qubit	1,01E-19
				14 TFLOP	6,26E-11	42 Qubit	1,92E-25
				200 PFLOPS	4,39E-15	54 Qubit	4,70E-29
			BtcRecover	150 GFLOP	5,32E-09	23 Qubit	9,18E-20
				14 TFLOP	5,70E-11	42 Qubit	1,75E-25
				200 PFLOPS	3,99E-15	54 Qubit	4,28E-29
	Combinaciones	9,35E+14	MWB Decryption tool	150 GFLOP	5,47E-09	23 Qubit	9,44E-20
				14 TFLOP	5,86E-11	42 Qubit	1,80E-25
				200 PFLOPS	4,10E-15	54 Qubit	4,39E-29
			BtcRecover	150 GFLOP	4,97E-09	23 Qubit	8,59E-20
				14 TFLOP	5,33E-11	42 Qubit	1,64E-25
				200 PFLOPS	3,73E-15	54 Qubit	4,00E-29
	Diccionario	5,78E+14	MWB Decryption tool	150 GFLOP	3,38E-09	23 Qubit	5,83E-20
				14 TFLOP	3,62E-11	42 Qubit	1,11E-25
				200 PFLOPS	2,53E-15	54 Qubit	2,72E-29
			BtcRecover	150 GFLOP	3,08E-09	23 Qubit	5,31E-20
				14 TFLOP	3,30E-11	42 Qubit	1,01E-25
				200 PFLOPS	2,31E-15	54 Qubit	2,47E-29
	Targuess	1,35E+14	MWB Decryption tool	150 GFLOP	7,89E-10	23 Qubit	1,36E-20
				14 TFLOP	8,46E-12	42 Qubit	2,60E-26
				200 PFLOPS	5,92E-16	54 Qubit	6,34E-30
			BtcRecover	150 GFLOP	7,18E-10	23 Qubit	1,24E-20
				14 TFLOP	7,70E-12	42 Qubit	2,36E-26
				200 PFLOPS	5,39E-16	54 Qubit	5,77E-30

Ilustración 38 - Estimación tiempos contraseña estándar, numérica y con información insuficiente

Longitud estándar – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	3,33E+23	MWB Decryption tool	150 GFLOP	1,95E+00	23 Qubit	3,37E-11
				14 TFLOP	2,09E-02	42 Qubit	6,42E-17
				200 PFLOPS	1,46E-06	54 Qubit	1,57E-20
			BtcRecover	150 GFLOP	1,77E+00	23 Qubit	3,06E-11
				14 TFLOP	1,90E-02	42 Qubit	5,84E-17
				200 PFLOPS	1,33E-06	54 Qubit	1,43E-20
	Combinaciones	3,12E+23	MWB Decryption tool	150 GFLOP	1,82E+00	23 Qubit	3,15E-11
				14 TFLOP	1,95E-02	42 Qubit	6,00E-17
				200 PFLOPS	1,37E-06	54 Qubit	1,47E-20
			BtcRecover	150 GFLOP	1,66E+00	23 Qubit	2,86E-11
				14 TFLOP	1,78E-02	42 Qubit	5,46E-17
				200 PFLOPS	1,24E-06	54 Qubit	1,33E-20
	Diccionario	1,93E+23	MWB Decryption tool	150 GFLOP	1,13E+00	23 Qubit	1,95E-11
				14 TFLOP	1,21E-02	42 Qubit	3,71E-17
				200 PFLOPS	8,45E-07	54 Qubit	9,06E-21
			BtcRecover	150 GFLOP	1,03E+00	23 Qubit	1,77E-11
				14 TFLOP	1,10E-02	42 Qubit	3,38E-17
				200 PFLOPS	7,69E-07	54 Qubit	8,24E-21
	Targuess	4,50E+22	MWB Decryption tool	150 GFLOP	2,63E-01	23 Qubit	4,54E-12
				14 TFLOP	2,82E-03	42 Qubit	8,66E-18
				200 PFLOPS	1,97E-07	54 Qubit	2,12E-21
			BtcRecover	150 GFLOP	2,40E-01	23 Qubit	4,13E-12
				14 TFLOP	2,57E-03	42 Qubit	7,89E-18
				200 PFLOPS	1,80E-07	54 Qubit	1,93E-21

Ilustración 39 - Estimación tiempos contraseña estándar, numérica, minúsculas y con información insuficiente

Longitud estándar – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	1,24E+27	MWB Decryption tool	150 GFLOP	7,24E+03	23 Qubit	1,25E-07
				14 TFLOP	7,75E+01	42 Qubit	2,38E-13
				200 PFLOPS	5,43E-03	54 Qubit	5,82E-17
			BtcRecover	150 GFLOP	6,59E+03	23 Qubit	1,14E-07
				14 TFLOP	7,06E+01	42 Qubit	2,17E-13
				200 PFLOPS	4,94E-03	54 Qubit	5,29E-17
	Combinaciones	1,16E+27	MWB Decryption tool	150 GFLOP	6,77E+03	23 Qubit	1,17E-07
				14 TFLOP	7,25E+01	42 Qubit	2,23E-13
				200 PFLOPS	5,08E-03	54 Qubit	5,44E-17
			BtcRecover	150 GFLOP	6,16E+03	23 Qubit	1,06E-07
				14 TFLOP	6,60E+01	42 Qubit	2,03E-13
				200 PFLOPS	4,62E-03	54 Qubit	4,95E-17
	Diccionario	7,16E+26	MWB Decryption tool	150 GFLOP	4,18E+03	23 Qubit	7,22E-08
				14 TFLOP	4,48E+01	42 Qubit	1,38E-13
				200 PFLOPS	3,14E-03	54 Qubit	3,36E-17
			BtcRecover	150 GFLOP	3,81E+03	23 Qubit	6,57E-08
				14 TFLOP	4,08E+01	42 Qubit	1,25E-13
				200 PFLOPS	2,86E-03	54 Qubit	3,06E-17
	Targuess	1,67E+26	MWB Decryption tool	150 GFLOP	9,77E+02	23 Qubit	1,69E-08
				14 TFLOP	1,05E+01	42 Qubit	3,22E-14
				200 PFLOPS	7,33E-04	54 Qubit	7,85E-18
			BtcRecover	150 GFLOP	8,89E+02	23 Qubit	1,53E-08
				14 TFLOP	9,53E+00	42 Qubit	2,93E-14
				200 PFLOPS	6,67E-04	54 Qubit	7,15E-18

Ilustración 40 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas y con información insuficiente

Longitud estándar – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
15	Permutaciones	6,33E+29	MWB Decryption tool	150 GFLOP	3,70E+06	23 Qubit	6,39E-05
				14 TFLOP	3,97E+04	42 Qubit	1,22E-10
				200 PFLOPS	2,78E+00	54 Qubit	2,98E-14
			BtcRecover	150 GFLOP	3,37E+06	23 Qubit	5,82E-05
				14 TFLOP	3,61E+04	42 Qubit	1,11E-10
				200 PFLOPS	2,53E+00	54 Qubit	2,71E-14
	Combinaciones	5,92E+29	MWB Decryption tool	150 GFLOP	3,46E+06	23 Qubit	5,98E-05
				14 TFLOP	3,71E+04	42 Qubit	1,14E-10
				200 PFLOPS	2,60E+00	54 Qubit	2,78E-14
			BtcRecover	150 GFLOP	3,15E+06	23 Qubit	5,44E-05
				14 TFLOP	3,38E+04	42 Qubit	1,04E-10
				200 PFLOPS	2,36E+00	54 Qubit	2,53E-14
	Diccionario	3,66E+29	MWB Decryption tool	150 GFLOP	2,14E+06	23 Qubit	3,69E-05
				14 TFLOP	2,29E+04	42 Qubit	7,05E-11
				200 PFLOPS	1,61E+00	54 Qubit	1,72E-14
			BtcRecover	150 GFLOP	1,95E+06	23 Qubit	3,36E-05
				14 TFLOP	2,09E+04	42 Qubit	6,41E-11
				200 PFLOPS	1,46E+00	54 Qubit	1,57E-14
	Targuess	8,55E+28	MWB Decryption tool	150 GFLOP	5,00E+05	23 Qubit	8,63E-06
				14 TFLOP	5,36E+03	42 Qubit	1,65E-11
				200 PFLOPS	3,75E-01	54 Qubit	4,02E-15
			BtcRecover	150 GFLOP	4,55E+05	23 Qubit	7,85E-06
				14 TFLOP	4,87E+03	42 Qubit	1,50E-11
				200 PFLOPS	3,41E-01	54 Qubit	3,66E-15

Ilustración 41 - Estimación tiempos contraseña estándar, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente

Longitud compleja – Solo números:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	1,00E+20	MWB Decryption tool	150 GFLOP	5,85E-04	23 Qubit	1,01E-14
				14 TFLOP	6,26E-06	42 Qubit	1,92E-20
				200 PFLOPS	4,39E-10	54 Qubit	4,70E-24
			BtcRecover	150 GFLOP	5,32E-04	23 Qubit	9,18E-15
				14 TFLOP	5,70E-06	42 Qubit	1,75E-20
				200 PFLOPS	3,99E-10	54 Qubit	4,28E-24
	Combinaciones	9,35E+19	MWB Decryption tool	150 GFLOP	5,47E-04	23 Qubit	9,44E-15
				14 TFLOP	5,86E-06	42 Qubit	1,80E-20
				200 PFLOPS	4,10E-10	54 Qubit	4,39E-24
			BtcRecover	150 GFLOP	4,97E-04	23 Qubit	8,59E-15
				14 TFLOP	5,33E-06	42 Qubit	1,64E-20
				200 PFLOPS	3,73E-10	54 Qubit	4,00E-24
	Diccionario	5,78E+19	MWB Decryption tool	150 GFLOP	3,38E-04	23 Qubit	5,83E-15
				14 TFLOP	3,62E-06	42 Qubit	1,11E-20
				200 PFLOPS	2,53E-10	54 Qubit	2,72E-24
			BtcRecover	150 GFLOP	3,08E-04	23 Qubit	5,31E-15
				14 TFLOP	3,30E-06	42 Qubit	1,01E-20
				200 PFLOPS	2,31E-10	54 Qubit	2,47E-24
	Targuess	1,35E+19	MWB Decryption tool	150 GFLOP	7,89E-05	23 Qubit	1,36E-15
				14 TFLOP	8,46E-07	42 Qubit	2,60E-21
				200 PFLOPS	5,92E-11	54 Qubit	6,34E-25
			BtcRecover	150 GFLOP	7,18E-05	23 Qubit	1,24E-15
				14 TFLOP	7,70E-07	42 Qubit	2,36E-21
				200 PFLOPS	5,39E-11	54 Qubit	5,77E-25

Ilustración 42 - Estimación tiempos contraseña compleja, numérica y con información insuficiente

Longitud compleja – Números y minúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	2,31E+31	MWB Decryption tool	150 GFLOP	1,35E+08	23 Qubit	2,33E-03
				14 TFLOP	1,45E+06	42 Qubit	4,45E-09
				200 PFLOPS	1,01E+02	54 Qubit	1,09E-12
			BtcRecover	150 GFLOP	1,23E+08	23 Qubit	2,12E-03
				14 TFLOP	1,32E+06	42 Qubit	4,05E-09
				200 PFLOPS	9,23E+01	54 Qubit	9,89E-13
	Combinaciones	2,16E+31	MWB Decryption tool	150 GFLOP	1,26E+08	23 Qubit	2,18E-03
				14 TFLOP	1,35E+06	42 Qubit	4,16E-09
				200 PFLOPS	9,48E+01	54 Qubit	1,02E-12
			BtcRecover	150 GFLOP	1,15E+08	23 Qubit	1,99E-03
				14 TFLOP	1,23E+06	42 Qubit	3,79E-09
				200 PFLOPS	8,63E+01	54 Qubit	9,25E-13
	Diccionario	1,34E+31	MWB Decryption tool	150 GFLOP	7,81E+07	23 Qubit	1,35E-03
				14 TFLOP	8,37E+05	42 Qubit	2,57E-09
				200 PFLOPS	5,86E+01	54 Qubit	6,28E-13
			BtcRecover	150 GFLOP	7,11E+07	23 Qubit	1,23E-03
				14 TFLOP	7,62E+05	42 Qubit	2,34E-09
				200 PFLOPS	5,33E+01	54 Qubit	5,72E-13
	Targuess	3,12E+30	MWB Decryption tool	150 GFLOP	1,83E+07	23 Qubit	3,15E-04
				14 TFLOP	1,96E+05	42 Qubit	6,01E-10
				200 PFLOPS	1,37E+01	54 Qubit	1,47E-13
			BtcRecover	150 GFLOP	1,66E+07	23 Qubit	2,87E-04
				14 TFLOP	1,78E+05	42 Qubit	5,47E-10
				200 PFLOPS	1,25E+01	54 Qubit	1,33E-13

Ilustración 43 - Estimación tiempos contraseña compleja, numérica, minúsculas y con información insuficiente

Longitud compleja – Números, minúsculas y mayúsculas:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	1,33E+36	MWB Decryption tool	150 GFLOP	7,77E+12	23 Qubit	1,34E+02
				14 TFLOP	8,33E+10	42 Qubit	2,56E-04
				200 PFLOPS	5,83E+06	54 Qubit	6,25E-08
			BtcRecover	150 GFLOP	7,07E+12	23 Qubit	1,22E+02
				14 TFLOP	7,58E+10	42 Qubit	2,33E-04
				200 PFLOPS	5,30E+06	54 Qubit	5,68E-08
	Combinaciones	1,24E+36	MWB Decryption tool	150 GFLOP	7,27E+12	23 Qubit	1,25E+02
				14 TFLOP	7,79E+10	42 Qubit	2,39E-04
				200 PFLOPS	5,45E+06	54 Qubit	5,84E-08
			BtcRecover	150 GFLOP	6,61E+12	23 Qubit	1,14E+02
				14 TFLOP	7,08E+10	42 Qubit	2,18E-04
				200 PFLOPS	4,96E+06	54 Qubit	5,31E-08
	Diccionario	7,68E+35	MWB Decryption tool	150 GFLOP	4,49E+12	23 Qubit	7,75E+01
				14 TFLOP	4,81E+10	42 Qubit	1,48E-04
				200 PFLOPS	3,37E+06	54 Qubit	3,61E-08
			BtcRecover	150 GFLOP	4,09E+12	23 Qubit	7,06E+01
				14 TFLOP	4,38E+10	42 Qubit	1,35E-04
				200 PFLOPS	3,07E+06	54 Qubit	3,29E-08
	Targuess	1,79E+35	MWB Decryption tool	150 GFLOP	1,05E+12	23 Qubit	1,81E+01
				14 TFLOP	1,12E+10	42 Qubit	3,45E-05
				200 PFLOPS	7,87E+05	54 Qubit	8,43E-09
			BtcRecover	150 GFLOP	9,55E+11	23 Qubit	1,65E+01
				14 TFLOP	1,02E+10	42 Qubit	3,14E-05
				200 PFLOPS	7,16E+05	54 Qubit	7,67E-09

Ilustración 44 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas y con información insuficiente

Longitud compleja – Números, minúsculas, mayúsculas, caracteres especiales:

Longitud Maxima	Tecnica	Estimado de contraseñas	Herramienta	Potencial FLOPS	Tiempo Hrs	Potencial Qubit	Tiempo Hrs
20	Permutaciones	5,44E+43	MWB Decryption tool	150 GFLOP	3,18E+20	23 Qubit	5,49E+09
				14 TFLOP	3,41E+18	42 Qubit	1,05E+04
				200 PFLOPS	2,38E+14	54 Qubit	2,56E+00
			BtcRecover	150 GFLOP	2,89E+20	23 Qubit	4,99E+09
				14 TFLOP	3,10E+18	42 Qubit	9,53E+03
				200 PFLOPS	2,17E+14	54 Qubit	2,33E+00
	Combinaciones	5,08E+43	MWB Decryption tool	150 GFLOP	2,97E+20	23 Qubit	5,13E+09
				14 TFLOP	3,19E+18	42 Qubit	9,79E+03
				200 PFLOPS	2,23E+14	54 Qubit	2,39E+00
			BtcRecover	150 GFLOP	2,71E+20	23 Qubit	4,67E+09
				14 TFLOP	2,90E+18	42 Qubit	8,91E+03
				200 PFLOPS	2,03E+14	54 Qubit	2,17E+00
	Diccionario	3,14E+43	MWB Decryption tool	150 GFLOP	1,84E+20	23 Qubit	3,17E+09
				14 TFLOP	1,97E+18	42 Qubit	6,05E+03
				200 PFLOPS	1,38E+14	54 Qubit	1,48E+00
			BtcRecover	150 GFLOP	1,67E+20	23 Qubit	2,89E+09
				14 TFLOP	1,79E+18	42 Qubit	5,51E+03
				200 PFLOPS	1,25E+14	54 Qubit	1,34E+00
	Targuess	7,34E+42	MWB Decryption tool	150 GFLOP	4,29E+19	23 Qubit	7,41E+08
				14 TFLOP	4,60E+17	42 Qubit	1,41E+03
				200 PFLOPS	3,22E+13	54 Qubit	3,45E-01
			BtcRecover	150 GFLOP	3,91E+19	23 Qubit	6,74E+08
				14 TFLOP	4,19E+17	42 Qubit	1,29E+03
				200 PFLOPS	2,93E+13	54 Qubit	3,14E-01

Ilustración 45 - Estimación tiempos contraseña compleja, numérica, minúsculas, mayúsculas, caracteres especiales y con información insuficiente

CAPÍTULO 4. CONCLUSIONES

4.1 VERIFICACIÓN, CONTRASTE Y EVALUACIÓN DE LOS OBJETIVOS

Conclusión sobre la hipótesis:

Luego de realizar la investigación y basado en los resultados obtenidos se puede concluir que el potencial que proporciona la computación cuántica, combinado con técnicas para poder generar posibles contraseñas y las herramientas mencionadas en la investigación nos indica que teóricamente se puede realizar la apertura de un monedero o billetera virtual si el dueño de la mismo olvido su contraseña.

Conclusión sobre el objetivo general:

Se presentar múltiples alternativas en la matriz de tiempos, dando al lector o persona que presente el problema planteado, una serie de opciones que combinan todos los factores investigados y que puede llegar a implementar para acceder a las criptomonedas almacenadas en estas billeteras o monederos virtuales.

Conclusión sobre los objetivos específicos:

Durante la investigación se presentaron y analizaron las técnicas criptográficas que son utilizadas actualmente para asegurar las billeteras o monederos virtuales dando así una perspectiva general del nivel de seguridad con el que cuentan actualmente estos sistemas.

Adicionalmente se investigó los avances y aplicaciones que ha tenido la computación cuántica hasta el momento y como se ha implementado en la actualidad frente a la seguridad informática, dando así un pronóstico general de que las técnicas criptográficas actuales podrán ser obsoletas en un futuro.

Para finalizar se generó una matriz con tiempos estimados en la apertura de una billetera virtual, teniendo en cuenta varios aspectos como lo es el potencial cuántico, la longitud y característica de la contraseña, las herramientas y técnicas utilizadas y lo más importante la información que el dueño de la billetera puede recordar referente a su contraseña, llegando así a tener unos tiempos teóricos estimados.

Conclusiones generales:

El proyecto puede brindar distintos tipos de soluciones o alternativas para lograr el objetivo principal, sin embargo, puede llegar a “complementarse” con otras técnicas o tecnologías como inteligencia artificial.

Los resultados de la investigación están basados en datos teóricos y puede que en la práctica exista algún tipo de desviación en los tiempos o resultados estimados.

4.2 APORTES ORIGINALES

La elaboración de la matriz cuenta con cálculos basados en la supremacía cuántica y en cómo se mide el rendimiento de la computación tradicional, de allí se realiza una estimación teórica de cuantas contraseñas pueden ser procesadas por segundo de acuerdo al potencial en FLOPS y en Qubits.

4.3 TRABAJOS O PUBLICACIONES DERIVADAS

Considero que basado en esta investigación se puede llegar a generar los siguientes trabajos:

- Potencial de la computación cuántica para otras áreas que requieran un gran procesamiento como por ejemplo simulaciones espaciales, desarrollo de medicamentos, materiales, etc.

- Soluciones basas en criptografía cuántica, teniendo en cuenta que teóricamente el potencial de la computación cuántica dejara obsoletos los actuales algoritmos de encriptación.

- Auditoria en la seguridad informática implementada en alguna empresa utilizando las técnicas mencionadas en la investigación.

CAPÍTULO 5. PROSPECTIVA DEL TRABAJO DE GRADO

5.1 LINEAS DE INVESTIGACIÓN FUTURAS

- Criptografía cuántica.

- Criptomonedas, Blockchain y billeteras virtuales.

- Diversas formas de asegurar y recuperar fácilmente criptoactivos.

5.2 TRABAJOS DE INVESTIGACIÓN FUTUROS

- Implementación de inteligencia artificial para hacer un perfil de la persona y generar combinaciones más precisas.

- Extender la funcionalidad a billeteras en frio que solo cuentan con un número limitado de intentos.

REFERENCIAS WEB

[1]. Bitcobie, Qué es una Wallet y cómo se crea [En línea]. Disponible en: https://www.bitcobie.com/wallet/ [Accedido: 20–Enero-2021]

[2]. Bit2Me, ¿Qué son las Cold Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-cold-wallets/ [Accedido: 4–Febrero-2021]

[3]. Bit2Me, ¿Qué son las paper wallets o monederos de papel? [En línea]. Disponible en: https://academy.bit2me.com/monedero-papel-bitcoin-paper-wallet/ [Accedido: 6–Febrero-2021]

[4]. Bit2Me, ¿Qué son las Hardware Wallets? [En línea]. Disponible en: https://academy.bit2me.com/hardware-wallets/ [Accedido: 25–Febrero-2021]

[5]. Bit2Me, ¿Qué son las Hot Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-hot-wallets/ [Accedido: 3–Marzo-2021]

[6]. SPRO, How to Develop a Bitcoin Wallet App? [En línea]. Disponible en: https://s-pro.io/blog/how-to-develop-a-bitcoin-wallet-app [Accedido: 15–Marzo-2021]

[7]. Bit2Me, ¿Qué son las HD Wallets? [En línea]. Disponible en: https://academy.bit2me.com/que-son-las-hd-wallets/ [Accedido: 27–Marzo-2021]

[8]. Bitcoin, Wallet [En línea]. Disponible en: https://en.bitcoin.it/wiki/Wallet [Accedido: 1–Abril-2021]

[9]. Bit2Me, Criptografia SHA-256 [En línea]. Disponible en: https://academy.bit2me.com/wp-content/uploads/2019/10/Criptography_SHA_256_es.pdf [Accedido: 3–Abril-2021]

[10]. Quiora, ¿Es posible romper una SHA-256? [En línea]. Disponible en: https://es.quora.com/Es-posible-romper-una-SHA-256 [Accedido: 18–Enero-2021]

[11]. Hardzone, Así funciona el sistema de cifrado AES-256 bits, ¿es realmente seguro? [En línea]. Disponible en: https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/ [Accedido: 10–Abril-2021]

[12]. El Diario, Dime tu contraseña y te diré quién eres: hay una historia fascinante en cada clave [En línea]. Disponible en: https://www.eldiario.es/hojaderouter/seguridad/contrasenas-seguridad-psicologia-historias_1_4271346.html [Accedido: 12–Abril-2021]

[13]. Magnet, Poder leer P4L4BR4S con NÚM3R05 no es tan difícil como creías, todo está en tu cerebro [En línea]. Disponible en: https://magnet.xataka.com/un-mundo-fascinante/poder-leer-p4l4br4s-con-num3r05-no-es-tan-dificil-como-creias-todo-esta-en-tu-cerebro [Accedido: 12–Abril-2021]

[14]. Psychology Today, Passwords reveal your personality [En línea]. Disponible en: https://www.psychologytoday.com/intl/articles/200201/passwords-reveal-your-personality [Accedido: 18–Abril-2021]

[15]. La Arena, Pemrutaciones [En línea]. Disponible en: https://danacaweb.com/permutaciones.html [Accedido: 30–Abril-2021]

[16]. AAA Math, Combinaciones [En línea]. Disponible en: https://www.aaamatematicas.com/sta-combin.htm [Accedido: 1–Mayo-2021]

[17]. GitHub, Diccionarios de: usuarios, passwords, xss, dorks [En línea]. Disponible en: https://github.com/hackingyseguridad/diccionarios [Accedido: 1–Mayo-2021]

[18]. El Pais, Este sistema adivina las contraseñas (y casi no falla) [En línea]. Disponible en:

https://elpais.com/tecnologia/2016/11/09/actualidad/1478694955_288239.html [Accedido: 05–Mayo-2021]
[19]. BTCRecover, Getting Started [En línea]. Disponible en: https://btcrecover.readthedocs.io/en/latest/ [Accedido: 6–Mayo-2021]
[20]. NIC Argentina, ¿Qué es criptografía? [En línea]. Disponible en: http://nic.ar/es/enterate/novedades/que-es-criptografia. [Accedido: 20–Enero-2020]
[21]. Cointelegraph, ¿Qué es criptomoneda? [En línea]. Disponible en: https://es.cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies [Accedido: 20–Enero-2020]
[22]. Bit2Me, Qué es una wallet o monedero de criptomonedas [En línea]. Disponible en: https://academy.bit2me.com/wallet-monederos-criptomonedas/ [Accedido: 20–Enero-2020]
[23]. BBVA, La computación cuántica y el futuro de la criptografía [En línea]. Disponible en: https://www.bbvanexttechnologies.com/la-computacion-cuantica-y-el-futuro-de-la-criptografia-la-criptografia-post-cuantica/ [Accedido: 20–Enero-2020]
[24]. Blockchainservices, ¿Qué es un monedero o cartera virtual? [En línea]. Disponible en: http://www.blockchainservices.es/novedades/que-es-un-monedero-o-cartera-virtual/ [Accedido: 20–Enero-2020]
[25]. Economipedia, Criptomoneda [En línea]. Disponible en: https://economipedia.com/definiciones/criptomoneda.html [Accedido: 20–Enero-2020]
[26]. Xataka, Computación cuántica: qué es, de dónde viene y qué ha conseguido [En línea]. Disponible en: https://www.xataka.com/ordenadores/computacion-cuantica-que-es-de-donde-viene-y-que-ha-conseguido [Accedido: 20–Enero-2020]
[27]. Tecnología, ¿Qué es la Criptografía? [En línea]. Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/ [Accedido: 20–Enero-2020]
[28]. Welive Security, Blockchain: qué es, cómo funciona y cómo se está usando en el mercado [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/ [Accedido: 20–Enero-2020]