Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

RI5C: Una Metodología para la Evaluación de un Sistema de Criptodivisas

T E S I S

Que para optar por el grado de:

Doctor en Ciencias de la Administración

P*resenta:*

Everardo J. Barojas-Méndez

C*omité Tutor:*

Tutor Principal Dr. Abdolreza Rashnavady Nodjoumi,
División de Estudios de Posgrado,
Facultad de Contaduría y Administración, UNAM

Dra. María Saiz Santos,
Facutad de Ciencias Económicas y Empresariales,
UPV/EHU

Dr. Fernando Ramírez Alatriste,
Dinámica no Lineal y Sistemas Complejos,
Universidad Autónoma de la Ciudad de México

Ciudad de México, 12 de julio de 2020

A mi madre y padre.

Índice

Índice de figuras

Índice de cuadros

RI5C: Una Metodología para la Evaluación de un Sistema de Criptodivisas

Resumen

Poco más de 10 años después de la génesis de Bitcoin, el primer activo digital habilitado por criptografía,[1] hemos visto una nueva categoría de activos financieros emerger. Con ello, una gran cantidad de criptodivisas han generado un mercado secundario altamente líquido. El valor de este mercado de activos basados en criptodivisas ha crecido enormemente, en su máximo histórico hasta $829 millones de millones de dólares Coinmarketcap (2018), equivalente al producto interno bruto de México en el 2005 The World Bank (2020). Durante el 2017 se vivió una burbuja financiera dentro de este ecosistema emergente, en la cual estos activos se valorizaron con tasas de crecimiento exponenciales y que hicieron eco a las valoraciones de acciones de empresas tecnológicas en la burbuja *PuntoCom*. Uno de los factores significativos que contribuyeron a esta burbuja, fue la introducción de un nuevo método de emisión de activos digitales, que en el 2017 no seguía ninguna regulación. La emisión de estos activos se lleva a cabo a través de redes descentralizadas, como Bitcoin o Ethereum, en donde cualquier individuo con capacidad técnica puede emitir un activo digital, mientras que los inversionistas participantes pueden liquidar estos activos en mercados secundarios. El objetivo de esta investigación es encontrar un modelo de evaluación para estos sistemas de criptodivisas y transmitir el panorama económico y social que las rodea. En esta investigación se propone una metodología para evaluar un sistema de criptodivisas basado en la cadena de bloques, en forma de una herramienta de software original distribuida con una licencia de código abierto, de tal forma que la propia metodología propuesta, llamada RI5C, es el resultado principal de esta investigación.

Keywords— Administración, Bitcoin, Riesgo, Blockchain, Cadena de Bloques

[1] También llamado criptodivisa

1. Introducción

Durante la crisis financiera del 2008 el gobierno de los Estados Unidos de América rescató a varios bancos con el proyecto de "Ley de Emergencia Económica y Estabilización del 2008" Emergency Economic Stabilization Act (2008), esta legislación asignó $700,000 millones de dólares para la re-compra de activos tóxicos de lo bancos. Estos mismos activos tóxicos, provenientes en gran parte de hipotecas de alto riesgo, fueron una causa importante de la crisis Duca et al. (2011). De un modo semejante, el gobierno del Reino Unido hizo un paquete de rescate de $850,000 millones de dólares Alastair Darling (2008). Con cotidianidad alarmante vimos fraudes masivos ocurrir en instituciones tradicionales, desde el fraude de Bernie Madoff[2] hasta la reciente perdida de $1,700 millones de dólares del banco nacional de Punjab en Mumbai Kolte and Wagh (2019). Los rescates bancarios, junto con la alta frecuencia de fraudes en la industria de valores financieros provocaron una crisis de confianza en instituciones financieras centralizadas, lo cual motivó a un grupo de desarrolladores independientes a la búsqueda de un sistema financiero menos centralizado Casey and Vigna (2018).

La tecnología que permite la generación e intercambio de criptodivisas parece ser una consecuencia directa de esta falta de confianza global en instituciones financieras tradicionales. Esta tecnología fue propuesta originalmente para crear un "Sistema de Dinero Electrónico sin Intermediarios" Nakamoto (2008), atribuida a un seudónimo nombrado como Satoshi Nakamoto y publicado como literatura gris mientras los rescates globales del 2008 sucedían. Desde que la capitalización de los bitcoin en circulación rebasó los $10,000 millones de dólares a finales del 2016, las noticias de criptodivisas han sido frecuentes en medios financieros, lo cual los ha convertido en parte de la cultura financiera del siglo XXI. Parece ser que la tecnología subyacente de registros distribuidos emerge como una innovación que puede, por si sola, desprender nuevos modelos de negocio basados en transparencia y descentralización para la industria tecnológica y financiera. La importancia tecnológica de la creación del Bitcoin ha sido comparada con la creación del Internet Andersen (2016), sin embargo hay evidencia que apunta a un impacto en la evolución en el concepto legal, financiero y operativo de una corporación. Un buen ejemplo son los cambios regulatorios que se han hecho en

[2] Por más de 10 años, Bernard Madoff ejecutó estrategias falsas de compra venta de activos que resultaron en $65,000 millones de dólares en pérdidas.

Wyoming, EUA House Bill No. HB0185 (2019) que permiten a corporaciones constituidas bajo su legislación emitir certificados de acciones representados por una criptodivisa. Otro ejemplo son los cambios legislativos en Malta, donde desde junio de 2018 se generó la MDIA, (que por sus siglas en inglés significa Malta Digital Innovation Authority) y la subsecuente legislación *TAS*, para el registro de auditores y administradores y certificación de plataformas de criptodivisas Schembri (2018). Estos cambios regulatorios inciden directamente en la operación y gobernanza corporativa, tomando ventaja clara en el manejo de acciones como activos digitales, agilizando el proceso de emisión de acciones, levantamiento de capital, votación y auditoría.

1.1. La crisis de COVID-19 en el 2020

El 31 de diciembre del 2019, la Organización Mundial de la Salud (OMS) recibió alertas de autoridades en China de un cúmulo de casos de pulmonía viral de causa desconocida en Wuhan, la capital de la provincia de Hubei. El 30 de enero del 2020, la OMS declaró una emergencia pública internacional, con apenas 7,818 casos confirmados globalmente. Hacia julio del 2020 hay casi 13 millones de casos confirmados, con 571,571 muertes COVID-19 Pandemic (2020). Los efectos de la pandemia de COVID-19 han ocasionado una recesión financiera y de salud internacional de gran impacto.[3]

Aunque la intervención para rescatar a empresas en quiebra data a la presidencia de Franklin D. Roosevelt en 1933, durante la Gran Depresión en EUA, tal vez los rescates gubernamentales más significativos han surgido durante la pandemia de COVID-19. En abril del 2020 casi 4 millones de millones de dólares han sido desplegados para intentar mantener la economía global a flote, este número ha ido en aumento Coronavirus Bailouts (2020).

Durante la crisis financiera provocada por esta pandemia, hemos visto un colapso en el precio del petróleo, un choque a la bolsa de valores en marzo del 2020 y tasas de desempleo que no se veían desde la Gran Depresión de 1929. En los EUA se registra oficialmente un 13 % de desempleo Coronavirus disease (COVID-2019) situation reports (2020) y un 10.7 % en México de acuerdo a Jonathan Heath, subgobernador del Banco de México. La confianza

[3] Aunque esta investigación estuvo terminada desde octubre del 2019, se agregó algo de información acerca de la pandemia COVID-19 ya que es relevante para el objeto de estudio

en instituciones financieras tradicionales está en un bajo histórico, mientras que el precio de bitcoin ha crecido en un 150 %.

Las características de descentralización y la alta liquidez internacional de los mercados de criptodivisas han sido un puerto seguro para inversionistas que quieren cubrir un riesgo financiero presente en la pandemia. Es en este marco histórico de crisis, que las criptodivisas han tomado fuerza y se han convertido en un activo digital regulado y aceptado en los mercados financieros más importantes del mundo.

1.2. Planteamiento del Problema

Durante los primeros tres cuartos del 2017, diversas empresas tecnológicas alrededor del mundo acumularon 2,300 millones de dólares Coinschedule (2017) en inversión a través de criptodivisas. Por un tiempo en el 2017 (ver Figura 1), la cantidad de capital desplegada mensualmente en eventos de generación de criptodivisas fue mayor a la del capital de riesgo invertido en empresas tecnológicas. La primera vez que esto sucede en la historia.

Tan sólo en los primeros 6 meses del 2017, se desplegó, a través de eventos de generación de criptodivisas, una cantidad de capital comparable a la que todo México invirtió en la industria de capital de riesgo desde sus inicios y hasta el 2016 Chelén and Bello (2014). Hacia el 2020 aún se entiende muy poco de las criptodivisas, los eventos de generación, colocación primaria y sus mercados secundarios. Aún no existen herramientas, ni estándares para entender cómo se puede evaluar el funcionamiento de una criptodivisas.

1.3. Justificación y pertinencia de la investigación en criptodivisas

El crecimiento que ha tenido el sistema de Bitcoin, mostrado en la Figura 2, ha mostrado características diferentes a las de cualquier tipo de activo. Es importante en materia financiera, en materia fiscal y en materia comercial. Este movimiento económico parece señalar el nacimiento de un nuevo tipo de activo con rendimientos diferentes, que por su complejidad y la velocidad con la que se ha desarrollado, es poco comprendido y poco estudiado por el gremio académico.

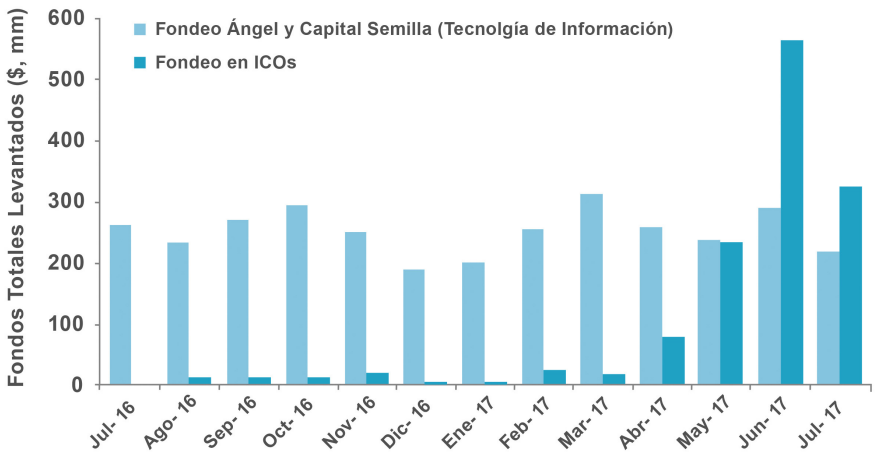


Figura 1: Capital desplegado a través de los 92 primeros eventos de generación de criptodivisas vs. capital desplegado por industria de capital de riesgo, fuente de CB Insights (2017) y Coinschedule (2017).

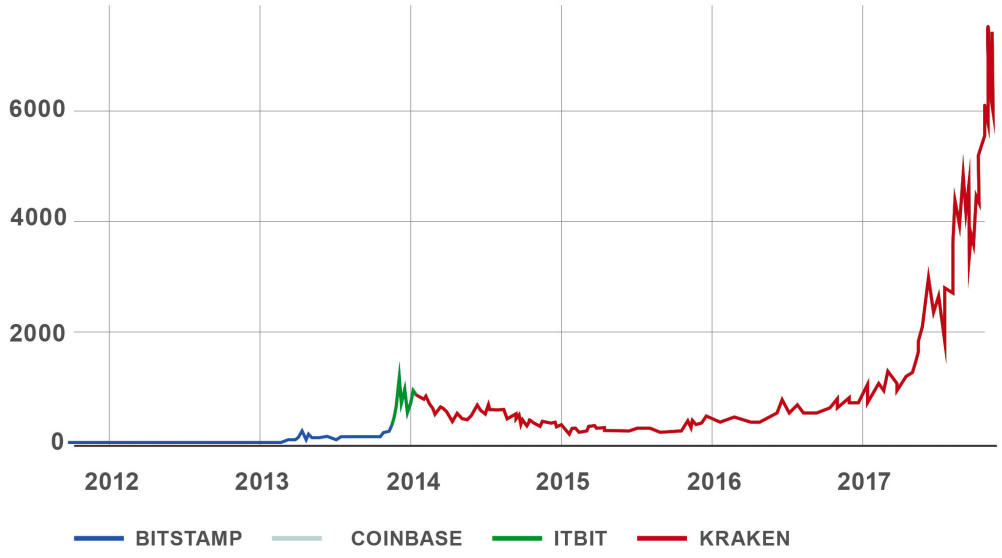


Figura 2: Histórico de precio BTC contra Dólar americano, datos de Bitstamp, Coinbase, ITbit y Kraken. Hacia finales de 2019 el precio actual está cerca de USD $8,000.00 dólares americanos. Generación propia, data original de Bitcoinity (2017).

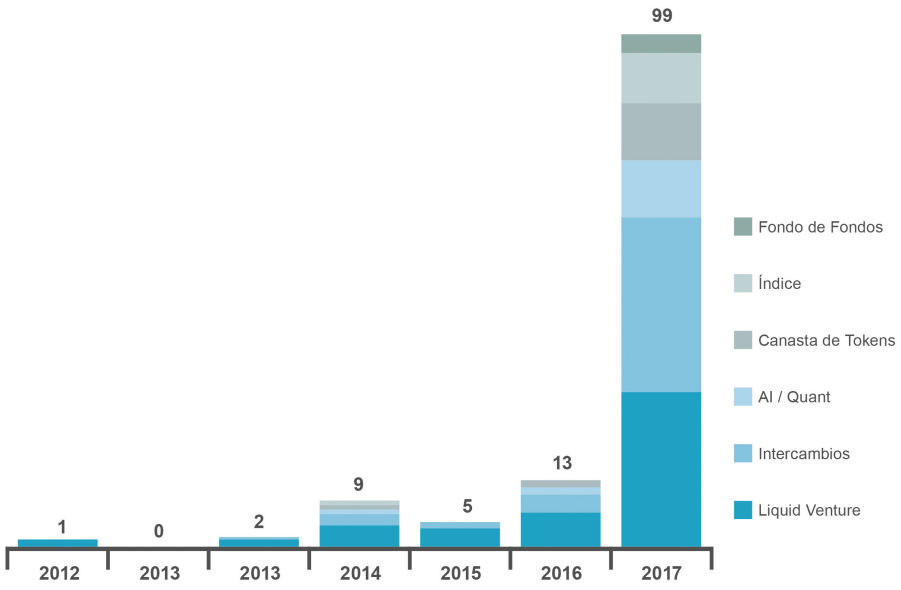


Figura 3: Inversión institucional en criptodivisas. Fuente, Autonomous Next 2018.

Hay que notar que la inversión en el sector ha crecido exponencialmente, como se puede ver en la Figura 3. Conforme el dinero institucional comienza a fluir en el sector, que se ilustra en un histórico de inversión en tecnologías relacionadas a Bitcoin y la cadena de bloques en la Figura 4, y el sector crece a pasos agigantados, es casi imposible no hacer un paralelo con la introducción del Internet a principios de los dos miles y la subsecuente burbuja DotCom.

Notoriamente, un estudio de redes de Bitcoin Griffin and Shams (2018), logró demostrar que una criptodivisa alterna, conocida como Tether, se utilizó durante el 2017 para manipular el precio de Bitcoin. Este es un excelente ejemplo de cómo un estudio de redes puede utilizarse para comprender el comportamiento de estos novedosos activos.

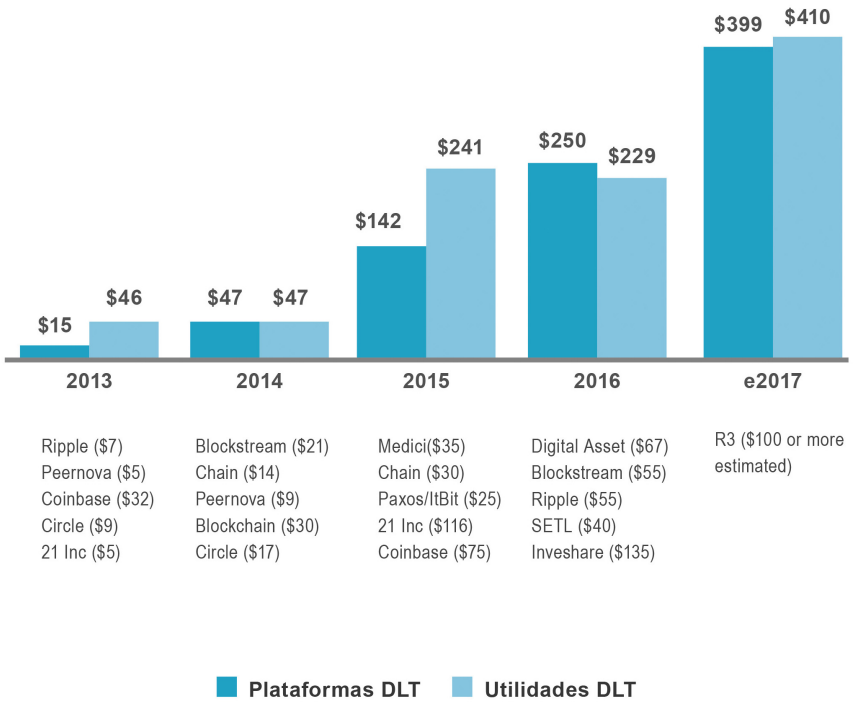


Figura 4: Inversión externa en tecnología de registros descentralizados y derivados Aite (2017).

1.3.1. La inversión de capital en la sociedad

En países desarrollados, hay indicios de que a mayor emprendimiento hay un impacto macro-económico positivo y que su crecimiento está en el interés del público general Amorós and Bosma (2015). De acuerdo con Minniti and Lévesque (2010), el bienestar que estas pequeñas empresas traen, está en el núcleo del desarrollo económico positivo. La Figura 5 sugiere una correlación importante entre el tamaño de una economía y la magnitud total de su inversión en capital de riesgo, cabe aclarar que un evento de generación de criptodivisas puede actuar como una forma de levantamiento de capital. Esta investigación pretende contribuir al entendimiento de la emisión y comportamiento de un sistema de criptodivisas, de tal modo que se facilite administrar el riesgo de participar, como inversionista, usuario o desarrollador. Está claro que una inversión y ejecución exitosa tienen un impacto positivo para el emprendedor también, y por ende es de interés nacional.

1.3.2. Alternativas de inversión local

Para que un ecosistema de inversión funcione, se tiene que lograr el retorno del capital de inversión. Los mecanismos de retorno de inversión más comunes en los casos emblemáticos, son:

1. Colocación primaria a la bolsa de valores,
2. Fusiones y adquisiciones,
3. Convertir a la empresa en rentable, y regresar dividendos sobre utilidades,
4. Emisión de un activo electrónico y colocación primaria.

Todos estos procesos son más rápidos y ágiles cuando el capital es percibido a través de un evento de generación de criptodivisas.

Se estima que entre el 2012 y 2018 haya una inversión total de un millón de millones de dólares en empresas startup Chelén and Bello (2014). La inversión es alta, sin embargo, es un mercado con poca liquidez y ningún ejemplo de crecimiento comparable a los unicornios de Silicon Valley. Hay tres cosas importantes que resaltar:

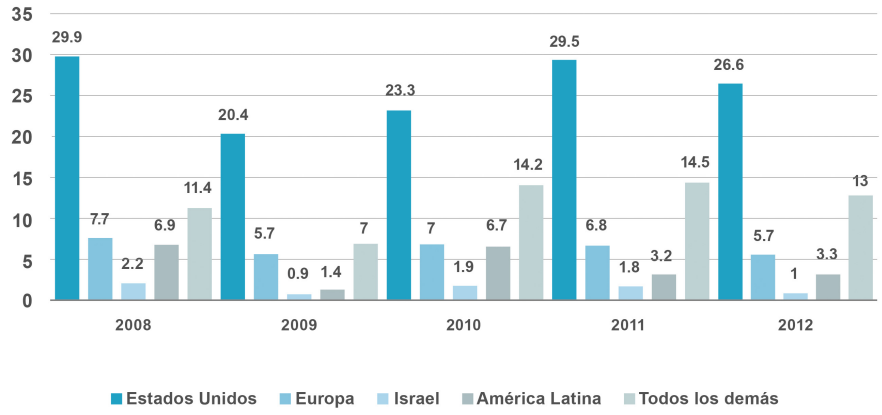


Figura 5: Capital de riesgo invertido por región, fuente: Con datos de Chelén and Bello (2014).

1. En México, las fuentes y criterios de inversión son diferentes, unidas a un ambiente regulatorio y legal con pocos incentivos y que se encuentra en los primeros pasos de crecimiento.

2. El mercado de salidas públicas (la Bolsa Mexicana de Valores) tiene una liquidez más de cien veces menor a la de los EUA Banco Mundial (2015), por lo que una salida pública no es igual de factible.

3. Por su lado, el mercado de fusiones y adquisiciones está concentrado en corporaciones que ya cotizan en la bolsa, el 30 % en bienes raíces Seale (2014) y es varias veces menor al de los EUA Seale (2014) Schwab Advisor Service News (2015). En el caso de Israel,

debido a su relación cercana a los EUA, hay fusiones y adquisiciones que toman lugar en el mercado estadounidense Senor and Singer (2009).

Por ello, para mercados en vías de desarrollo como México, ofrecen una avenida atractiva para el desarrollo de negocios en la generación, colocación primaria y venta secundaria de criptodivisas, especialmente desde el punto de vista del emprendedor, que puede acceder a mercados de mucho mayor liquidez.

1.3.3. Justificación de la Investigación para Diferentes Sectores

Se puede ver una justificación con base en interés de sectores importantes que derivan beneficios potenciales significativos:

1. **Las autoridades responsables de formular políticas públicas**, pues es un tema complejo, no estudiado y con alto riesgo para la sociedad en general. Es de particular interés en México para la Comisión Nacional Bancaria y de Valores, o su equivalente,[4] cuya principal función principal es supervisar y regular a las entidades que conforman el sistema financiero Mexicano. Adicionalmente, una herramienta como la que se propone en esta investigación, puede ayudar a los legisladores y auditores a entender qué está sucediendo en estos eventos.

2. **La comunidad académica**, con múltiples líneas de investigación nuevas y sin metodologías disponibles. Se muestra como un tema apropiado para la comunidad académica, en donde se presenta una notoria falta de información y conocimiento del tema. Para avanzar la ciencia de la administración en materia de criptodivisas, se necesitan herramientas para generar y transferir el conocimiento necesario para evaluar estos sistemas.

3. **La sociedad en general**, pues un ecosistema que permita el acceso a inversiones de alto rendimiento le ofrece oportunidades nuevas y mejores a posibles individuos, que de otro modo, se verían limitados por las inversiones de la banca tradicional, con rendimientos que habitualmente son negativos.

[4] Su equivalente en los EUA es la Security and Exchange Commission y en España la CNMV, Comisión Nacional del Mercado de Valores

4. **Comunidad de código abierto**, en donde también hacen falta metodologías para el análisis y desarrollo de estos sistemas. Empujar la ciencia en la evaluación de estos sistemas conlleva una mejora en el desarrollo y manutención. Un efecto secundario es tener un entendimiento superior de lo que sucede en estos sistemas, y a crear una nueva generación de mejores productos.

5. **La policía cibernética e investigadores privados**. En el 2015 Kathryn Haun, en aquel entonces coordinadora de divisas digitales del departamento de justicia de los EUA, dirigió un juicio contra el sitio "The Silk Road", un mercado negro operado como un servicio oculto accesible sólo a través del navegador Tor. La investigación comenzó en el 2011 y fue el primer caso en que el FBI investigó crímenes relacionados a criptodivisas. Después de analizar las transacciones públicas guardadas en la cadena de bloques, en el 2015 pudieron sentenciar al autor intelectual, gracias a un análisis de datos profundo de la data en la cadena de bloques Haun (2013). Las agencias de ciber-seguridad públicas y privadas tienen una gran necesidad de herramientas faciliten la evaluación de sistemas de criptodivisas y contribuyen fuertemente a la administración pública.

6. **La autoridad fiscal**, la autoridad fiscal podría usar un análisis de redes para rastrear a individuos o instituciones que hayan adquirido, o utilizado criptodivisas.

Sin embargo, la mayor pertinencia de la investigación, es la propia novedad del tema. Con poco más de 10 años de existencia.[5] existen muy pocos artículos publicados y las opiniones en el tema son aún divergentes y poco académicas, lo cual dificulta la investigación, pues la búsqueda de fuentes veraces requiere de una investigación extenuante. Como hemos visto, la mayor parte de la bibliografía es publicada por avenidas informales y aún no existen metodologías académicas para su estudio.

Conforme la economía de Bitcoin y otras criptodivisas crece en tamaño y alcance, se vuelve cada vez más importante entender los componentes y jugadores clave. Sin embargo, esta tarea ha sido torpe y difícil, dado que aunque la data es técnicamente pública, la cantidad de transacciones es enorme y muy difícil de manejar y por si sola, cada transacción individual

[5] Si consideramos la publicación del documento de Satoshi Nakamoto Nakamoto (2008).

no tiene suficiente información para ser valioso. El valor de esta investigación se centra en entregar una herramienta original y fácil de utilizar para que el usuario pueda observar y evaluar la estructura de transacciones de cualquier sistema de criptodivisas.

1.4. Preguntas de Investigación

Pregunta Central

¿Cómo se puede evaluar un sistema de criptodivisas?

Preguntas Subyacentes

- ¿Cómo se puede extraer data de la cadena de bloques y modelar la composición de un sistema de criptodivisas?
- ¿Cómo se puede utilizar la data pública de la cadena de bloques para aumentar el entendimiento de un sistema basado en la cadena de bloques?

1.5. Objetivos

1.5.1. General

Generar una metodología para la evaluación y entendimiento de un sistema de criptodivisas.

1.5.2. Específicos

1. Desarrollar la tecnología para la extracción, estandarización y visualización de un modelo de datos de una cadena de bloques.
2. Implementar la herramienta tecnológica de fuente abierta para visualizar e interactuar con la data pública de la cadena de bloques y facilitar su entendimiento, la identificación de patrones y por consiguiente su evaluación.

1.6. Hipótesis

1.6.1. H1: Hipótesis primera

Una metodología para la evaluación de un sistema de criptodivisas permitirá entender, analizar y evaluar las cualidades de un sistema de criptodivisas.

1.6.2. H2: Hipótesis segunda

Modelar la data pública de una cadena de bloques como una red de transacciones es una representación adecuada para evaluación de un sistema de criptodivisas.

1.6.3. H3: Hipótesis tercera

El uso de la herramienta de visualización interactiva permite la identificación de patrones de una cadena de bloques, el entendimiento de sus participantes y la evaluación cualitativa visual.

1.6.4. Alcance

Debido a la naturaleza del objeto de investigación, el alcance es global y no está sujeto a limitantes geográficas. El trabajo comprende un análisis de redes de los datos públicamente accesibles de contratos para la generación de criptodivisas que se han desarrollado en la red de Ethereum hasta el momento del estudio.

Se pretende generar una base de conocimiento y entendimiento que aumente el entendimiento de estos activos con el objetivo de desarrollar una metodología para la evaluación de sistemas de criptodivisas. La evaluación de diversos tipos de riesgo y su propia administración, quedan fuera del alcance de esta investigación, ya que el tema demanda un entendimiento y evaluación de los sistemas antes de poder profundizar.

El alcance del proyecto comprende la generación de un repositorio de código distribuido con licencia de código abierto de tal modo que la comunidad académica tenga acceso a una

herramienta original de evaluación para sistemas de criptodivisas y se pueda continuar con las siguientes líneas de investigación del proyecto, empujando la ciencia.

Debido a la naturaleza masiva de los datos de la red de Ethereum,[6] se buscará analizar sub-conjuntos de datos delimitados por contratos inteligentes; en caso de que aún ese sub-conjunto fuera muy extenso, se delimitará por fechas o número de transacciones.

1.6.5. Metodología de Investigación

En este sub-capítulo de desarrollan los elementos metodológicos de la investigación así como las bases del resultado principal, la metodología de análisis de sistemas de criptodivisas a través de la herramienta RI5C, desarrollado como auxiliar para esta investigación.

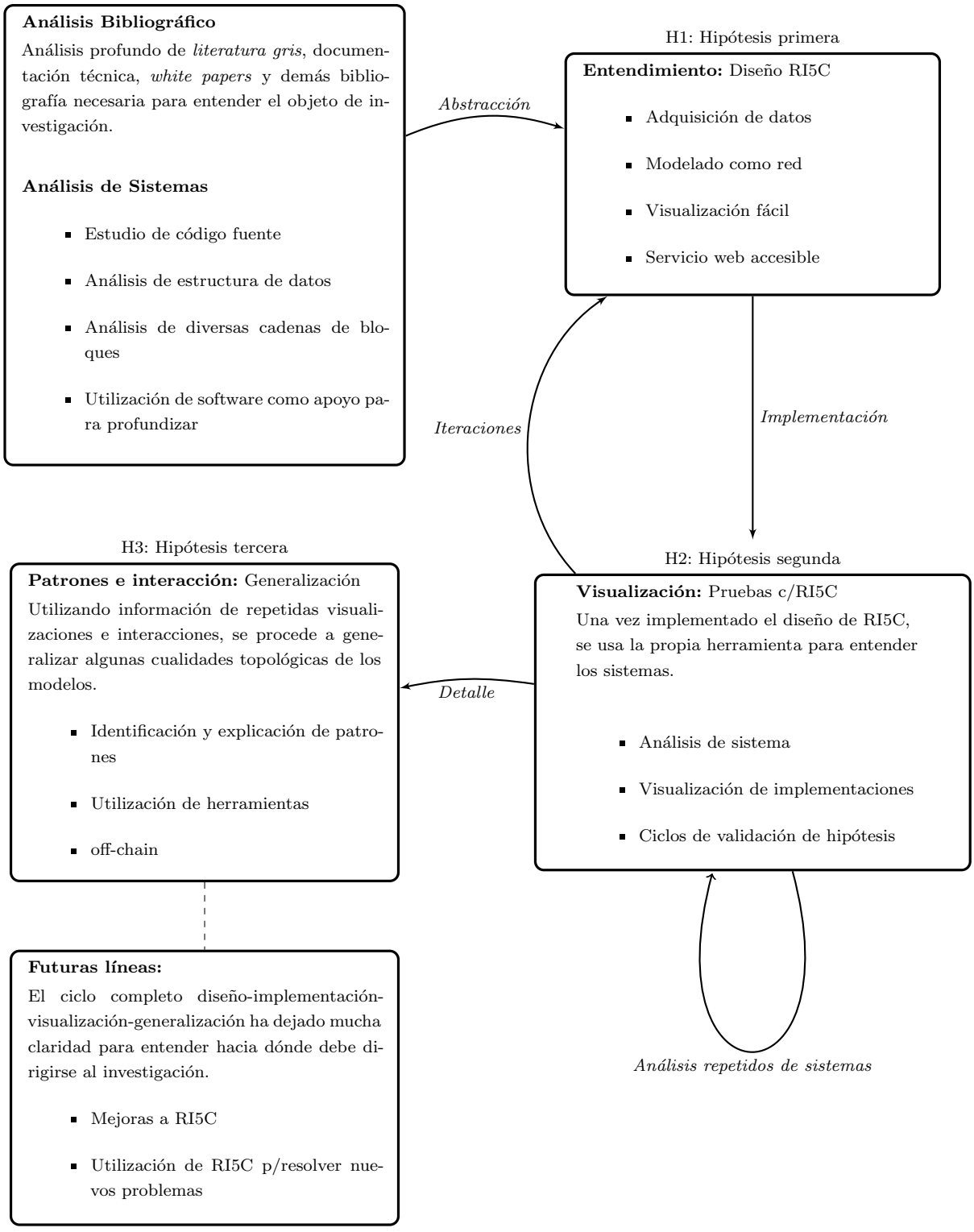
1.6.6. Metodología Empírica

Se propone analizar un sub-conjunto de transacciones de la red de Ethereum delimitado por contratos inteligentes específicos a través de un análisis de redes. Será una investigación descriptiva histórica con una componente correlacional, ya que fundamentalmente buscamos correlacionar la estructura de una red de transacciones con la volatilidad del precio a través del tiempo Sampieri Hernández et al. (2003). Es un ámbito científico novedoso y dinámico del cual se tiene poco precedente académico. Se espera que el resultado final de la investigación sea la herramienta RI5C.

1.7. Diagrama de Metodología

Dada la complejidad de la metodología, se ha hecho el esfuerzo de expresarla como un diagrama que muestra las diferentes fases de la metodología y cómo se relacionan entre si.

[6] En junio de 2018 pesa más de 100 GB


Análisis Bibliográfico
Análisis profundo de *literatura gris*, documentación técnica, *white papers* y demás bibliografía necesaria para entender el objeto de investigación.
Análisis de Sistemas
Estudio de código fuente
Análisis de estructura de datos
Análisis de diversas cadenas de bloques
Utilización de software como apoyo para profundizar
Abstracción
H1: Hipótesis primera
Entendimiento: Diseño RI5C
Adquisición de datos
Modelado como red
Visualización fácil
Servicio web accesible
Implementación
Iteraciones
H2: Hipótesis segunda
Visualización: Pruebas c/RI5C
Una vez implementado el diseño de RI5C, se usa la propia herramienta para entender los sistemas.
Análisis de sistema
Visualización de implementaciones
Ciclos de validación de hipótesis
Detalle
H3: Hipótesis tercera
Patrones e interacción: Generalización
Utilizando información de repetidas visualizaciones e interacciones, se procede a generalizar algunas cualidades topológicas de los modelos.
Identificación y explicación de patrones
Utilización de herramientas
off-chain
Futuras líneas:
El ciclo completo diseño-implementación-visualización-generalización ha dejado mucha claridad para entender hacia dónde debe dirigirse al investigación.
Mejoras a RI5C
Utilización de RI5C p/resolver nuevos problemas
Análisis repetidos de sistemas

1.8. Estado del Arte: Conceptualización y Modelos de Criptodivisas

1.8.1. Red de Transacciones en la Cadena de Bloques

Debido a la naturaleza pública de los datos de transacción en la cadena de bloques, es posible analizar los vínculos y conexiones que hay dentro de cualquier sistema basado en cadena de bloques. Durante la burbuja Dot-Com Smith (2013) hemos visto como interrupciones masivas de instituciones específicas rápidamente contaminaron los mercados principales de todo el sistema financiero.

Un aspecto importante es que existen un gran número de interconexiones en una red que pueden funcionar como amplificadores y no como atenuantes, lo cual puede generar sistemas frágiles.

Algunos nodos de la red pueden tener pocas conexiones entre si, mientras otros nodos pueden estar altamente conectados y por ello tener influencias importantes en el sistema. Estos nodos exponen vulnerabilidades importantes. Se ha visto en la literatura, que cuando existe una onda de entrada en el sistema, el número de participantes afectados en la red (nodos) puede ser muy bajo, pero la onda se expande a lo largo de todo el sistema.

Jugadores claramente grandes e importantes, como la red de Ethereum Buterin (2014) o Bitcoin Nakamoto (2008), son sistemáticamente importantes, lo cual tiene implicaciones fuertes para la estabilidad económica del sistema. El análisis de redes es crucial para la identificación de tales jugadores importantes en la red de exposiciones.

El impacto de la falla de uno de estos mercados primarios o secundarios a menudo depende de la capacidad que tiene la infraestructura de soportar variaciones y facilitar el desenvolvimiento de las posiciones en los diversos intercambios.

La literatura nos muestra que hay evidencia de tres características importantes que son influyentes en un sistema:

1. El grado de conectividad, relacionado a la frecuencia de las transacciones,
2. El grado de concentración, relacionado a la distribución de los fondos en el sistema,
3. El tamaño de las exposiciones, relacionado al peso (volumen) de cada transacción.

Vemos claramente que el análisis de redes nos puede ayudar a comprender las inter-conexiones sistémicas de los diferentes segmentos del sistema de generación de tokens actual, que van desde el intercambio de tokens, la emisión de nuevos tokens y hasta la destrucción de tokens.

El entendimiento y conceptualización de modelos de criptodivisas está apenas comenzando. Mientras que la aplicaciones técnicas se van descubriendo orgánicamente, la investigación va un paso atrás logrando conceptos abstractos de modelos que son muy complejos, con mucha información y meta información de transacciones que antes no existía. En el modelo actual, se entiende y acepta que las criptodivisas se pueden abstraer con un modelo de redes, y esto se ha aplicado en varios modos.

Los conceptos y modelos contemporáneos se describen en este capítulo, cuyo espectro abarca desde otros modelos de riesgo, hasta la utilización de estos métodos para demostrar manipulación en el mercado.

1.8.2. La Red en un Sistema de Pagos

La red en un sistema de pagos en Bitcoin es analizada en el documento Tasca et al. (2017) y se puede visualizar tal como se muestra en la Figura 6. En este artículo, se considera una tarea académica de valor la exploración de la economía de Bitcoin, en específico, cómo está estructurada una red compuesta por transacciones y cómo se trazan la relaciones entre los nodos a lo largo del tiempo. Específicamente en este artículo, se logra identificar varias de las inter-conexiones que de otro modo serían anónimas.

Se toma un conjunto de datos masivo, desde el tiempo de concepción de la red hasta mayo del 2015 y analizando la red, se logran identificar supernodos aislados, que con información disponible por terceros, han podido correlacionarse con entidades formales.

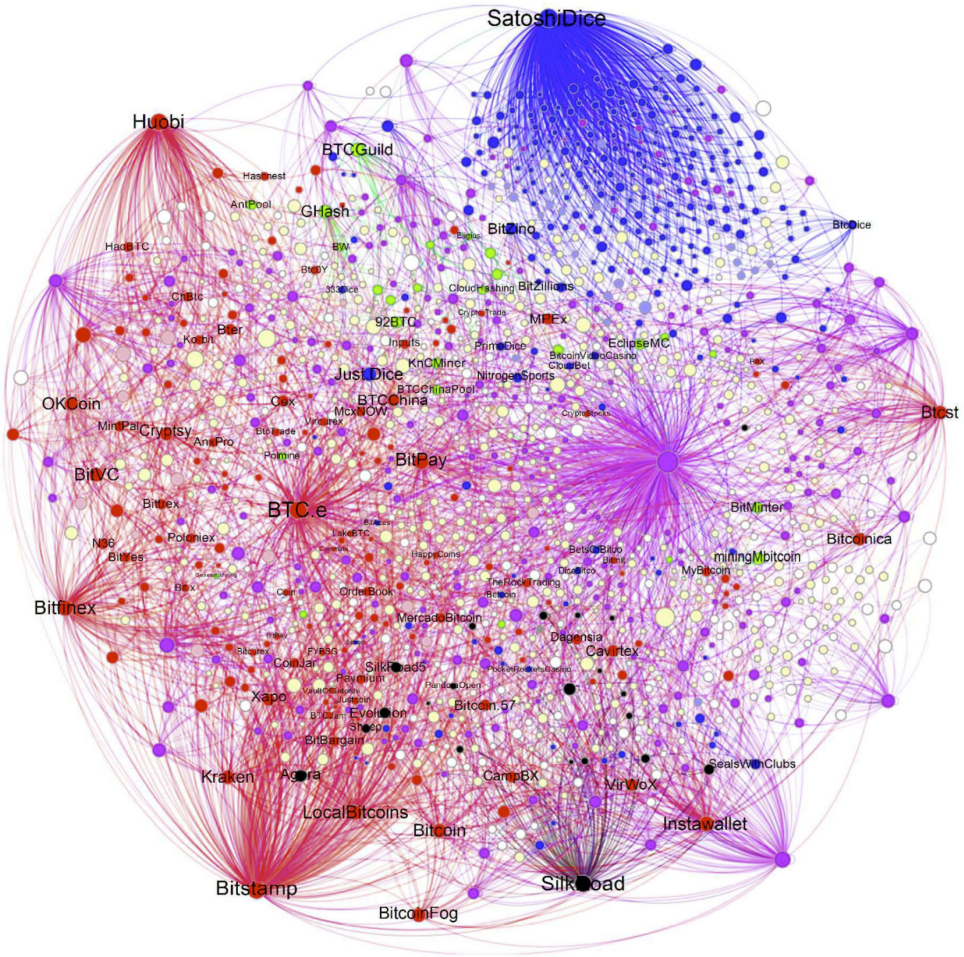


Figura 6: Diagrama de redes identificando supernodos en red Bitcoin. Fuente Tasca et al. (2017)

1.8.3. Modelos de Redes para Detectar Manipulación del Mercado

Notoriamente, un estudio de redes de Bitcoin Griffin and Shams (2018) logró demostrar que una criptodivisa alterna, conocida como Tether, se utilizó durante el 2017 para manipular el precio de Bitcoin. Este es un excelente ejemplo de cómo un estudio de redes puede utilizarse para comprender el comportamiento y riesgos de estos novedosos activos, se puede ver en la

Figura **??**.

Es importante resaltar que es la primera vez que esto sucede en el sector, la utilización de datos públicos para el descubrimiento de actividades nefarias a través de un análisis de redes tiene implicaciones importantes.

El trabajo utilizó una muestra de red de Bitcoin con una estructura de redes simple, en la que se identificaron con información de terceros, algunos nodos importantes que pertenecían a casas de cambio. Se identificaron diferenciales en el flujo y logran demostrar cómo el movimeinto de la criptodivisa Tether está correlacionado a altas en el precio de Bitcoin, lo que sugiere manipulación masiva de precio, ya que la emisión del activo de Tether no está regulada.

1.8.4. El Futuro del Análisis de Criptodivisas

Evaluar sistemas de criptodivisas es difícil sin las herramientas adecuadas. La tecnología es nueva y los emprendedores en el sector muestran habilidades y capacidad amplias, sin embargo, las mejores prácticas apenas están por ser definidas e implementadas.

Aún después de escándalos como el de MtGox, la industria de casas de cambio parece tener un antecedentes preocupantes. Científicos como Tyler Moore y Nicolas Chrisin encontraron que unas 40 casas de cambio se establecieron en tres años y de esas, 18 cerraron, muchas llevándose fondos de sus consumidores con ellas. Es aparente que la tecnología no está en su etapa de madurez. En el análisis de Beecroft (2015) se muestra que en algunos casos, el origen de las debilidades es tecnológico. Se requieren herramientas urgentemente para ayudar al entendimiento de estas tecnologías, dirigidas a perfiles de oficiales gubernamentales que desarrollen las políticas públicas, economistas, administradores y estudiantes de cualquier disciplina.

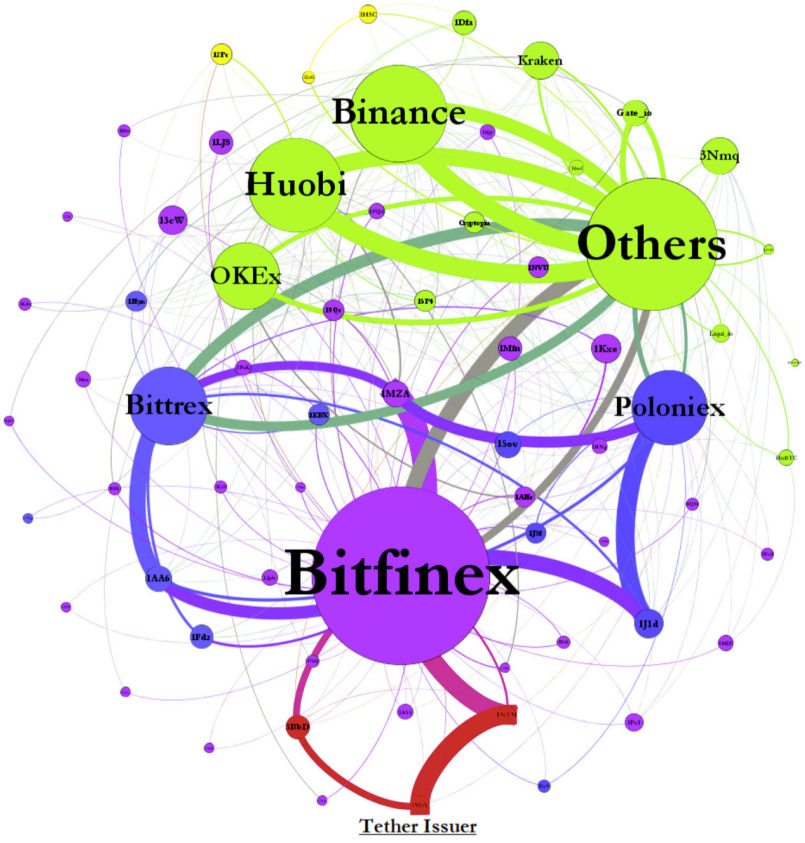


Figura 7: Análisis de redes en la cadena de bloques de Tether Griffin and Shams (2018)

2. Fundamentos de Criptodivisas

Gran parte del contenido de esta sección viene de una investigación profunda en *literatura gris* Auger (1975), definida como publicaciones en un punto medio entre documentación publicada y no publicada. *White papers*,[7] publicaciones empresariales, gubernamentales, foros de internet son buenos ejemplos de publicaciones que no caen dentro del alcance de medios de publicación tradicionales y son los canales más comunes para recabar data relacionada a criptodivisas. Esta literatura gris es de particular importancia para la distribución de conocimiento técnico, práctico y política pública Fjordback Søndergaard et al. (2003).

2.1. Los inicios y la publicación de *Bitcoin: A Peer-to-Peer Electronic Cash System*

Hacia el año de 2008, un autor bajo el pseudónimo de Satoshi Nakamoto[8] publicó un documento llamado *Bitcoin: A Peer-to-Peer Electronic Cash System* Nakamoto (2008) que traduce al español como: Bitcoin, un sistema de dinero digital sin intermediarios. El documento propone una moneda digital completamente descentralizada, con transacciones punto a punto y habilitada por criptografía. En el 2009 se despliega una red prototipo basada en el modelo propuesto y se genera la primera transacción, el primer registro guardado en una cadena de bloques: es decir, se crea el primer Bitcoin. Hubo algunos precursores, como lo fueron el DigiCash y el e-cash, ambos creados por David Chaum. Innovaron al usar criptografía para hacer anónimas las transacciones financieras, sin embargo, había una entidad central que gestionaba las transacciones, validaba a los usuarios y se aseguraba que la base de datos no se modificara, tal cual como lo haría un banco.

Bitcoin y su tecnología subyacente *The Block Chain* o la cadena de bloques en español, han traído la era de activos digitales y de confianza entre partes. Hoy en día, las criptodivisas totalmente descentralizadas almacenan varios miles de millones de dólares en valor, exitosamente intercambiando valores a través de una red descentralizada, sin una autoridad central. Esta red, llamada Bitcoin también, puede incluir actores no confiables, que son capaces de

[7] En español: *Publicación Blanca*, ver sub-capítulo 2.1.1
[8] En enero del 2019 aún no sabemos su identidad.

validar transacciones verazmente utilizando algoritmos matemáticos basados en evidencia criptográfica.

Compañías globales consultoras como Deloitte Andersen (2016), PwC Diemers and Koster (2016), KPMG Brown (2017), EY Crawford and Meadows (2017) han utilizado referencias que identifican la utilidad de servicios financieros basados en la tecnología de la cadena de bloques y de cómo pueden ayudar a la capacidad de auditorías financieras totalmente automatizadas, transparentes, a tiempo, sin errores y a prueba de manipulaciones.

Las arquitecturas basadas en la cadena de bloques facilitan la verificación de la autenticidad de mensajes de datos, creando un registro inmutable de transacciones en forma de funciones de resumen criptográficas (i.e., *hashes*) que se calculan utilizando datos de las transacciones. Esta tecnología se ha aplicado de manera muy heterogénea en la industria, por ejemplo: existen implementaciones de cadenas de bloques privadas y públicas. Las privadas se utilizan comúnmente para establecer confianza en transacciones entre partes conocidas y confiables, como negocios. Hearn (2016) y el proyecto Hyperledger Cachin (2016), son ejemplos recientes de aplicaciones empresariales de esta tecnología en modalidad privada que facilitan la auditoría y aumentan la seguridad del almacenamiento y transmisión de datos. Sin embargo, aún no hay un consenso en la industria que defina si una cadena de bloques privada se diferencía lo suficiente de otras tecnologías como para ameritar el nombre de *cadena de bloques.*

2.1.1. Acerca de *white papers*

Los *white papers* o en español, publicaciones blancas son reportes autoritativos que informan sobre algún tema complejo, problema o decisión y por definición, no son publicados a través de medios tradicionales. Debido a que la primera publicación de del área fue publicada como un *white paper*, este medio es el preferido para explicar y desarrollar sistemas de criptodivisas e incluso para publicitarlos. Siguiendo el ejemplo de Nakamoto (2008), este tipo de documentos suelen tener un formato académico y comúnmente se escriben en el editor académico de LaTeX. Importante recordar que la publicación de estos documentos toma formalismos académicos prestados, bajo ninguna circunstancia son revisados entre partes y hacia el 2019, aunque la práctica ha caído significativamente en desuso, aún se

presentan documentos publicitarios disfrazados de artículos académicos, que tienen poca o nada credibilidad.

2.2. Fundamentos Técnicos: la Cadena de Bloques

No existen criptodivisas (bitcoin, Ether, etc) físicas y no se pueden entender como archivos de software de Word o del tipo .mp3. Un bitcoin, o cualquier otra criptodivisa o fracción de criptodivisa, se puede entender como una sucesión de firmas electrónicas que es almacenada en un registro público llamado: la cadena de bloques. En donde la última firma electrónica, *endosa* la criptodivisa al último dueño y le permite acceder a esos fondos. La última firma electrónica en la cadena más antigua, será la del poseedor, quien será reconocido por una cadena única de caracteres, llamada dirección, cuenta o llave pública. La posesión de cualquier criptodivisa se equipara con tener conocimiento de las llaves públicas que están matemáticamente ligadas a esa llave pública. Si esas llaves públicas han recibido cualquier cantidad de criptodivisa en el pasado, y esto está almacenado en la cadena de bloques, el usuario que tenga la llave privada ligada a esa llave pública es el único usuario con capacidad de transferirlo a otro usuario.

Al firmar un mensaje de transacción con su llave pública, el emisor le pide a los mineros (i.e., los servidores que corren el software de Bitcoin Core) que agreguen una nueva firma electrónica que identifique al receptor de la transacción a través de su llave pública, al registro general de transacciones, la cadena de bloques. Este registro comprueba la cadena de posesión de cualquier bitcoin desde el comienzo de la red.

Los bitcoins se crean cuando los mineros resuelven problemas matemáticos difíciles que se requieren para escribir en la cadena de bloques, cuyo propósito es registrar transacciones validas e invalidas a lo largo de la red.

El software de la cadena de bloques que valida las transacciones y es ejecutado por los mineros, tiene un algoritmo de consenso entre nodos que previene a usuarios de crear un doble registro en diferentes nodos que pudiera llevar al problema de doble gasto: en el cual un usuario de la red pudiera endosar dos veces los mismos bitcoins. En algunos sentidos, la

cadena de bloques es semejante al registro público de la propiedad, en donde por definición, la condición única de tener propiedad es estar listado como el último dueño. En el registro público de los bitcoins, es decir la cadena de bloques, estar listado como el último propietario es la condición única para demostrar propiedad.

En este sentido, la red Bitcoin no es una herramienta para transmitir bitcoins, sino una herramienta para construir un registro público oficial en donde se registra el título de posesión de cualquier bitcoin y que previene a individuos de crear títulos o transacciones falsas.

2.2.1. Estructura y Composición de una Transacción

En el punto más básico, una transacción en la red se compone de un mensaje de datos firmado electrónicamente por el emisor. Una transacción está compuesta por pedazos de código llamados scripts, los hay de entrada y de salida. La salida de una transacción se usa como la entrada de otra transacción, tal cual se haría en una función matemática. Las transacciones son irreversibles en cualquier criptodivisa, en tanto que las firmas electrónicas son técnicamente irrepudiables. En la red de Bitcoin, por ejemplo, los scripts de salida se usan como los scripts de entrada de otra nueva transacción. Si los scripts de entrada son mayores a los de salida, el cliente de Bitcoin genera una transacción de vuelta al emisor: esto se llamada *cambio*. Como referencia, podemos tomar como ejemplo la transacción real con txid 0a1c0b1ec0ac55a45b1555202daf2e08419648096f5bcc4267898d420dffef87 y revisarla en algún navegador como `www.blockchain.info`. Podemos ver como un script de salida de 10.89 BTC se gasta por el cliente. El tamaño del pago es en realidad de 10 BTC y 0.89 BTC se regresa al firmante como cambio. El cliente de software no puede gastar solamente los 10 BTC del mismo modo que no podemos gastarnos una división de un billete o moneda. En esta transacción, el script de salida de 10.89 BTC entero se convirtió en el script de entrada de esta nueva transacción y en el proceso produjo dos nuevos scripts de salida, cuyo valor conjunto es de 10.89 BTC. El script de entrada original se considera como "gastado", destruido, para todos fines prácticos ya que no puede volverse a usar, lo único que se conserva son los scripts de entrada nuevos que se pueden utilizar en futuras transacciones.

2.2.2. Criptodivisas Alternas

Debido a la naturaleza abierta del código y de sus implementaciones, el concepto fundamental de Bitcoin empezó a vivir transformaciones y extrapolaciones a diferente industrias. Como referencia, analizaremos a las 3 monedas con mayor capitalización de mercado,[9] la Figura 8 muestra las 12 criptodivisas con mayor capitalización, graficando la fecha de fundación contra la capitalización del mercado:

- **Bitcoin (BTC)** – lanzada en el 2009 y con una capitalización de 163 miles de millones de dólares, la criptodivisa más antigua. Tiene limitantes para escalar pero es la más segura.
- **Ethereum (ETH)** – lanzada en 2015 y con una capitalización de 70 miles de millones de dólares, se caracteriza por su capacidad de ejecutar contratos electrónico.
- **Ripple (XRP)** – lanzada en 2012, capitalización de 32 miles de millones de dólares. No tiene problemas de escalabilidad, pero es propiedad de una compañía privada.
- **Stellar (XLM)** – lanzada en 2013, Stellar comenzó como un clon de Ripple, compartiendo su base de código por unos años hasta que desarrollara su propia infraestructura.
- **Litecoin (LTC)** – lanzada en 2011, como un clon de Bitcoin, actualmente tiene una capitalización de varios cientos de millones de dólares y es utilizada como campo de experimentación para cambios en bitcoin, para lo cual funciona muy bien puesto que tienen una historia de código compartida.
- **Monero (XMR)** – lanzada en 2016, Monero está basada sobre una cadena de bloques que utiliza firmas electrónicas de anillos para salvaguardar la anonimidad de sus participantes.
- **Bitcoin Cash (BCH)** – lanzada en 2017 como un clon con historia compartida de Bitcoin. Bitcoin Cash cambió algunos fundamentales de la red original de Bitcoin, sin embargo tiene problemas diferenciándose de bitcoin y su capitalización ha estado en constante disminución.

[9] Datos obtenidos en marzo del 2018

- **Dash (DASH)** – lanzada en 2016, Dash también comenzó como un clon de bitcoin, que poco a poco fue modificado para tener cualidades aumentadas de privacidad y velocidad.
- **EOS (EOS)** – lanzada en 2018, EOS es un modelo basado en las interacciones de Ethereum facilita, como contratos inteligentes. Actualmente existe como un token ERC20 basada en Ethereum.
- **NEO (NEO)** – lanzada en 2015, NEO es un modelo semejante a Ethereum, pero enfocado hacia China. No es un modelo muy descentralizado, pero tiene capacidad de emitir y correr contratos inteligentes.
- **IOTA (MIOTA)** – lanzada en 2017, IOTA utiliza un registro compartido en lugar de una cadena de bloques, tiene como objetivo ser el registro distribuido del internet de las cosas.
- **Cardano (ADA)** – lanzada en 2017, una criptodivisa que en teoría podrá gestionar contratos inteligentes en el futuro. Utiliza un modelo de consenso diferente a Ethereum y Bitcoin.

2.2.3. Representación y Estandarización de Data

Pese a que la data de la cadena de bloques es pública, hay pocos canales de acceso a esta información que sean prácticos, en el 2019 interactuar directamente con estos datos requiere alto conocimiento técnico y en la mayor parte de los casos hardware especializado y dedicado.[10] La información de la cadena de bloques suele ser visualizada en una capa externa llamada *navegador*, un navegador de la cadena de bloques hace el trabajo de estandarizar la data de la cadena de bloques y proveer una plataforma amigable para humanos para su visualización (se puede ver la visualización estandar en la Figura 9), sin embargo, esta visualización suele ser basada en texto y aunque es útil para confirmar la existencia de transacciones, es difícil de analizar varias interacciones. No existen herramientas para visualizar y tratar estos datos fuera de los llamados navegadores de la cadena de bloques.

[10] Interactuar con la cadena de bloques de cualquier criptodivisa directamente, involucra la gestión de un nodo, y esto involucra sincronizar con el resto de la red, que en algunos casos pesa más de 100 GB.

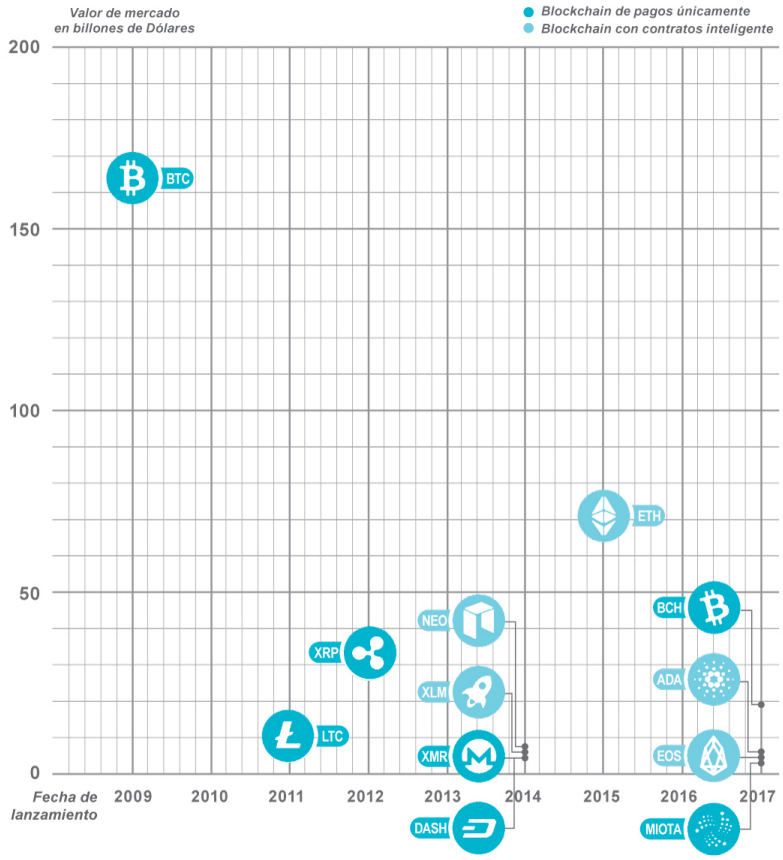


Figura 8: Las 12 criptodivisas con mayor capitalización y su cronología. Fuente: Casey and Vigna (2018).

2.2.4. Breve conclusión de la sección

Es posible definir una criptodivisa o cualquier cadena de bloques como un sistema complejo, que se puede modelar como un conjunto de nodos y aristas en donde cada arista es una transacción y cada nodo una cartera.

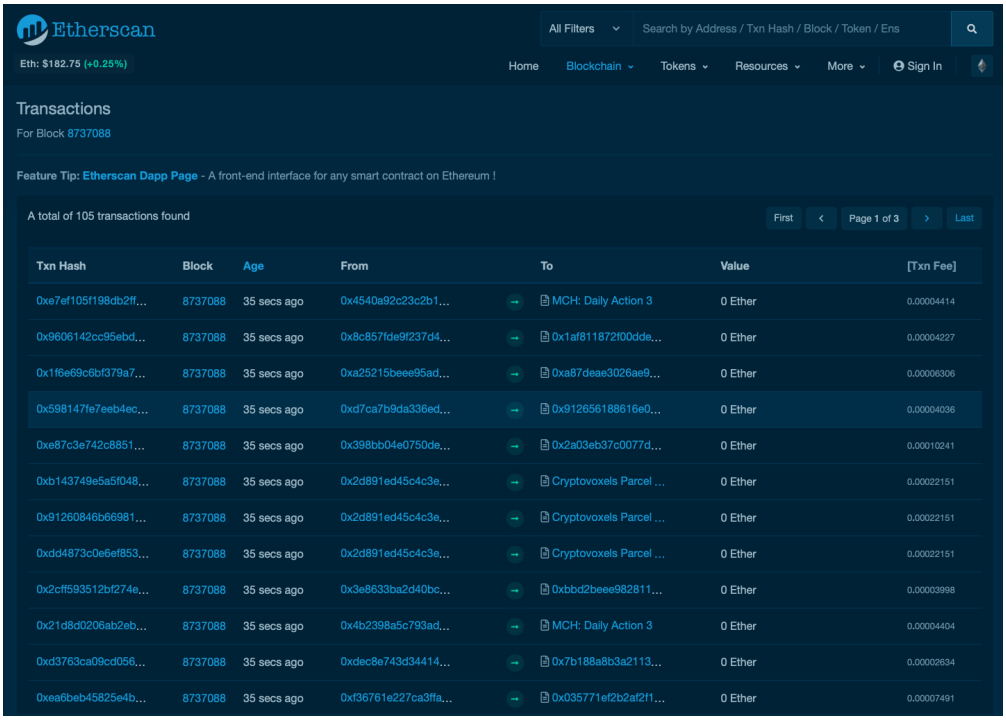


Figura 9: Lista de transacciones para el bloque no. 8737088 a través del navegador Etherscan disponible en `www.etherscan.io/txs?block=8737088`. Fuente: Etherscan.

2.3. Código de Fuente Abierta

proyecto es desarrollado por desarrolladores de software de todo el mundo, que se coordinan utilizando herramientas tecnológicas como Github, un repositorio público de código que puede gestionar versiones y colaboraciones de una base de código. La apertura del código y de la red ha logrado un avance increíblemente rápido del sector. El código de Bitcoin es públicamente accesible desde `www.github.com/bitcoin/bitcoin`. Existe literatura gris acerca de la evolución y los objetivos de los creadores al decidir el tipo de licencia y las implicaciones que tendría Bitcoin-Talk (2010), fundamentalmente la idea de que el código permaneciera propiedad de los usuarios sin importar cambios futuros era el principal motivador.

2.3.1. La evolución del código abierto

En el modelo de fuente abierta, se permite el uso de código, documentos de diseño o contenido de un producto. El uso del término y el origen del movimiento comenzó con software, pero se ha expandido a varios tipos de colaboraciones. Originalmente, nació de un grupo de personas involucradas con el navegador Netscape en 1998. El código de este navegador fue distribuído libremente, con una licencia de uso permisivo, dando lugar a un sin-fin de colaboraciones y una producción distribuida entre partes. Varios desarrollos de alto impacto se han desarrollado protegidos por licencias de código abierto, entre ellos Linux (respaldado por el movimiento GNU), varias implementaciones de bases de datos SQL, Firefox (evolucionado del código fuente de Netscape) y porsupuesto, Bitcoin.

Se puede entender que el movimiento de de fuente abierta distribuye código libremente, es decir, permite al público en general revisar el código libremente, copiarlo, comercializarlo y modificarlo. Las criptomonedas y la cadena de bloques extienden el concepto de fuente abierta, ya que por primera vez existe una componente de infraestructura que también es públicamente accesible, lo cual convierte una implementación como Bitcoin en un servicio de fuente abierta, exponiendo que las licencias y el movimiento de fuente abierta se encuentran en necesidad de una revisión y extensión en sus términos y condiciones.

2.3.2. Código abierto en la investigación

La investigación contemporánea conlleva una componente importante de uso de herramientas informáticas que son en su mayoría, parte del movimiento de fuente abierta. Herramientas tradicionales para la escritura y distribución de artículos académicos, así como para el análisis y visualización de datos y creación de algoritmos son todas parte del movimiento de fuente abierta. El propio trabajo de la creación de RI5C ha sido posible gracias a que el resto de las herramientas (Python, Google BigQuery, NetworkX y SigmaJS) son todas distribuidas bajo este esquema. La creación y extensión de herramientas de fuente abierta es una contribución importante para la comunidad[11], y permite que una generación nueva de investigadores avancen la ciencia y entendimiento. Adicionalmente, se ha visto que el código abierto genera un vínculo importante y duradero entre el mundo académico y privado[12].

2.4. Los Fundamentos Financieros

2.4.1. La Inversión en Criptodivisas como Diversificador

La crisis financiera global reciente y la crisis de deuda soberana europea han obligado a inversionistas e instituciones financieras a identificar activos que protejan sus inversiones en caso de condiciones extremas del mercado o riesgos sistémicos Stavroyiannis (2018).

La literatura reciente Baur and Lucey (2010), Baur and McDermott (2010) y Baur and McDermott (2016) distingue a las criptodivisas como agentes que diversifican, anclan y proveen una inversión que diversifica eficientemente el riesgo en tiempos de crisis.

Levantamiento de Capital Utilizando Criptodivisas

Desde el 2016, grupos de personas han generado activos digitales, semejantes a Bitcoin, para hacer una colocación primaria de estos activos directamente a inversionistas privados, de

[11] Hay comunidades académicas muy activas en el desarrollo y manutención de herramientas de fuente abierta, un ejemplo en bioinformática es la conferencia anual "The Bioinformatics open source conference".

[12] La primera instancia documentada de este vínculo es el navegador Mosaic, que posteriormente se convierte en la base de Netscape y a su vez, Netscape Communications Corporation la empresa más joven en hacer una colocación primaria en la bolsa. Netscape también creó el lenguaje Javascript y lo licenció como código libre, hoy es uno de los lenguajes más usados para el desarrollo web.

un modo no muy diferente a la colocación primaria de acciones en la bolsa. Durante el 2017 se llamaron ICOs, (del inglés Initial Coin Offering una variación de colocación primaria en inglés: *IPO*), posteriormente se llamaron STOs (Security Token Offerings) y TGEs (Token Generation Events) pero el espíritu es el mismo: el levantamiento de capital a través de la creación y venta de un activo digital. En junio de 2017 Sehra (2017), por primera vez en la historia, el levantamiento de capital a través de ICOs superó al levantamiento de capital de riesgo, con 1,200 millones de dólares acumulados en 92 ICOs. Existe poca documentación formal que describa la estructura y proceso de estos eventos, que suceden en un mundo que se va regulando *a posteriori*. Apenás a tres años de su clímax, han bajado significativamente en popularidad.

La emisión de activos digitales provee un método para que una startup evite el proceso burocrático, costoso y reglamentariamente complejo de recibir capital externo. Aunque aumentan ciertos factores de riesgo para inversionistas, son una fuente de volatilidad interesante y también prometen facilitar su futura venta, ya que un inversionista poseedor del token es capaz de venderlo en un mercado secundario sin esperar el ciclo completo de la compañía, suponiendo que el mercado secundario tenga suficiente liquidez.

La primera emisión de activos digitales con estos fines, fue llevada a cabo por Mastercoin en julio del 2013. Sin embargo, tal vez el caso más conocido es el de la red Ethereum, quien logró percibir el equivalente a 2 millones de dólares en Bitcoin durante el 2014. Durante el 2017, esta práctica se popularizó y vimos un incremento de 40 veces el capital levantado durante 2016, como lo muestra la figura 3.

Se debe entender, que desde el punto de vista financiero una emisión de activos digitales es solamente un vehículo diferente para la industria del capital de riesgo y un medio para que una startup se capitalice.

2.4.2. La Raíz de un Token

Los tokens existen en Ethereum u otra cadena de bloques como una sub-divisa o sub-activo electrónico. La funcionalidad de Ethereum que les da lugar, es su capacidad de generar y ejecutar contratos inteligentes. Los contratos inteligentes permiten la creación de *sistemas de tokens*, que tienen múltiples aplicaciones, desde sub-divisas que representen activos tales

como el USD, oro, acciones, propiedad inteligente o representaciones de objetos abstractos como obras de arte. Los sistemas de tokens financieros son muy fáciles de implementar, en el Algoritmo 1 se puede ver un ejemplo simplificado del código que genera un contrato inteligente para emisión de un token. En algunos casos un token puede ser sinónimo de una criptodivisa, sin embargo el concepto de token es más amplio y hay algunas acepciones de token que no son financieras.

El punto clave es entender que la definición de una moneda, o de un token, es una base de datos con sólo una operación: resta `X` unidades de `A` y suma `X` unidades a `B`, con la condición que `A` tenga al menos `X` unidades y la transacción sea aprobada por `A`. Ver Algoritmo 1.

Algoritmo 1: Definición simple de un contrato inteligente bancario.

```
1 send (to, value);
  Input  : ETH
  Output : Token
2 if self.storage[msg.sender] ¿= value: then
3 |   self.storage[msg.sender] = self.storage[msg.sender] - value;
4 |   self.storage[to] = self.storage[to] + value;
5 else
6 |   return False;
7 end
```

2.4.3. Un estudio de caso: La Burbuja *Dot-Com*

La burbuja *Dot-Com* se conoce como el periodo marcado por la creación, y en muchos casos, espectacular fracaso de muchas compañías basadas en el Internet (nuevo en aquel momento), que comúnmente se conocían como punto-coms por la popularidad y novedad de los dominios de Internet que terminaban en punto-com. Llego a extremos tan ridículos que las compañías podían incrementar sustancialmente el valor de sus acciones simplemente agregando un prefijo "e"- o sufijo ".com" Nanotech Excitement Boosts Wrong Stock (2003) - conocido como inversión de prefijo.

En concreto fue una burbuja especulativa que sucedió aproximadamente desde 1997 hasta el 2000, con el clímax definitivo en marzo del 2000, cuando el NASDAQ llegó a un pico de 5,132.52 puntos, el más alto de la historia (ver Figura 10). Causado por una combinación de precios de capital en subida, sobre-confianza en el mercado y capital en alta disponibilidad, el resultado fue un ambiente en el que muchos inversionistas estaban dispuestos a pasar por alto índices de desempeño tradicionales a favor de avances tecnológicos.

Hechos notables:

- La acciones de Books-a-Million.com incrementaron su valor 1000 % en una semana
- La empresa de ropa y moda Boo.com gastó 188 mdd en seis meses
- Geocities.com fue comprado por Yahoo.com en $3.57 mmdd, cerró operaciones pocos años después con grandes pérdidas
- AOL.com fue adquirido por Time Warner en lo que se conoce como la peor fusión de la historia

La startup después de la burbuja *Dot-Com* Miles de empresas desaparecieron después de que la burbuja Dot-Com estalló, pero lo que sí sobrevivió fueron avances tecnológicos creados con abundante inversión y exuberancia irracional Smith (2013). Junto con tres de las empresas tecnológicas más grandes de la historia: Amazon.com, Google.com y eBay.com. Por otro lado, La figura 10 muestra claramente que la inversión en capital de riesgo nunca bajó después del auge en el clímax de la burbuja Dot-Com.

Para este momento, la esencia de una startup se había destilado en cuatro características importantes:

- Ambición
- Escalabilidad
- Innovación y
- Crecimiento

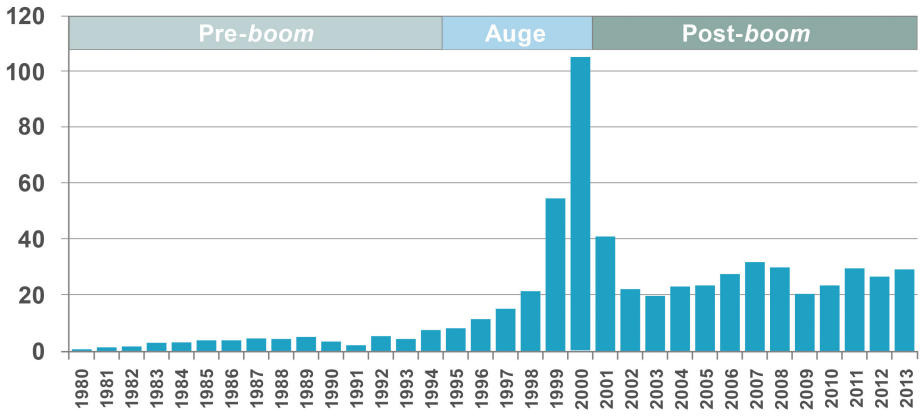


Figura 10: Inversión histórica en capital de riesgo, clara representación de la Burbuja Dot-Com, fuente: PricerwaterhouseCoopers/National Venture Association MoneyTree.

Sin embargo, había más que esto separando a la empresa privada tradicional: la búsqueda de un nuevo modelo de negocios rentable. Una empresa, deja de ser startup en el momento en que consigue encontrar una oportunidad estratégica, y por ende más que un tipo de empresa, es una etapa en la vida de una empresa.

2.5. Gobernanza

La gobernanza son todos los procesos de gobierno ejecutados por un gobierno administrativo, un mercado, una red, un sistema social (familia, tribu, organizaciones formales o informales, territorios) a través de leyes, normas, lenguaje o poderes de una sociedad organizada Bevir (2013). Se relaciona a los procesos de interacción y toma de decisiones entre los actores relacionados en un problema colectivo que lleva a la creación, refuerzo o reproducción de normas sociales. Se puede ver, también como los procesos políticos que existen entre organizaciones formales.

El término gobernanza se usa sobre todo en situaciones económicas, pero también en situaciones sociales o de funcionamiento institucional. Esencialmente en la interacción que existe entre sus distintos niveles administrativos.

Una variedad de entidades, conocidas como órganos de gobierno, pueden gobernar. La más formal y conocida es el gobierno soberano de un estado o país, un gobierno cuyo propósito explicito y autoridad es tomar decisiones vinculantes en un sistema geo-político al establecer leyes. Otros gobiernos existen, tales como el de una organización, como una corporación reconocida a través de una entidad legal o un grupo socio-político, una familia, tribu, etc. En los negocios es común que haya estructuras de gobernanza construidas en contratos vinculantes que tratan de fomentar colaboración a largo plazo e innovación.

2.5.1. La Gobernanza en una cadena de bloques

La gobernanza en un sistema de criptodivisas se define dentro de las reglas de negocio de la cadena de bloques. Se puede definir como el conjunto de reglas, normas y acciones estructuradas, sostenidas, vigiladas y reguladas por la cadena de bloques. En algunos casos, estas reglas se pueden modificar a través de contratos inteligentes. En algunos sistemas, como Bitcoin, el grado de formalidad es mayor y estas reglas no se pueden modificar sin que haya un consenso de todos los miembros de la red.

La cadena de bloques es efectivamente un órgano descentralizado de gobierno que se adhiere a reglas programadas en el código fuente de los servidores. Diferentes sistemas de criptodivisas y cadenas de bloques tienen reglas de gobierno y capacidad de ejecución diferentes.

2.5.2. La Identidad en las Criptodivisas

Las identidades verdaderas de los usuarios están escondidas detrás de sus cuentas, pero pueden ser identificadas cuando transaccionan con alguien más. En otras palabras, si Alice manda un pago a Bob, sus identidades verdaderas se revelan al otro por virtud de compartir

sus direcciones (cuentas) para enviar o recibir la criptodivisa.

Sin embargo, debido a las cualidades de la criptografía de curva elíptica, es posible generar cuentas *hijas* a través de cuentas HD (que por sus siglas en inglés, significa Hierarchical Deterministic, que se traduce como cuentas jerarquimante deterministas). Las cuentas que poseen estas características pueden generar direcciones de cuentas criptográficamente relacionadas con una llave maestra, pero que son imposibles de relacionar entre sí, de tal modo que se ofusque la identidad un poco más.

2.5.3. La cadena de bloques como un Sistema Complejo

Un sistema de criptodivisas, con su respectiva cadena de bloques, es un conjunto de componentes que interactúan entre si. Es efectivamente una red de nodos que se conectan y relacionan entre ellos; el Internet o los sistemas económicos son otros claros ejemplos de sistemas complejos. Sin embargo, a diferencia de las criptodivisas, los órganos de gobierno no son autónomos ni parte integral del sistema. Los sistemas complejos se caracterizan por la gran dificultad en la predicción y modelado del comportamiento de sus componentes. Esto radica en las relaciones, dependencias e interacciones que entre ellas o entre el sistema y su medio ambiente. La complejidad es una característica intrínseca a este tipo de sistemas.

2.5.4. Teoría de Gobernanza de Williamson

En 1964, Oliver E. Williamson hipotetizó que la maximización de las ganancias no iba a ser el objetivo de los gerentes de una corporación. La teoría de Williamson supone que un gerente, director o administrador busca maximizar su propia utilidad, ya que existe una separación entre la propiedad y el control. De ahí se desprende que para una startup sea tan importante que la propiedad y el control no estén separados.

Esencialmente es una aplicación del *problema del agente*, que se define cuando una persona o entidad es capaz de tomar decisiones y tomar acciones que afectan negativamente a la entidad principal. En campos corporativos, un administrador puede usar su discreción para crear y ejecutar políticas que maximicen sus propias utilidades en lugar de las de los

accionistas Davidson (1990). Cabe resaltar que en aplicaciones administrativas humanas, Ghoshal (2005) hace una muy buena crítica al trabajo de Williamson y aboga por considerar el lado de interacción humana más a fondo, en lugar de crear una división marcada entre dueño y trabajador.

La creación de un órgano descentralizado de gobierno supone que aún separando el control de la propiedad, las políticas sean creadas y ejecutadas por el sistema. Es decir, la gobernanza de las redes descentralizadas, como Bitcoin, tiene como tarea considerar que todos los elementos de la red actúen en beneficio de la misma.

2.6. Connotaciones Negativas

2.6.1. Silk Road

El Silk Road fue un mercado negro y el primer mercado moderno completamente basado en la red obscura del Internet. En la época del 2010 - 2015, el mismo momento histórico cuando nacieron las criptodivisas, era una plataforma conocida por la venta de drogas. Operaba como un servicio escondido del navegador Tor, de tal modo que los usuarios podían visitarlo anónimamente, sin riesgo a que su tráfico fuera monitoreado. Los usuarios utilizaban bitcoin para realizar los pagos. El sitio lanzó en 2011, con el desarrollo principal habiendo comenzado unos 6 meses antes. Inicialmente hubo una cantidad limitada de cuentas para vendedores, quienes tenían que comprar cada cuenta en una subasta. Posteriormente, una cuota fija se cobraba por cada cuenta de vendedor nueva. En octubre del 2013 Haun (2013), el FBI cerró el sitio y arrestó a Ross Ulbricht bajo cargos de ser el fundador del Silk Road, llamado “Dread Pirate Roberts” o “DPR”. El 6 de noviembre del 2013 la versión 2.0 del sitio fue lanzada, administrada por un ex-miembro del sitio original. El sitio nuevo también fue cerrado y en noviembre del 2014, su operador fue arrestado también.

El caso que los EUA hicieron en contra de Ross Ulbricht Haun (2013) fue la primera experiencia que el gobierno tenía ante un crimen perpetrado utilizando medios masivos, y el primero en el cual se involucraron criptodivisas. Acerca del juicio, Kathryn Haun Haun (2013) dijo que la base de datos de la cadena de bloque facilitó enormemente su trabajo. Ya que los culpables dejaron rastros indelebles de sus transacciones, que eventualmente fueron ligados

a su identidad. Bitcoin comprobó ser una pobre elección para criminales, como desarrollo secundario del juicio, y gracias a vínculos de transacciones en la cadena de bloques, el FBI encontró que dos de sus agentes habían malversado fondos de la investigación para ganancia personal. Dichos registros hubieran sido muy difíciles de obtener o de modificar si hubieran sido transacciones bancarias. El desarrollo del caso de los EUA vs. Ulbricht Haun (2013) fue un avance importantísimo en el desarrollo de los activos virtuales, pues mostró que más que ser un impedimento para las agencias de seguridad, su diseño transparente y auditable resultó un aliado.

2.6.2. La primera casa de cambio: MtGox

Entre las cosas que el autor anónimo de la tecnología de Bitcoin, Satoshi Nakamoto Nakamoto (2008) no consideró en el documento original, fue cómo iba a intercambiarse este nuevo activo digital, bitcoin, con otros pares de divisas, como el Dólar americano o cualquier otra divisa.

En el 2006, un desarrollador de software llamado Jed McCaleb pensó en construir un sitio para usuarios de un juego de cartas para niños llamado "Magic: The Gathering". Lo lanzo en el 2017 y lo llamo "Magic: The Gathering Online Exchange" o "Mt Gox" en el sitio `mtgox.com`. En julio del 2010, McCaleb leyó acerca de bitcoin y decidió re-lanzar el sitio de `mtgox.com` como una casa de cambio de bitcoin, con servicio de compra-venta y búsqueda de precio. El sitio fue vendido al desarrollador de software Mark Karpeles en el 2011.

MtGox fue testigo de varios fraudes y vulnerabilidades en la seguridad de la red. En el 2011 una computadora comprometida por un hacker logró que se intercambiaran 8.7 millones de dólares en bitcoin por un centavo. En octubre del mismo año, el software de MtGox descubrió un error en la red de bitcoin al enviar 2,609 bitcoins a direcciones invalidas, efectivamente perdiéndolos. Sin embargo, MtGox creció vertiginosamente y para el 2013 era el procesador más grande del mundo de intercambios en bitcoin. Para abril del 2013 estaba gestionando el 70 % de las transacciones del mundo. Para el 7 de febrero del 2014, la casa de cambio cesó operaciones, canceló retiros en dólares y bitcoin y publicó un anunció describiendo como un error Frunza (2017) en la red de bitcoin había ocasionado una pérdida de fondos masiva Karpeles (2014). El 28 de febrero del 2014 se declaró en bancarrota en la

corte de Tokyo, con 65 millónes de dólares en riesgo. Los usuarios se comunicaban en foros como Reddit y BitcoinTalk, sospechaban fraude masivo y muchos tenían pérdidas millonarias.

Mark Karpeles, en ese momento el director de MtGox alegó que la pérdida había sido causada por un error en la red bitcoin que había permitido que un hacker se robará los fondos ilícitamente. Sin embargo, gracias a un análisis profundo de las transacciones en la cadena de bloques, la firma de seguridad japonesa WizSec Nilsson (2015) logró demostrar el paradero de los fondos perdidos. La investigación fue fondeada, al inicio, por victimas del fraude de MtGox. Su investigación trazó la red de transacciones históricas de cuentas afiliadas a la casa de cambio, y eventualmente logró comprobar que los bitcoins habían sido robados paulatinamente. Finalmente, en agosto de 2015 Mark Karpeles fue arrestado por la policía de Japón Mochizuki (2015) y acusado de fraude, enriquecimiento ilícito y manipulación del mercado de MtGox. A la fecha de escribir esta investigación, el juicio y la búsqueda por los bitcoins perdidos sigue. Karpeles fue encarcelado por 30 meses y una vez más, la naturaleza pública de las transacciones de bitcoin fue instrumental en encontrar la evidencia necesaria para construir un caso en contra de un criminal.

2.6.3. La Cadena de Bloques en Crímenes

En estos dos casos, es claro como los principios de transparencia de la red Bitcoin resultan ser contraproducentes para uso criminal. Cualquier transacción queda publicada en la cadena de bloques, y ésta tiene una propiedad de inmutabilidad y auditabilidad pública que resulta ser un aliado para las agencias de seguridad. Acerca del caso EUA vs. Ulbricth Haun (2013), Kathryn Haun dijo que auditar un registro en la cadena de bloques era al menos una orden de magnitud más fácil que emitir una citación para ver transacciones de *cualquier* banco internacional. La cadena de bloques y las criptodivisas presentan retos para las autoridades fiscales, de seguridad y financieras; sin embargo presentan cualidades muy superiores a las instituciones bancarias en muchos aspectos, tanto para los usuarios, como para las autoridades.

2.7. Clasificación Legal de Criptodivisas

2.7.1. FINMA en Suiza y la SEC en los EUA

La pregunta de cuándo un token o criptodivisa emitido por una firma se debe considerar como un valor se ha debatido ampliamente por la SEC *Security and Exchange Commission* de los EUA Clayton (2018).

Si el valor de un activo electrónico *no* está fijo a un activo afuera del control de la firma, como el Dólar americano o el precio del oro, entonces normalmente sería considerado como un valor. Los siguientes extractos del presidente de la SEC Jay Clayton Clayton (2018) son pertinentes:

Dentro de la Sección 2(a)(1) de la Acta de Valores Sección 3(a)(10) de la Acta de Intercambio, los valores incluyen, entro otros "un contrato de inversión". Ver el detalle 15 U.S.C §§77b-77c. Un contrato de inversión es una inversión de dinero en una empresa común con expectativa razonable de ganancias derivada de los esfuerzos de emprendimiento y administrativos de otros. Ver SEC vs. Edwards, ver también 540 U.S. 389, 393 (2004); SEC vs. W.J. Howey Co., 328 U.S. 293, 301 (1946); ver también United Housing Found., Inc. vs. Forman, 421 U.S. 837, 852-53 (1975).

Meramente llamar a un activo una "utilidad" o estructurar la tecnología para proveer cierto nivel de utilidad, no previene al activo de ser considerado por la SEC como un valor. Ver también el caso de la SEC vs. C.M. Joiner Leasing Corp., 320 U.S. 344, 351 (1943) (El alcance de la Acta de Valores no se detiene con aparatos nuevos o irregulares, independientemente de lo que aparenten ser, estos serán alcanzados y tratados de acuerdo a su carácter en el comercio como 'inversión' o 'contratos de inversión' o como cualquier otro instrumento que conozcamos como un 'valor'); ver también Reves vs. Ernst & Young, 494 U.S. 56, 61 (1990) en la que el ("Congreso ejecuta las leyes de valores para regular inversiones en cualquier forma y por cualquier nombre diferente").

En el ambiente internacional, la mayor parte de los eventos de generación de activos digitales, criptodivisas o tokens se llevan a cabo en Suiza. Las autoridades financieras Suizas

también han comenzado sus consideraciones legales FINMA (2018), de acuerdo a estas consideraciones, tres categorías de activos digitales han sido identificados y definidos.

1. Activos de pago: Los activos de pago, sinónimos con criptodivisas son activos cuya intención de uso, ahora o en el futuro, sea un método de pago para adquirir bienes o servicios o como un medio de dinero o transferencia de valor. Las criptodivisas no pueden originar demandas a sus emisores.

2. Activos utilitarios: Los activos utilitarios son aquellos cuya intención es proveer acceso a una infraestructura digital, aplicación o servicio por medio de infraestructura basada en la cadena de bloques.

3. Activos de valor: Los activos de valor representan activos externos tales como deuda o acciones del emisor. Los activos de valor prometen, por ejemplo, acciones en una futura compañía, dividendos o flujos de capital futuros. En términos de su función económica, estos activos son equivalentes a valores, bonos o derivativos. Activos digitales que habiliten el intercambio de activos físicos en la cadena de bloques caen en esta categoría también.

Estas clasificaciones individuales no son mutuamente exclusivas. Los activos utilitarios y de valor pueden también ser calificados como activos de pago. En estos casos, los requerimientos son acumulativos, en otras palabras, estos activos pudieran ser definidos como valores y como medios de pago.

De tal modo que para que un activo sea considerado cualquiera de estas categorías, debería cumplir estrictamente estas definiciones e interpretaciones de la SEC y FINMA. Se espera que otras entidades regulatorias internacionales sigan caminos similares.

2.7.2. Ley Fintech en México

En México, estos activos se regularon por la Ley para Regular las Instituciones de Tecnología Financiera (conocida como *Ley Fintech*) en marzo del 2018 DOF-09-03-2018 (2018), la Ley Fintech regula las criptodivisas como *activos virtuales*, definidos a continuación DOF-09-03-2018 (2018).

Artículo 30.- Para efectos de la presente Ley, se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia unicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas.

Las ITF (Instituciones de Tecnología Financiera) solo podrán operar con los activos virtuales que sean determinados por el Banco de México mediante disposiciones de carácter general. En dichas disposiciones, el Banco de México podrá establecer plazos, términos y condiciones que deberán observar las ITF para los casos en que los activos virtuales que este haya determinado se transformen en otros tipos o modifiquen sus características.

Para realizar operaciones con los activos virtuales a que se refiere el párrafo anterior, las ITF deberán contar con la previa autorización del Banco de México.

El Banco de México para la determinación de los activos virtuales tomará en cuenta, entre otros aspectos, el uso que el público dé a las unidades digitales como medio de cambio y almacenamiento de valor así como, en su caso, unidad de cuenta; el tratamiento que otras jurisdicciones les den a unidades digitales particulares como activos virtuales, así como los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades.

Para tratar con activos virtuales en México es necesario estar regulado como una ITF, i.e., una Institución de Tecnología Financiera. La Ley Fintech no diferencía la topología de criptodivisas como FINMA en Suiza, y sólo considera activos virtuales legales los que Banxico designe. La Ley Fintech es un instrumento legal estricto en México que le otorga a Banxico amplios poderes sobre el futuro y uso corriente de esta tecnología. Por ello, la mayor parte del desarrollo tecnológico en relación a criptodivisas se lleva fuera de México, en legislaciones amigables como Wyoming en los EUA House Bill No. HB0185 (2019) y Malta Schembri (2018).

2.8. Las Criptodivisas en el Emprendimiento

Es imposible hablar de criptodivisas sin tocar el tema del emprendimiento y las startups. De acuerdo a Toby Lewis (2013), pocos trabajos han resumido tan bien el rol del emprendedor en la sociedad capitalista, como el de Joseph Schumpeter en 1942 "Capitalismo, Socialismo y Democracia". En él argumenta, que al introducir combinaciones nuevas de mercados y productos, los pequeños emprendedores generan métodos nuevos y más eficientes de desplazar a las compañías con bajo desempeño, un proceso que llamó: Destrucción Creativa Schumpeter (1942).

Formalmente una startup es cualquier compañía u organización diseñada para buscar un modelo de negocios repetible y escalable Blank (2013) *en un ambiente de alta incertidumbre*. Se espera que una startup opere con recursos justos (semejante a manufactura esbelta) y que tenga una curva de crecimiento alta. El ciclo financiero y etapas estratégicas de una startup se ven representadas en la Fig. 11. Las criptodivisas y la tecnología de la cadena de bloques son herramientas tecnológica y financieras que habitualmente son usadas por organizaciones de este tipo, ya sea como una herramienta de levantamiento de capital, o como una herramienta para generar una ventaja competitiva.

2.8.1. Etimología del Término *Startup*

El origen del término startup, usado para referirse a un negocio pequeño en vías de crecimiento, fue documentado primero en una edición de la revista Business Week, el 5 de septiembre de 1977 Startup Etymology (2015).

Sin embargo, la idea de una empresa en búsqueda de un modelo de negocio replicable y escalable no se popularizó hasta mediados de los noventa, cuando a través del internet, hubo un cambio de raíz en el método con el que se hacían los negocios, consecuentemente creando lo que se conoce como la burbuja Dot-Com. La era de las criptodivisas ha traído periodos de especulación semejantes a los vistos en la burbuja Dot-Com, sin embargo, estos han sucedido en mercados secundarios diferentes, de carácter global y con regulaciones que en algunos casos son muy diferentes.

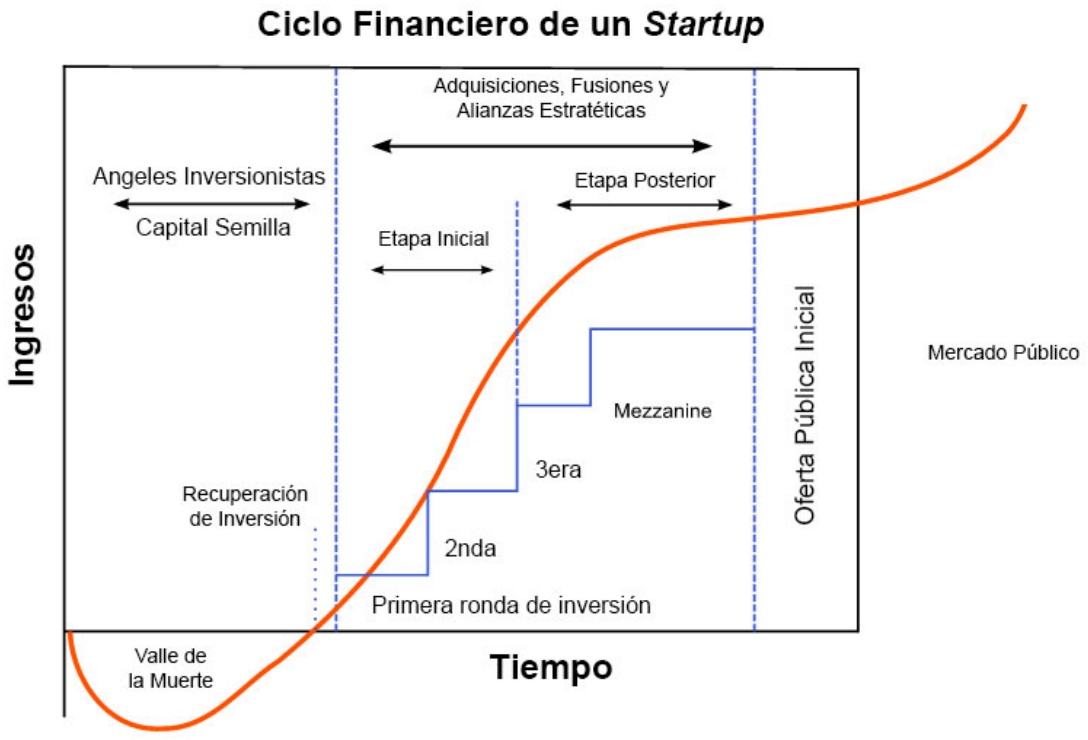


Figura 11: La vida de una startup. Fuente Ries (2011)

3. Administración de Riesgo

Todo negocio toma riesgos basados en dos factores: la probabilidad de que circunstancias adversas intervengan, y el costo de dichas circunstancias adversas. La administración de riesgo es el estudio de cómo controlar estos riesgos y maximizar las posibilidades de ganancias.

La administración del riesgo es la identificación, evaluación y priorización de los riesgos[13], seguidos por aplicación económica coordinada de recursos para minimizar, monitorear y controlar la probabilidad y el impacto de eventos infortunados o para maximizar la realización de oportunidades Hubbard (2009). El objetivo de la administración del riesgo es asegurarse de que la incertidumbre no afecte los objetivos de negocio.

[13] Definidos en el estándar ISO 31000 como el efecto de la incertidumbre en los objetivos

Los riesgos pueden venir de varias fuentes, incluyendo incertidumbre en mercados financieros, amenazas de fallas de un proyecto en sus diversas fases (diseño, producción y sustento), riesgos legales, accidentes, causas naturales, desastres, ataques deliberados, crediticios o de causas no identificadas. Se definen dos tipos de eventos, los negativos, que pueden ser clasificados como riesgos y los positivos que se consideran como oportunidades.

Hay varios estándares de administración de riesgo que se han desarrollado:

- El instituto de la administración del riesgo,
- El instituto nacional de estándares y tecnología,
- Sociedades actuariales,
- Estándares ISO.

Los métodos, definiciones y metas varían ampliamente de acuerdo al método de administración de riesgo, seguridad, ingeniería, procesos industriales, portafolios financieros, evaluaciones actuariales, salud pública y seguridad en general. Las estrategias para manejar los riesgos típicamente incluyen evadir el riesgo completamente, reducir los efectos negativos, la probabilidad de la amenaza o en el caso de un evento considerado una oportunidad, la retención de algunas o todas de las características anteriores.

3.1. Riesgo Financiero

Por definición, el riesgo financiero es cualquier tipo riesgo asociado con finanzas, incluyendo transacciones financieras o préstamos. Comúnmente se entiende como el riesgo de pérdidas, es decir, el potencial de pérdida financiera y la incertidumbre de su extensión.

Hay una ciencia que evolucionó alrededor de manejar el mercado y el riesgo financiero. La teoría del portafolio moderno, del Dr. Harry Markowitz Markowitz (1952). Dentro de este esquema, la varianza (o desviación estándar) de un portafolio, se identifica como el riesgo.

Tipos de riesgo financiero:

- **Riesgo de activos respaldados:** El riesgo de activos respaldados es el riesgo de que cambios en uno o más activos que soporten valores respaldados por activos puedan significativamente impactar al valor soportado. Los riesgos incluyen tasa de interés, modificación de términos y riesgo de pre-pago. Un valor respaldado por activos es un valor respaldado por el efectivo que pueda venir de varios otros activos. El valor financiero puede ser respaldado por deuda de varios tipos y otras cosas.

- **Riesgo de administración de crédito:** Es una profesión que se enfoca en reducir y prevenir pérdidas a través del entendimiento y medición de las causas posible de pérdidas. El riesgo de administración de crédito es usado por bancos, prestadores y otras instituciones financieras para mitigar pérdidas asociadas principalmente con el no-pago de préstamos.

- **Riesgo de Intercambio Internacional:** También conocido como riesgo FX, o riesgo cambiario, es el que ocurre cuando una compañía tiene una transacción con una compañía extranjera que utiliza otra divisa, que puede ser más o menos fuerte. Hay varios tipos de riesgo cambiario:

  - Riesgo transaccional: La diferencia cambiaria puede ocasionar limitantes de flujo de efectivo.
  - Riesgo de traducción: Es el riesgo que ocurre por el estado de resultados extranjero y la variación en los activos y deudas que pueden existir.
  - Riesgo económico: Riesgos políticos, regulatorios o económicos inherentes a transacciones internacionales.

- **Riesgo de liquidez:** Es el riesgo que ocurre cuando un activo o valor no puede ser intercambiado lo suficientemente rápido para prevenir que haya pérdidas, por ejemplo en una caída de precio o crisis.

- **Riesgo de mercado:** Las cuatro subdivisiones clásicas del Riesgo de Mercado son:

  - Riesgo de valores: Es el riesgo inherente a que los valores o su volatilidad puedan cambiar en general, no en particular.

  - Riesgo de interés: Es el riesgo de que las tasas de interés o la volatilidad implícita puedan cambiar. El riesgo de los cambios en mercados y su impacto en la probabilidad de que un banco lleve el riesgo de esos intereses. Está claro que los riesgos no siempre son negativos para el consumidor.
  - Riesgo de divisa: El riesgo de que cualquier activo que esté valuado en una divisa pueda cambiar de precio debido a fluctuaciones propias de la divisa.
  - Riesgo de productos básicos: Es el riesgo de que el precio real o implícito de productos básicos (maíz, petroleo crudo, cobre) pueda cambiar.

- **Riesgo operacional:** El riesgo que una compañía o individuo debe enfrentar debido a su propia operación y decisiones.

3.1.1. Riesgos Financieros Particulares a Criptodivisas

Cuando se lidia con criptodivisas en mercados financieros, existen algunos riesgos particulares con los cuales hay que lidiar. Las criptodivisas son un tipo de activo diferente a los activos con valor intrínseco y derivados, con características y riesgos financieros diferentes, algunos explicados a continuación:Buchholz et al. (2012)

- **Riesgo de precio o volatilidad:** Este es un riesgo de mercado, derivado del riesgo de valores y es inherente a las criptodivisas, debido a que su valor puede cambiar en cualquier momento.

- **Riesgo Regulatorio:** En la intersección entre riesgo de intercambio de internacional y de mercado, este riesgo económico, político y regulatorio se debe a que la situación legal y fiscal de las criptodivisas está poco clara y podría cambiar en cualquier momento. La falta de claridad fiscal es una limitante importante para fondos de inversión tradicionales.

- **Riesgo de Custodia:** Este riesgo, fundamentalmente operativo, tiene que ver con que la tecnología es poco conocida y custodiar criptodivisas en el 2019, requiere conocimiento especializado y lidiar con software o hardware que tiene canales de ataque muy particulares. Existen pocos servicios de custodia y el riesgo es poco entendido, por ello es común que un usuario, particular o institucional tenga que almacenar las llaves que representan propiedad sobre los activos personalmente.

3.1.2. Medir riesgo de Mercado: Valor en riesgo

Valor en riesgo (VeR) es una medida del riesgo de pérdida de inversión. Estima qué tan probable es que un conjunto de inversiones puedan perderse de acuerdo a condiciones nominales del mercado acotadas a un periodo de tiempo, como un día o una semana. VeR es usado por firmas y reguladores en la industria financiera para valorizar el tamaño de los activos requeridos para cubrir una pérdida.

Para un portafolio específico con un horizonte de tiempo y una probabilidad p, la p VeR se define informalmente como la máxima pérdida posible. Por ejemplo, un VeR diario de 5 % de $ 1 millón, quiere decir que hay un probabilidad de 0,05 de que el valor del portafolio disminuya por $ 1 millón. Informalmente, esperaríamos que perdiera $ 1 millón uno de cada 20 días (5 %).

La medida de riesgo del VeR define riesgo de valores de mercado de un portafolio fijo dentro de un rango de tiempo definido. Por ello, es de utilidad limitada para proyectar riesgos a futuro. Sin embargo, la utilización de VeR impone una metodología estructurada para el pensamiento crítico de riesgo.

3.2. Administrando el Riesgo Inversiones de Alto Riesgo

3.2.1. Instrumentos Derivados

Un instrumento derivado financiero es un producto financiero cuyo valor está basado en el precio de otro activo: el activo subyacente. Un ejemplo puede ser el valor de un contrato futuro sobre el maíz, el cual está basado en el precio de mercado del maíz. Los subyacentes pueden ser muy diferentes, acciones, índices bursátiles, valores de renta fija, tipos de interés o también materias primas. Existen diferentes tipos de "contratos" derivados, que son administrados por instituciones bancarias y ejecutados en mercados específicos, como el *New York Futures Exchange* o el *London Internation Futures Exchange*.

Entre las operaciones más comunes se encuentran las operaciones de permuta financiera, los contratos futuros y las opciones, cuya variante la "Opción Europea" es de particular

interés, pues existen metodologías para su valoración relevantes para la administración de riesgo, como lo es el modelo de Black-Scholes.

3.2.2. El Modelo de Black-Scholes

El modelo de Black-Scholes-Merton es un modelo matemático para las dinámicas del mercado financiero con instrumentos derivados. Utilizando la derivada parcial del modelo, conocida como la ecuación Black-Scholes, uno puede deducir la fórmula de Black-Scholes-Merton, que entrega un estimado teórico del precio de opciones de estilo Europeo y muestra que una opción tiene un precio único sin importar el riesgo del valor y su retorno esperado.Black and Fischer (1973) La creación de esta fórmula trajo legitimidad matemática a las actividades del *Chicago Board Options Exchange* y trajo un boom en los mercados de intercambio de opciones. Se sigue usando ampliamente, a veces con algunos ajustes o modificaciones.

La ecuación de Black-Scholes es una ecuación diferencial parcial que describe el precio de la opción a través del tiempo:

$$\frac{\partial V}{\partial t} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2} + rS\frac{\partial V}{\partial S} - rV = 0 \tag{1}$$

En donde:

- $S(t)$, el precio de activo subyacente en el tiempo t,
- $V(S,t)$, el precio de la opción en función del activo subyacente S en el tiempo t,
- $C(S,t)$, el precio de la opción Europea de compra y $P(S,t)$, el precio de la opción Europea de venta,
- K, el precio de ejercicio de la opción,
- r, la tasa de interés libre de riesgo, compuesta continuamente,
- σ, la desviación estándar de los retornos , esta es la raíz cuadrara de la variación cuadrática de los precios del activo,
- t, tiempo en años, generalmente usamos: ahora = 0, tiempo de expiración = T.

Fundamentalmente, la ecuación de Black-Scholes describe que uno puede cubrir el riesgo de una opción comprando y vendiendo el activo subyacente justo en el modo adecuado, eliminando y cubriendo contra el riesgo de pérdidas. Esta cobertura implica que sólo hay un precio correcto de venta para la opción, que retorna la fórmula de Black-Scholes.

Otra observación importante de la ecuación de Black-Scholes, es que el valor de una opción es proporcional a la volatilidad del activo subyacente. Contrario a opinión popular, la volatilidad es una componente vital de cualquier sistema financiero.

En la práctica, el modelo de Black-Scholes tiene muchas imperfecciones y su aplicación requiere un entendimiento del sistema profundo, aunque ayuda a lograr una cobertura del riesgo de volatilidad, expone otros riesgos que no quedan resueltos. Es de interés que desde el 2017 el *Chicago Mercantile Exchange* lanzó futuros basados en Bitcoin y otras criptodivisas, el modelo de Black-Scholes se aplica comúnmente en estos mercados y su aplicación tiene las mismas limitantes que otros mercados de derivados.

3.2.3. El Capital de Riesgo

La administración de riesgo en la industria del capital de riesgo es una fundamentalmente, una cuestión de estrategia. Este ecosistema es una parte fundamental en el ecosistema de startups y florece con un modelo asimétrico altamente no lineal (mostrado en figura 12), en donde varios errores o pérdidas controladas dan lugar a una ganancia sin ninguna limitante clara. Es decir, las perdidas son limitadas y las ganancias no. Es común que un fondo de inversión logre sus ganancias con una sola startup de 100 inversiones. Como ejemplo, el fondo de inversión de riesgo Andreessen Horowitz hizo 78 millones de dólares con una (1) inversión de 250 mil dólares en la plataforma Instagram en tan sólo dos años. En terminos prácticos quiere decir que hubiera podido invertir (ver ecuación 2) en 311 otras startups y aún duplicar su inversión al cabo de dos años.

$$78,000,000/250,000 = 312 \tag{2}$$

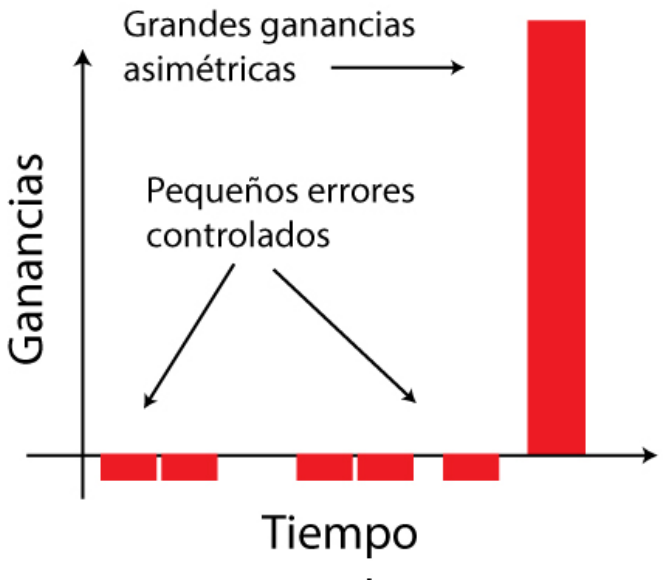


Figura 12: Una representación gráfica del riesgo y las posibles ganancias asimétricas de fondos de inversión de riesgo. Fuente: Generación propia.

El autor Nassim Nicholas Taleb describe este fenómeno utilizando teoría de juego Taleb (2012) y utiliza la desigualdad de Jensen para describirlo. Describe un fenómeno en donde se estimula hacer errores constantes y cuantificables, (i.e., experimentar) y finalmente el sistema tiende a ganar. Para un fondo de inversión de riesgo o cualquier inversión de alto riesgo, las pérdidas siempre son controladas y cuantificables, pero las ganancias no tienen límite superior definido. Son una función con distribución convexa Taleb (2012), lo opuesto a una distribución normal o *campana*. Algo que se describe correctamente con la desigualdad de Jensen, que generaliza la noción de que la línea secante de una función convexa siempre yace *arriba* de la función, como se muestra en la figura 13. Esta estrategia funciona siempre que se puede hacer un número grande inversiones pequeñas con retornos potenciales muy altos, para cual es necesario alta volatilidad. Esta estrategia no es diferente a la que siguen algunos fondos de inversión, que suelen limitar el monto de sus inversiones a menos del 1 % de su monto principal.

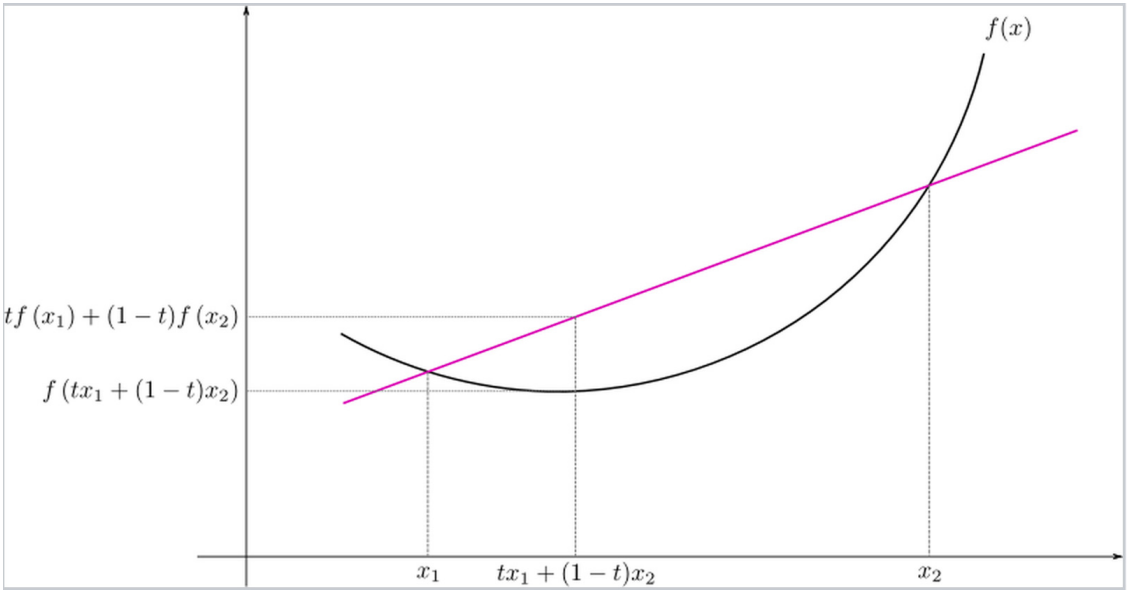


Figura 13: La desigualdad de Jensen comprueba la noción de que la línea secante de una función convexa yace arriba de la función. Fuente: Needham (1993).

3.3. Evaluación de Sistemas de Criptodivisas

Si la designación de activos se divide en activos con valor intrínseco y con valor derivado, las criptodivisas no cumplen con las características de ninguno y se sirven mejor de describirse con un modelo nuevo. Por ello que no hay muchos parámetros para la evaluación de sistemas en materia financiera.

Es un hecho que la componente financiera de estos sistemas es la más desarrollada, tanto en materia operativa, como legal. Operativamente, las personas que se han dedicado al intercambio de criptodivisas se han servido de data para la evaluación de estos sistemas, data que fundamenta o valida sus diversas hipótesis de inversión. En términos generales, esta data se puede dividir en data dentro de la cadena de bloques y data fuera de la cadena de bloques.

Para ello hay que entender el ciclo de vida da la data del mercado, que existe en diferentes planos y es accesible en diferentes momentos a diferentes jugadores.

3.3.1. Data externa al sistema de criptodivisas

El origen de esta data es normalmente un mercado, tal como una casa de cambio o algún servicio tercero. Esta data no está persistida en la cadena de bloques, y normalmente es valiosa por si sola. Esta data no es muy diferente a la originada en cualquier sistema de intercambio, y el perfil financiero se encontrará en un ambiente familiar. La mayor parte de esta data está ligada al precio, habitualmente seguido a través del tiempo y en otros casos correlacionado a otros parámetros, como volumen de intercambio, frecuencia, etc.

Esta data puede ser de naturaleza menos confiable, que la data en la cadena de bloques, ya que es susceptible a manipulación unilateral, sin embargo tiene un valor importante.

1. **Data de mercado:** Existen casas de cambio distribuidas por todo el mundo, estos son negocios regulados, que operan de manera muy semejante a casas de cambio de divisas, la bolsa, etc. Cabe recalcar, que la data de intercambio, el libro de pedidos, con información de intercambios en ningún momento se almacena ni se refleja en la cadena de bloques. Desde RI5C, las casas de cambio se visualizan como clusters, y sólo vemos depósitos y retiros.

2. **Data de algún proveedor tercero:** Hay proveedores terceros que también pueden acumular data, como casas de subasta para criptodivisas no financieras.

3. **Metadata:** En diversos lugares del internet, puede haber referencias a carteras o transacciones. Estas se pueden referenciar en casi cualquier tipo de sitios, en blogs, foros o redes sociales. Esta es data no estructurada que requiere trabajo arqueológico para obtenerse, sin embargo, algunos navegadores de la cadena de bloques almacenan metadata que la propia comunidad genera. De tal modo que si alguna casa de cambio fue robada, por ejemplo, es común que estos sitios anexen una etiqueta visible desde su navegador para ayudar a la comunidad a identificar actores importantes o peligrosos.

3.3.2. Data intrínseca al sistema de criptodivisas

La data intrínseca al sistema, es data almacenada dentro de la cadena de bloques, esta data tiene una estructura estática, aunque hay diversos niveles de almacenarla y puede cambiar, lentamente, con el tiempo. El espacio en la cadena de bloques es caro y limitado, por lo que data persistida en el sistema suele ser el mínimo necesario para cumplir los requerimientos. La data común intrínseca al sistema es la mínima data para un sistema bancario: es decir, se almacenan transacciones, compuestas por emisor, receptor y monto. Adicionalmente a esto, hay cierta metadata necesaria para el funcionamiento del sistema, tal como el sello de tiempo, función hash de la transacción etc.

3.3.3. Correlaciones entre Data Intrínseca y Externa

En un intento por profundizar las métricas de mercado tradicionales, la comunidad ha generado algunos datos que triangulan entre varias fuentes y obtienen data de utilidad para el intercambio de criptodivisas. Esta área, empujada por intereses comerciales, está en la intersección entre data de mercados tradicionales y data de la cadena de bloques. Dos ejemplos relevantes descritos a continuación, sin embargo, existen incontables ejemplos de métricas así,[14] y al menos 20 documentados correctamente:

- **Tasa NVT:** Del inglés *Network Value to Transactions Ratio* o relación entre la valoración de la red y sus transacciones, es semejante a la relación precio / ganancia en mercados tradicionales, se utiliza como parámetro para detectar si está sobre o sub-valuado. Cuando el NVT de Bitcoin es alto, indica que la valoración de la red supera el valor total transmitido en su red de pagos, la hipótesis detrás, es que esto sucede cuando la red está en estados de crecimiento.Woo (2019) Este parámetro, utiliza datos de mercado como precio, y datos de la cadena de bloques, como las transacciones.

- **Impulso de la Red de Bitcoin:** El Impulso de la Red, fue creado por Philip Swift y está basado en el valor transmitido a través de la cadena de bloques (data intrínseca), graficado contra el precio de Bitcoin (data externa).Woo (2019) Se utiliza como un

[14] Es común que los *traders* describan métricas, gráficas y parámetros útiles para encontrar patrones en precios de criptodivisas en la plataforma de Twitter, de donde es difícil rescatar datos detallados.

indicador de mercado en expansión, ya que para alimentar la expansión, es necesario la transmisión de mucho valor.

3.4. Diversificadores y Riesgos en Criptodivisas

La crisis financiera global reciente y la crisis de deuda soberana europea han obligado a inversionistas e instituciones financieras a identificar activos que protejan sus inversiones en caso de condiciones del mercado extremas o riesgos sistémicos Stavroyiannis (2018).
En estos términos se distinguen las criptodivisas como diversificadores y refugios seguros. Hasta ahora, el oro parece el ejemplo más prometedor de un refugio seguro que puede ayudar a inversionistas a diversificar su riesgo en caso de crisis. Sin embargo, las criptodivisas han emergido en gran variedad durante los último años. El término cripto divisa como tal, se inició en la comunidad de Bitcoin (BTC o XBT) en MtGox (Magic the Gathering online exchange) casi al mismo tiempo del Linden Dollar de Second Life. Otras criptodivisas surgieron de los pasos de Bitcoin, más notoriamente Ethereum en el 2015.

Los riesgo de una inversión en la industria de las criptodivisas se puede dividir, en general, en varias categorías que surgen del riesgo de mercado Beecroft (2015):

1. Riesgo de mercado: Cualquier elemento intrínseco a un sistema de criptodivisas que pueda ocasionar la caída o el incremento del precio de un activo.

2. Riesgo regulatorio: Elementos externos que por definición pueden modificar el precio de una criptodivisa al cambiar el ámbito legal y regulatorio en el que se desempeñan.

3. Riesgo de custodia: Dado que la tecnología es muy nueva y en algunos casos confusa, existe un riesgo grande de perder el acceso a una criptodivisa.

4. Riesgo de ejecución: Cada criptodivisa es desarrollada por un grupo de personas que pueden o no estar agrupados por una compañía. Existe un riesgo operacional intrínseco a la ejecución de la compañía.

Esta investigación se enfoca en la evaluación de sistema de criptodivisas, requerimiento fundamental previo a poder administrar el riesgo en diversas aplicaciones, desde el espectro financiero hasta el operativo y de diseño.

4. Teoría de Grafos

En el campo de las matemáticas, la teoría de grafos es el estudio de grafos, estructuras matemáticas que se usan para modelar relaciones entre conjuntos de pares de objetos. En este contexto, un grafo está compuesto de vértices (nodos o puntos) conectados por aristas. Hay una distinción entre grafos direccionados donde las aristas vinculan nodos simétricamente y grafos no-direccionados, donde las aristas tienen una dirección.

En el sentido más básico, un grafo es un par ordenado $G = (V, E)$ compuesto de un conjunto de vértices V junto con un conjunto de aristas E que a su vez son sub-conjuntos de dos elementos de V. Es decir, una aristas está definida por dos nodos.

Hay muchas aplicaciones a la teoría de grafos para mostrar relaciones en procesos físicos, biológicos, sociales y de sistemas de información. Muchos problemas prácticos pueden ser representados usando grafos. La teoría que expresa y busca entender sistemas reales como redes se conoce como **teoría de redes**.

4.1. Sistemas Complejos

La teoría de grafos está particularmente bien adecuada al entendimiento de sistemas complejos. Un sistema complejo es un sistema creado con varios componentes que interactúan entre si. Ejemplos típicos son: organismos, el cerebro, infraestructura eléctrica, sistemas de comunicación, el clima global y sistemas económicos, tales como las criptodivisas. El comportamiento de sistemas complejos es intrínsecamente difícil de modelar debido al gran número de dependencias, relaciones e interacciones entre las partes. Los sistemas complejos tienen diversas propiedades que emergen de estas relaciones, como no-linealidad, orden espontáneo, adaptación y ciclos de retroalimentación. Debido a estas particularidades, los sistemas complejos son tema de su propia área de investigación. En muchos casos, es útil representar estos sistemas como redes, en donde los nodos representen las componentes y las aristas sus interacciones.

4.2. Teoría de Redes

La teoría de redes es el estudio de grafos como una representación de relaciones simétricas o asimétricas entre objetos discretos. En ciencias de la computación y ciencias de redes, la teoría de redes es parte de la teoría de grafos, una red puede ser definida como un grafo en donde los nodos y aristas tienen atributos.

La solución de los siete puentes de Königsberg dada por Leonard Euler, publicada en 1736 Biggs et al. (1986) es considerada como la primera verdadera prueba en teoría de redes. Este problema matemático histórico trataba de encontrar una ruta que cruzara todos los puentes una sola vez, (ver la figura 14). Euler probó que el problema no tiene solución, para ello comprobó que la elección de ruta dentro de cada masa geográfica era irrelevante, lo único importante era la secuencia en la que se cruzaban los puentes. De tal modo que definió el sistema como una red con cuatro nodos (las áreas geográficas identificables en la figura 14) y 7 aristas, (los puentes). La estructura resultando es un grafo. Euler crea una formula que relaciona el número de vértices y aristas en un poliedro como una abstracción de los puentes y procede a comprobar que siempre y cuando los nodos no tengan un número de aristas par, problemas semejantes no tendrán solución.

La teoría de redes tiene aplicaciones en varias disciplinas, incluyendo física estadística, ciencias de la computación, ingeniería eléctrica, biología, economía, finanzas, operaciones, ecología y sociología. Problemas de redes que involucran encontrar una manera óptima de resolver un problema se conocen como optimización combinatoria. Ejemplos importantes incluyen análisis de ruta crítica, problema de la distancia más corta, etc.

4.3. Análisis de Redes

El análisis académico de estructuras de redes complejas que mezcla elementos de teoría de grafos, mecánica estadística, minado de datos, visualización de información y ciencias de la computación, se conoce como análisis de redes y se define como el estudio de representaciones de redes de fenómenos físicos, biológicos y sociales que llevan a modelos predictivos de dichos fenómenos. Las redes se pueden entender con base en las siguientes cualidades.

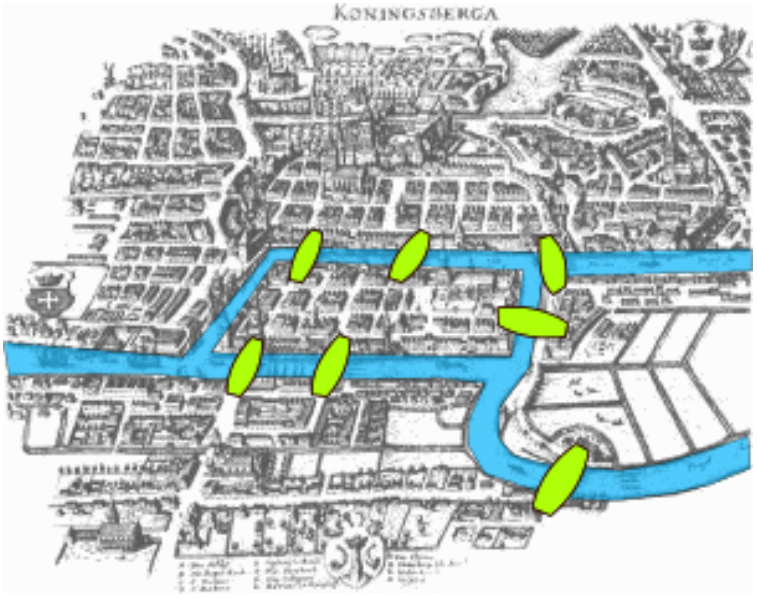


Figura 14: Los 7 Puentes de Konigsberg. Fuente: Biggs et al. (1986).

4.4. Propiedades de una Red

4.4.1. Tamaño

El tamaño de una red se define como el número de nodos N o el número de aristas E. En el caso de un grafo simple, una red en donde cuando menos hay una arista E que existe entre nodos y estos no se conectan entre sí. El tamaño máximo se puede definir como $E_{max} = \frac{N}{2}$, sin embargo, para grafos con múltiples aristas entre nodos, el tamaño puede ser infinito: $E_{max} = \infty$.

4.4.2. Densidad y Grado

La densidad D de una red se define como la tasa entre el número de aristas E y el número posible de aristas en una red con N nodos. Muy relacionado a la densidad, también existe el *grado promedio*. Definido como $\langle k \rangle = \frac{2E}{N}$ para redes no-direccionadas y $\langle k \rangle = \frac{E}{N}$ para redes direccionadas.

4.4.3. Diámetro de una red

Otro método para medir redes de grafos se define como la más larga entre las trayectorias; o la distancia más corta entre los nodos más alejados de una red. En otras palabras, una vez que la trayectoria más corta entre todos los nodos es calculada, el diámetro es la trayectoria más larga. Es una representación del tamaño lineal de una red.

4.4.4. Trayectoria Característica

El promedio de la trayectoria-más-corta entre nodos se calcula encontrando la trayectoria más corta para todos los pares de nodos y obteniendo un promedio simple entre todas las trayectorias, esto se conoce como la trayectoria característica de una red. Se define como la distancia $d_{u,v}$ entre dos nodos u y v de una red. Esto nos muestra, en promedio el número de pasos que toma llegar entre un miembro de la red y otro. El comportamiento de la trayectoria más corta como una función del número de vértices N de una red define comportamientos importantes de ciertas redes.

4.4.5. Conectividad

El modo en que una red está inter-conectada juega un papel importante en cómo se analiza e interpreta. En general, las redes están clasificadas en cuatro categorías:

- **Clique/grafo completo:** Una red completamente conectada, en donde todos los nodos se conectan entre sí. Estas redes son simétricas en el sentido que todos los nodos tienen conexiones hacia dentro y hacia afuera de otros nodos.
- **Componente gigante:** Un único componente conectado que contiene la mayor parte de los nodos en la red.
- **Componente débilmente conectado:** Un conjunto de nodos en donde existe una trayectoria entre cualquier par de nodos, ignorando la direccionalidad de la red.
- **Componente fuertemente conectado:** Un conjunto de nodos en donde existe una trayectoria *direccionada* entre cualquier par de nodos.

4.4.6. Medidas de centralidad

Información de la importancia relativa de nodos y aristas en un grafo se puede obtener a través de medidas de centralidad. Por ejemplo, la centralidad de los eigenvectores usa los eigenvectores de las matriz adyacente que corresponde a una red para determinar los nodos más frecuentes.

La centralidad indica los vértices más importantes dentro de un grafo. Aplicaciones típicas involucran detectar a la persona más influencial en redes sociales, nodos claves en redes urbanas o en el internet o super-dispersores de una enfermedad.

Una de las desventajas de las medidas de centralidad es que son muy particulares a la aplicación específica. Es decir, la medida de centralidad para una red social de conexiones en Twitter, por ejemplo, puede ser inútil para medir la centralidad de una red de transacciones financieras.

Las medidas de centralidad más importantes son:

- **Grado de centralidad:** Históricamente la primera medida de centralidad y conceptualmente la más sencilla. Se define como el número de aristas que tiene un nodo. Se puede interpretar de muchos modos, como que un nodo bien conectado está en mayor riesgo de captar lo que sea que se transmita por una red. En casos donde las aristas de la red tengan dirección, se definen dos medidas de centralidad, interna y externa. Interna es una cuenta de los vértices dirigidos hacia el nodo, y externa una cuenta de los vértices dirigidos afuera del nodo.

  El grado de centralidad Sabidussi (1966) de un vértice v para un grafo $G := (V, E)$ con vértices $|V|$ y aristas $|E|$ se define como:

$$C_D(v) = deg(v) \tag{3}$$

  donde deg es el grado de centralidad.

- **Centralidad de cercanía:** En un grafo conectado, es una medida de la centralidad de una red, se calcula como el recíproco de la suma de la longitud de la trayectoria más corta entre un nodo y los demás nodos del grafo. De tal modo que mientras más céntrico un nodo, está más cerca del resto de los nodos. La cercanía fue definida por Bravelas (1950) como el recíproco de la lejanía, de tal modo que se define cono C, en donde:

$$C(x) = \frac{1}{\sum_y d(y,x)} \tag{4}$$

  donde $d(y,x)$ es la distancia entre los vértices x y y. Normalmente nos referimos a la forma normalizada que representa la longitud promedio de las trayectorias más cortas.

- **Centralidad de intercesión:** Es la medida de centralidad de un grafo basado en las trayectorias más cortas. Para cada par de vértices en un grafo conectado existe al menos una trayectoria más corta entre los vértices, de tal modo que la suma de aristas (para grafos no pesados) o la suma de los pesos de las aristas (para grafos pesados) se minimice.

  La medida de intercesión encuentra amplias aplicaciones en teoría de redes, representa el grado en que los nodos se interponen entre sí. Por ejemplo, en una red de telecomunicaciones, un nodo con mayor intercesión tiene mayor control sobre la red. El grado de intercesión Freeman (1977) se define como g en donde:

$$g(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{5}$$

  donde σ_{st} es el número total de trayectorias más cortas entre el nodo s y el nodo t y $\sigma_{st}(v)$ es numero de esas trayectorias que pasan por v.

- **Centralidad de eigenvectores:** También llamada eigencentralidad, es una medida de la influencia de un nodo en una red. Calificaciones relativos son asignados a todos los nodos en una red de acuerdo al concepto de que las conexiones a nodos con calificaciones más altas contribuyen más que aquellas a nodos con calificaciones bajas. Los algoritmos de clasificación de páginas de Google y la centralidad de Katz son variaciones de

eigencentralidad.

Se puede utilizar la matriz adyacente para encontrar la eigencentralidad Newman (2009). Para un grafo $G := (V, E)$ con $|V|$ vértices, donde $A = (a_{v,t})$ es la matriz adyacente, i.e., $a_{v,t} = 1$ si el vértice v está conectado al vértice t y $a_{v,t} = 0$ en el caso opuesto. La calificación de centralidad relativa, x, de un vértice v se define como:

$$x_v = \frac{1}{\lambda} \sum_{t \in M(v)} x_t = \frac{1}{\lambda} \sum_{t \in G} a_{v,t} x_t \tag{6}$$

donde $M(v)$ es un grupo de vecinos de v y λ es una constante. Despejando y reduciendo un poco, esto se puede escribir como la ecuación de eigenvectores:

$$Ax = \lambda x \tag{7}$$

Puede haber muchos diferentes eigenvalores λ para los cuales existensoluciones de eigenvectores no triviales. Sin embargo, el requerimiento adicional de que los eigenvectores sean no-negativos implica (de acuerdo al teorema Perron-Frobenius Perron (1907)) que sólo los eigenvalores más altos resulten la medida de centralidad deseada. El componente número v del eigenvector relacionado dará la calificación de centralidad relativa del vértice v de una red. El eigenvectore sólo se define hasta un factor común, de tal modo que que sólo las tasas de las centralidades de los vértices estén bien definidas. Para definir una calificación absoluta, se deben normalizar los eigenvectores, de tal modo que la suma de todos los vértices sea 1 con el número total de vértices n. La Iteración de Potencia es uno de los varios algoritmos de eigenvectores que pueden utilizarse para encontrar el eigenvector dominante. Esto se puede generalizar de tal modo que las entradas en A puedan ser números reales que representen la fuerza de las conexiones.

- **Centralidad de Katz:** Fue introducida por Leo Katz en 1953 Katz (1953) y es utilizada para medir el grado relativo de influencia de un nodo en una red social. A diferencia de otras medidas de centralidad que consideran sólo la trayectoria más corta de un par de nodos, la centralidad de Katz mide la influencia tomando en cuenta el número total de trayectorias entre un par de nodos. Es semejante a la eigencentralidad, pero

específica a redes sociales.

La centralidad de Katz cumputa la influencia relativa de un nodo dentro de una red midiendo el número de vecinos inmediatos (nodos de primer grado) que se conectan a ese nodo y las conexiones con otros nodos más lejanos a través de los nodos vecinos. Conexiones hechas con nodos distantes, se penalizan con un factor atenuante α. A cada trayectoria o conexión entre nodos se le asigna un peso determinado por α y por la distancia entre nodos α^d. Se formula de la siguiente manera.

Deja A ser la matriz adyacente de una red. Los elementos $(a_{i,j})$ de A son variables que toman valor 1 si un nodo i está conectado a un nodo j y 0 si no. Las potencias de A indican la presencia o ausencia de conexiones entre dos nodos a través de intermediarios. Por ejemplo, en una matriz A^3, si el elemento $a_{2,12} = 1$, indica que el nodo 2 y el nodo 12 están conectados a través de conexiones de primero y segundo grado. Si $C_{Katx}(i)$ denota la centralidad de Katz de un nodo i, entonces matemáticamente:

$$C_{Katz}(i) = \sum_{k=1}^{\infty} \sum_{j=1}^{n} \alpha^k (A^k)_{ij} \tag{8}$$

Donde la locación de un elemento (i, j) de A^k refleja el número total de conexiones grado k entre nodos i y j.

Resumen

En una red de transacciones financieras como la propuesta, una medida de centralidad puede dar información importante de un nodo. Se espera que ciertos nodos tengan alto grado de centralidad, como lo puede ser un mercado secundario o una cuenta administrativa que gestione la distribución de activos.

4.5. Propagación en Redes

El contenido en una red compleja se puede propagar a través de dos métodos fundamentales: Propagación contenida y propagación no-contenida. En la propagación contenida,

el contenido total en una red se mantiene constante. En la propagación no-contenida, la cantidad de contenido cambia conforme este pasa por redes complejas.

4.6. Redes Interdependientes

Existen sistemas de redes que son interdependientes entre sí, en donde nodos de una red pueden depender de nodos de otra red. Estas dependencias pueden descubrirse fácilmente con desarrollos de tecnología de la información. Estas dependencias pueden llevar a fallas en cascada entre las redes, efectivamente propagando un error posiblemente pequeño hasta una falla catastrófica de un sistema. Los *apagones* convencionales son una manifestación interesante de cómo afectan las dependencias entre redes.

4.7. Optimización de Redes

La optimización de redes involucra encontrar el método óptimo de hacer algo a través de la optimización combinatoria. Ejemplos importantes involucran flujo de redes, el problema de la ruta más corta, etc. En muchos casos, estos problemas son imposibles de resolver con otras herramientas. La optimización de una red de transacciones financieras tiene varias posibles aplicaciones en el mundo real, como lo puede ser agrupar transacciones que pudieron haber sido ofuscadas a través de diversos esquemas. En algunos otros casos, pudiera utilizarse un algoritmos semejante para aprovechar oportunidades de arbitraje en diferentes mercados de divisas. En aplicaciones más complejas de cadenas de bloques, como lo puede ser un esquema como Cryptokitties, en el que usuario adquiere activos coleccionables y se dedica a *cruzarlos* para generar activos de mayor valor, un análisis de optimización podría entregarle la ruta crítica para lograr un objetivo en el menor tiempo posible.

4.8. Topología Básica de Redes

4.8.1. Red Aleatoria

Grafo aleatorio es el término general para referirse a la distribución de probabilidad sobre grafos. Grafos aleatorios se pueden describir simplemente como un proceso aleatorio que los general. La teoría de grafos aleatorios yace en la intersección entre teoría de grafos y teoría de probabilidad. Desde el punto de vista matemático, los grafos aleatorios se utilizan

para responder preguntas de otros tipos de grafos y sus aplicaciones prácticas en todas las áreas en donde redes complejas tienen que modelarse.

4.8.2. Grafos Libres de Escala

Una red libre de escala es una red en donde la distribución de grado sigue una ley potencial, al menos asintóticamente. Es decir, cuando una fracción de los nodos de la red tienen varias aristas hacia otros nodos. En la práctica, muchas redes son libres de escala. Se pueden simular utilizando modelos de redes jerárquicas.

Estructura de comunidades

En el estudio de redes complejas, se dice que tiene una estructura de comunidad si los nodos de la red pueden ser fácilmente agrupados en conjuntos de nodos, a veces traslapados, de tal modo que cada conjunto de nodos este densamente interconectado. Cuando las comunidad no tienen subconjuntos traslapados, esto implica que la red se divide naturalmente en grupo de nodos con conexiones densas internas, pero sin conexiones entre grupos. La estructura de comunidades se puede usar para resolver un problema de búsqueda de comunidad, en la cuál se busca encontrar la comunidad a la que un nodo pertenece.

Contagio en Sistemas Complejas

El contagio de sistemas complejos, es un fenómeno visto en redes sociales, en que múltiples fuentes de exposición a un estímulo se necesitan para que un nodo adopte el cambio. Se distingue del contagio simple, porque puede no ser posible que el fenómeno se extienda a través de un solo nodo o exposición. El esparcimiento del contagio en sistemas complejos, por definición, depende de muchos factores. En un sistema financiero, el contagio podría representar un cambio de precio o de algún comportamiento emergente.

5. Propuesta de una metodología para la evaluación de un sistema de criptodivisas: RI5C

En este capítulo presentamos la metodología desarrollada, con una descripción comprehensiva de la herramienta tecnológica, cómo está estructurada y las componentes de diseño. Adicionalmente, se ejemplifican algunos usos de RI5C y se documentan sus servicios principales a fin de facilitar la colaboración.

5.1. Los Datos en la cadena de bloques

Pese a que los datos de transacciones en una cadena de bloques son públicas por naturaleza, no se encuentran de un modo fácil de interpretar y en algunos casos hay mucha información ofuscada por capas intermedias de la red. Tal es el caso de software de gestión de carteras basadas en claves HD (Hierarchical Deterministic), las cuales permiten la gestión de llaves *padre* que a su vez pueden generar una cantidad infinita de llaves *hijas*, de tal modo que se pierda el lazo del emisor.

5.1.1. Estructura de los Datos

Utilizaremos datos públicos de la red de Ethereum, desde su creación en el 2015 hasta el día de la publicación. Almacenaremos todo en una base de datos estructurada con lenguaje de bases de datos estructuradas SQL, de acuerdo a la estructura de datos propuesta en la Figura 15.

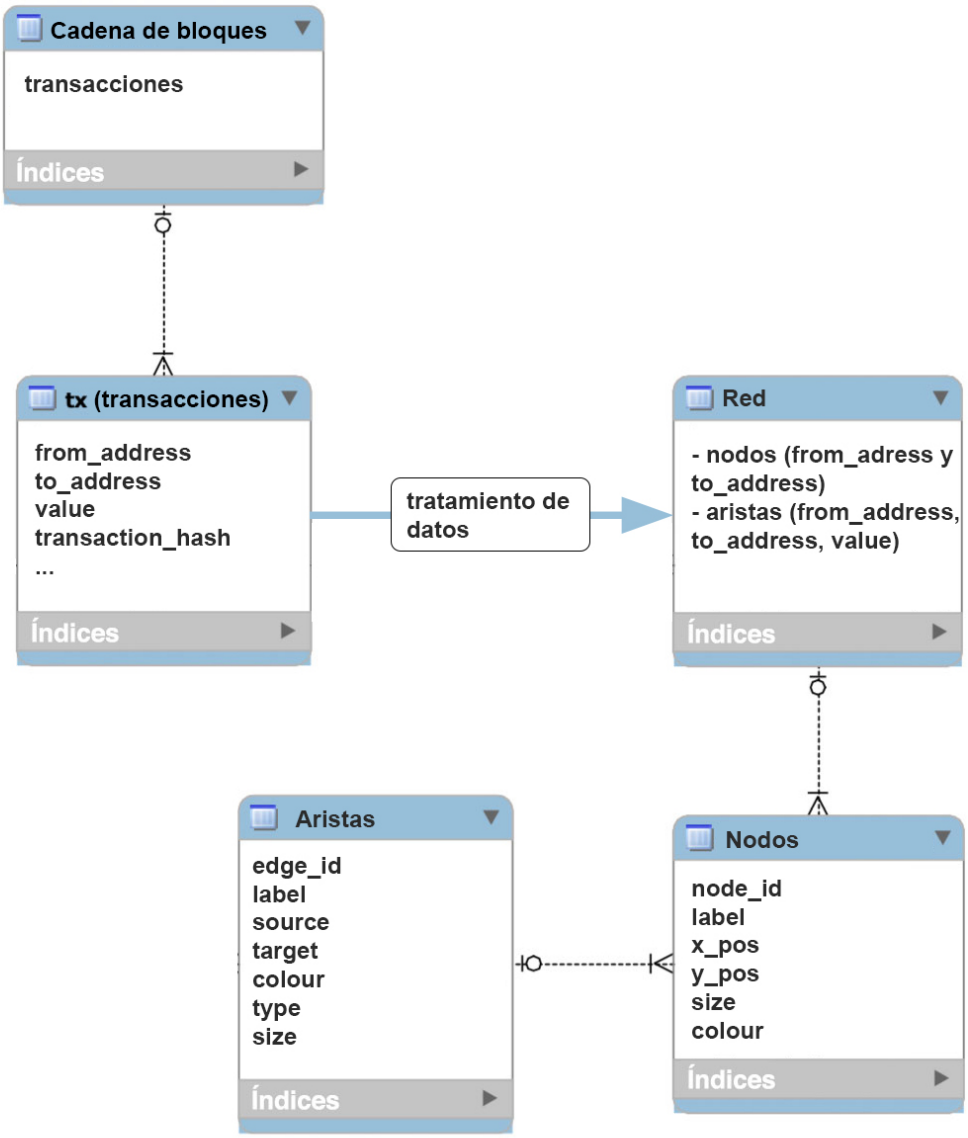


Figura 15: Estructura de datos obtenidos directamente de la cadena de bloques y tratados para conformar a una estructura de red. Fuente, Generación propia.

5.1.2. Topología de una Red de Criptodivisas

La red tendrá varios elementos importantes, clusters y súper clusters, que pueden ser elementos con actividad económica mucho mayor. Se puede correlacionar con cierta veracidad el volumen de las transacciones para entender que hay casas de cambio, inversionistas institucionales, FFF (Friends Fools and Family), inversionistas ángeles y traders.

Identificación de clusters Se ha visto que las transacciones almacenadas en la cadena de bloques son semi-anónimas, sin embargo, aplicando técnicas de clustering o etiquetado podemos agrupar transacciones y en los casos en los que exista información, podemos asignar una etiqueta a una cuenta en particular para identificar.

Se comienza a identificar clustering con unidades mínimas de identidad, que en este caso son las direcciones de contratos inteligentes provenientes de la generación de un token nuevo, que son las direcciones individuales de lo que llamaremos súper-clusters. Se utilizan métodos no convencionales para tratar de des-anonimizar los clusters y súper-clusters relevantes y tratar de organizarlos en categorías útiles. Finalmente, describimos las dinámicas de estos clusters a lo largo del tiempo. En muchos casos, estos súper clusters se pueden reducir a una entidad de negocios discreta con un grupo de direcciones y transacciones que se usan colectivamente para un propósito en general.

5.1.3. Los Contratos Inteligentes como Concentradores: *Clusters*

Se ha encontrado que durante un evento de generación de tokens, o para tal caso, la existencia de cualquier contrato inteligente, todas las transacciones se concentran en la dirección del contrato, lo cual definimos como un cluster. De tal modo que se puede monitorear la cuenta de un contrato inteligente como concentrador de transacciones. En algunos casos, podemos ver a varios contratos que definen un ecosistema, lo cual definimos como un súper cluster.

Dentro de un contrato inteligente, se pueden definir dos sub conjuntos de datos importantes:

1. Las transacciones de ETH (la moneda de cambio en la red de Ethereum) hacia el Token, con las cuales se convierte una cantidad especifica de ETH a una cantidad del Token. Un ejemplo real de estas se puede ver en el cuadro 1.

2. Las transacciones internas al Token, entre los diferentes dueños del token. Un ejemplo real de estas transacciones se puede ver en el cuadro 2.

Todos estos datos son de naturaleza pública y se pueden acceder utilizando interfaces para aplicaciones con relativa sencillez. Más aún **esta es la división mínima de una red que se puede utilizar como objeto de estudio.**

Transacción	**Bloque**	**Edad**	**Desde**	**Hacia**	**Valor [ETH]**
0xa4133901	5383181	5 mins ago	0xefa5e0ae	SnglrtToken	0.000910323
0x830c993c	5383160	10 mins ago	0x291ca568	SnglrtToken	0.000186655
0x1908cac0	5383154	12 mins ago	0xd74f65f5	SnglrtToken	0.00186335
0x476ecbf1	5382954	1 hr ago	0x2b5634c4	SnglrtToken	0.000559005
0x2dcb65d4	5382866	1 hr 20 mins ago	0x2b5634c4	SnglrtToken	0.000559005
0xbbacc5e7	5382589	2 hrs 20 mins ago	0x2b5634c4	SnglrtToken	0.000558045
0x80cd8eb0	5382079	4 hrs 21 mins ago	0x2b5634c4	SnglrtToken	0.000784005
0x8c2ea564	5381897	5 hrs 4 mins ago	0x2b5634c4	SnglrtToken	0.000559005
0x620720da	5381267	7 hrs 36 mins ago	0xf751033d	SnglrtToken	0.001525323
0x2625663a	5381214	7 hrs 51 mins ago	0xe5fc4ddf	SnglrtToken	0.000156609
0x49c931c7	5381157	8 hrs 4 mins ago	0xb2363b4f	SnglrtToken	0.000910323
0xba18db70	5381064	8 hrs 29 mins ago	0x2b5634c4	SnglrtToken	0.000559005
0xbb504831	5380903	9 hrs 8 mins ago	0x40d035a2	SnglrtToken	0.002349135
0xa5e3a311	5380902	9 hrs 8 mins ago	0x2b5634c4	SnglrtToken	0.000559965
0x68acb872	5380881	9 hrs 14 mins ago	0x2b5634c4	SnglrtToken	0.000558045
0xb308207e	5380864	9 hrs 17 mins ago	0x2b5634c4	SnglrtToken	0.000784005
0x0be5515d	5380842	9 hrs 23 mins ago	0x2b5634c4	SnglrtToken	0.000558045
0xf449c2bb	5380821	9 hrs 29 mins ago	0x2b5634c4	SnglrtToken	0.000784005
0xf13743ac	5380800	9 hrs 36 mins ago	0x2b5634c4	SnglrtToken	0.000559005
0xab41f13f	5380757	9 hrs 46 mins ago	0x2b5634c4	SnglrtToken	0.000559005
0xe0b71230	5380741	9 hrs 50 mins ago	0x2b5634c4	SnglrtToken	0.000558045
0x92970e96	5380730	9 hrs 52 mins ago	0x2b5634c4	SnglrtToken	0.000783045
0xc8c7243f	5380513	10 hrs 41 mins ago	0x75a7b8a7	SnglrtToken	0.001525323
0xe3b8de7c	5380423	11 hrs 3 mins ago	0xaf602888	SnglrtToken	0.001522699
0xade7cb9b	5380421	11 hrs 4 mins ago	0xaf602888	SnglrtToken	0.001525323

Cuadro 1: Transacciones externas para convertir ETH a un Token, en este caso, estos son datos reales de la venta de tokens de SingularityNetToken.

Transacción	**Edad**	**Desde**	**Para**	**Cantidad [ETH]**
0xa4133901	3 mins ago	0xefa5e0ae	0x0956cb33	6910
0x830c993c	8 mins ago	0x291ca568	0xcea0e0dc	52718.94670433
0x1908cac0	10 mins ago	0xd74f65f5	0xedcc2f17	188.747
0x476ecbf1	57 mins ago	0x2b5634c4	0x846a8018	63.9
0x2dcb65d4	1 hr 18 mins ago	0x2b5634c4	0x72dfc730	9394.7
0xbbacc5e7	2 hrs 17 mins ago	0x2b5634c4	0xa8a15338	2643
0xaeeec7e5	2 hrs 22 mins ago	0x0e5e061a	0xb3b8dd57	24873.36330398
0x80cd8eb0	4 hrs 18 mins ago	0x2b5634c4	0xdfe7633e	338.8916
0x8c2ea564	5 hrs 2 mins ago	0x2b5634c4	0x5c49bbea	8969.515
0x620720da	7 hrs 34 mins ago	0xf751033d	0xa518c8ea	4000
0x2625663a	7 hrs 49 mins ago	0xe5fc4ddf	0x0ebe1c44	5174
0x49c931c7	8 hrs 2 mins ago	0xb2363b4f	0xe5fc4ddf	5174
0xba18db70	8 hrs 26 mins ago	0x2b5634c4	0x0181a709	199998
0xbb504831	9 hrs 6 mins ago	0x40d035a2	0x58d9d673	250
0xa5e3a311	9 hrs 6 mins ago	0x2b5634c4	0x8952afa3	23088.886
0x68acb872	9 hrs 12 mins ago	0x2b5634c4	0x496fd957	2998
0xb308207e	9 hrs 15 mins ago	0x2b5634c4	0x5f0dce24	501.3247
0x0be5515d	9 hrs 21 mins ago	0x2b5634c4	0x537188ce	2056
0xf449c2bb	9 hrs 26 mins ago	0x2b5634c4	0xfac4c874	1637.0222
0xf13743ac	9 hrs 33 mins ago	0x2b5634c4	0xb918a13d	4419.4485
0xab41f13f	9 hrs 44 mins ago	0x2b5634c4	0x03c8060e	473.436
0xe0b71230	9 hrs 47 mins ago	0x2b5634c4	0x03c8060e	153
0x92970e96	9 hrs 49 mins ago	0x2b5634c4	0xd45f9e97	145
0x7f5ee1e9	9 hrs 52 mins ago	0xa4ffec21	0x29a51483	241902.20115778
0xc8c7243f	10 hrs 38 mins ago	0x75a7b8a7	0xd79ed884	2104.48
0xe3b8de7c	11 hrs 1 min ago	0xaf602888	0x0980e662	17
0xade7cb9b	11 hrs 2 mins ago	0xaf602888	0x0980e662	17.5
0x85c45708	11 hrs 35 mins ago	0x2a0c0dbe	0x9d902494	149.85574335
0x959647dd	11 hrs 40 mins ago	0xdb8d5dab	0x6afa128c	36554.584962
0x4c0faa4a	12 hrs 35 mins ago	0x51146e9e	0x062263af	10302.3425
0xe0b4561d	12 hrs 48 mins ago	0x2b5634c4	0x0b1a8cfa	3

Cuadro 2: Ejemplo de transacciones de un token, conjunto interno a una sub-moneda o sub-divisa.

5.2. Metodología RI5C: Un navegador interactivo para la evaluación de una cadena de bloques

El resultado final y conclusión de él objetivo principal de esta investigación, es una metodología original para la evaluación de una cadena bloques, por limitantes prácticas, enfocado en contratos inteligentes de la red de Ethereum. La metodología RI5C: que por sus siglas en inglés significa *Risk InspeCtor* o en español inspector de riesgo. El software se encuentra disponible en `www.github.com/ebarojas/RI5C`, con una documentación técnica detallada y bajo una licencia de código abierto Apache 2.0, de tal modo que sea una contribución a la sociedad. El código fuente de las funciones básicas se puede ver en Apéndice B.

La implementación de la metodología consiste en tres etapas, que representan componentes de la arquitectura básica del software:

1. **Adquisición de datos,** en donde se deben adquirir los datos relacionados al contrato inteligente. Los datos se adquieren a través de una integración con Google BigQuery, en donde filtramos la cadena de bloques entera de Ethereum por transacciones internas de un contrato inteligente en particular.

2. **Generación y definición de un grafo,** de acuerdo a parámetros definidos previamente, RI5C debe de generar una red con los datos obtenidos. La red se genera con dos elementos básicos: nodos y aristas, en donde los nodos son representaciones de direcciones o cuentas y las aristas representaciones de transacciones individuales.

3. **Etapa de graficación,** en esta etapa se asignan características visuales a los nodos y aristas de la red. Se utiliza un algoritmo de comunidades de Louvain para ubicar grupos o clusters de nodos, las comunidades se identifican y separan por color. Se asigna un diámetro proporcional al volumen total transferido en el periodo analizado y se representan las aristas como flechas, en donde la dirección de la flecha refleja el flujo de la transacción y el ancho de la arista el valor de la transacción. Es decir, se genera una red pesada. Adicionalmente, se anexa información adicional que pudiera ser de utilidad, como registros de las cuentas y transacciones en navegadores de la cadena de bloques no visuales, tales como Etherscan.

Para lograr estos objetivos de un modo sistemático y hacer una contribución significativa, se ha creado un software de fuente abierta, con licencia Apache 2.0 [15]. Este software tiene como objetivo proveer una plataforma que permita evaluar un sistema de criptodivisas por personal sin antecedentes técnicos, entregando una plataforma de fácil uso para la continuación de las futuras líneas de investigación.

El software se encuentra en el repositorio https://github.com/ebarojas/ri5c. Se ha escogido tener un software publicado en Github ya que se puede descargar por cualquier interesado, gestionar contribuciones de terceros y generar una base de conocimiento pública, accesible y que ayude a su replicabilidad de los resultados y futuras validaciones.

5.2.1. Componentes de Diseño

El software RI5C fuente cuenta con los siguientes componentes fundamentales de diseño, con el objetivo de poderse implementar ágilmente y poder validar las hipótesis de modo contundente y permanecer como un activo valioso para la comunidad:

1. **Componentes primarios:**

   - **Adquisición de datos** – Uno de los principales retos para el entendimiento está en la adquisición y estandarización de datos. Después de mucha investigación, el método más accesible para la adquisición de datos resultó ser Google Big Query.[16]
   - **Compartimentalización** – El código fuente ha sido implementado con una instancia customizada de máquina virtual a través de Vagrant, y se han diseñado una serie de APIs para cada etapa de la metodología, con el objetivo de maximizar colaboración y utilidad.
   - **Lógica de negocio**– Una instancia de NetworkX llevará la carga principal de modelar el grafo, generar una red de conexiones y graficar resultados de manera expedita.

[15] La licencia Apache permite explotación comercial.

[16] Google Big Query a su vez, está basado en otro proyecto open source, localizado aquí https://console.cloud.google.com/marketplace/details/bigquery-public-data/ethereum-blockchain

- **Interacción con el usuario** – El software presenta una interfaz de usuario intuitiva a través de una red interactiva dibujada por el software SigmaJS, esta interfaz se accede utilizando un servicio web.
- **Adquisición de datos detallados y externos a la cadena de bloques** – La data disponible en la cadena de bloques de Ethereum siempre es semi-anónima y no contiene información de relevancia comercial y operativa, además RI5C utiliza el mínimo de datos para maximizar la eficiencia de su servidor. Para complementar su interacción, RI5C está integrado con los servicios de un navegador de Ethereum llamado Etherscan,[17] de tal modo que se pueda triangular con algo de información externa a la cadena de bloques, ya que Etherscan guarda etiquetas[18] para carteras y transacciones de interés.

2. **Componentes secundarios:**

- **Exportación** – Sería deseable, más no necesario para la implementación final, que un usuario pudiera exportar estos datos estandarizados.
- **Estadísticas de uso** – Se utiliza una implementación de PostgreSQL para almacenar estadísticas de uso simples, tales como historial de búsquedas e historial de interacciones. Estas estadísticas se pueden acceder interactuando con las tablas de PostgreSQL directamente.
- **Servicio web** – Otra característica deseable más no necesaria, es que el código sea accesible como un servicio web desde un servidor remoto, por lo que, en la medida de lo posible, RI5C está diseñado e implementado para la fácil operación de un servidor que administre múltiples conexiones externas.

5.2.2. El servicio web de RI5C

El código de RI5C incluye un servidor web basado en Tornado e implementado con Python. Este servidor web tiene algunas funciones públicas y algunas funciones privadas,

[17] Disponible en `https://www.etherscan.com`, este navegador es mantenido por la Fundación de Ethereum.

[18] Estas etiquetas, cuya utilización es muy práctica son mantenida por la comunidad y contienen advertencias o nombres.

hacia octubre del 2019, RI5C tiene un servicio web local habilitado por Vagrant y tiene código de integración continua.

Servicios públicos

- **Búsqueda de contrato inteligente en Ethereum:** La funcionalidad primaria de RI5C, accesible al público desde la ruta principal del servidor, consiste en buscar un contrato inteligente utilizando su identificador. Una vez que RI5C recolecte los datos, el servidor utiliza una librería propietaria para el tratamiento de datos y la generación del grafo y subsecuentemente la red, el objeto final es servido como HTML para que el usuario pueda interactuar con él utilizando su navegador. Hay una limitante en la capacidad del servidor, por lo cual sólo se consideran queries de entre 3,000 y 6,000 transacciones.
- **Exportación de grafos:** Adicionalmente, los datos visualizados en el servicio de búsqueda de contrato inteligente, se pueden exportar en formato nativo para tratarse posteriormente.

Servicios privados

- **API privada de adquisición de datos:** Los servicios de búsqueda por contrato inteligente, generación del grafo y graficación utilizando SigmaJS pueden ser accedidos internamente utilizando la API privada documentada en el repositorio principal. Está dentro de la planeación a corto plazo que estos servicios puedan convertirse en una API pública bajo el estándar REST.

5.2.3. Marco Tecnológico

Mientras que el software de la cadena de bloques de Ethereum tiene una API de fácil acceso para un conjunto de funciones muy utilizadas (revisar el estatus de una transacción, revisar el balance de una cuenta, etc), hay muchos datos que no son fácilmente accesibles, entre ellos los datos necesarios para el estudio de las transacciones internas de un contrato inteligente.

El software RI5C es concretamente una herramienta para la visualización de estos datos y tiene una utilidad significativa para la toma de decisiones técnicas, como priorización

de objetivos en el software subyacente (i.e., Ethereum y el contrato inteligente) pero también para decisiones financieras, tales como la evaluación de un portafolio de inversión o la auditoría de uno existente.

La información en el sistema actual es pública pero no fácilmente accesible. Aunque la cadena de bloques tiene algunas herramientas para su navegación, la cantidad de información es tal que muy difícilmente se puede utilizar productivamente sin un software de apoyo. En concreto, el software RI5C propone una metodología original para la evaluación de contratos inteligentes que se puede ver como un software para navegación de la cadena de datos.

5.3. Posibles usos acotados de RI5C

Para ilustrar mejor la funcionalidad del software, se ha preparado una lista enunciativa más no limitativa de los usos potenciales enfocados en profundizar el entendimiento de sistemas de criptodivisas.

- Evaluación de la estructura de transacciones de un contrato inteligente, en donde utilizando el software de RI5C se podrá obtener una medida cualitativa de qué tan activa es la red.
- Monitoreo de la emisión de criptodivisas, en donde durante el transcurso de un evento de generación de criptodivisas se puede hacer un análisis de las transacciones existentes y distribución.
- Ayuda complementaria para la evaluación de los parámetros de operación y de diseño de un sistema de criptodivisas. En donde la visualización e interacción con la red obtenida a través de RI5C pueden ayudar a evaluar cualitativamente el sistema y validar la hipótesis de una inversión.
- Auditoría de un sistema de criptodivisas o una cadena de bloques. El software proporciona una herramienta para una inspección rápida visual, que se puede convertir en una auditoría detallada.

- El software es una herramienta potente para la investigación académica, permitiendo a un estudiante analizar muestras de una cadena de bloques y descargar los datos para mayor análisis.

6. Validación de Metodología: Hallazgos

6.1. Algunos hallazgos anotados

La evaluación de sistemas de criptodivisas es difícil sin herramientas de soporte. La tecnología es nueva y los emprendedores en el sector muestran habilidades y capacidad amplias, sin embargo, las mejores prácticas apenas están por ser definidas e implementadas.

Aún después de escándalos como el de MtGox, la industria de casas de cambio parece tener un antecedentes preocupantes. Científicos como Tyler Moore y Nicolas Chrisin encontraron que unas 40 casas de cambio se establecieron en tres años y de esas, 18 cerraron, muchas llevándose fondos de sus consumidores con ellas. Es aparente que la tecnología no está en su etapa de madurez, por momentos parece haber un grupo de principiantes a cargo, a veces aparentemente criminales. En el análisis de Beecroft (2015) se muestra que en algunos casos, el origen de las debilidades es tecnológico, representando un riesgo operativo alto. Se requieren herramientas urgentemente para ayudar al entendimiento de estas tecnologías y avanzar el estado del arte.

RI5C genera redes agrupadas por comunidades utilizando el algoritmo de modularidad de Louvain, las comunidades se separan e identifican con colores, los nodos y las aristas son pesadas. A continuación se muestran algunos casos de interés académico, financiero, legal y regulatorio:

6.1.1. Leyendo un sistema financiero ERC-20

Como un ejemplo práctico se presenta una lectura del contrato inteligente de Tether, una criptodivisa que tiene equivalencia al Dólar americano. Tether se conforma al estándar de contratos inteligentes financieros ERC-20 y está diseñada para moverse entre casas de cambio situadas en diferentes países sin necesidad de pasar por el sistema bancario tradicional. De

tal modo que un usuario que está intercambiando divisas en una casa de cambio en Eslovenia (como Bitstamp) pueda liquidar su posición en alguna criptodivisa y mover sus fondos a una casa de cambio americana, donde pudiera hacer un retiro a una cuenta de banco. En este ejercicio, analizaremos una red altamente conectada entre si, con muchos jugadores grandes.

- Nombre: Tether
- Dirección del contrato: 0xdac17f958d2ee523a2206206994597c13d831ec7
- Número de transacciones: 4,000
- Número de nodos: 2499
- Número de aristas: 3263
- Grado promedio: 2.6114445778311324
- Densidad promedio: 0.001045414162462423

Inmediatamente, en la Figura 16 vemos que la red tiene una alta densidad de información, un red jerárquica y libre de escala, con una estructura de comunidades traslapadas marcada. Con información de terceros (no disponible en la cadena de bloques, pero accesible desde RI5C) podemos identificar los clusters más importantes: casas de cambio. Vemos tres nodos de Huobi, una casa de cambio China, Bitfinex, una casa de cambio registrada en la islas vírgenes pero originalmente de Hong Kong, vemos Gate.io, una casa de cambio Koreana y OKEX, otra casa de cambio situada en Hong Kong. Los nodos alrededor de los clusters, son usuarios que están haciendo depósitos o retiros a las casas de cambio.

Con mayor detalle, vemos en la Figura 17 un acercamiento al cluster de la casa de cambio Gate.io. El software de RI5C escoge un color homogéneo para los nodos que está relacionados con este grupo y podemos identificarlos visualmente sin mucha dificultad. Vemos dos dinámicas importantes: primero, que los nodos que tienen un color diferente al del cluster están conectados a otros clusters y segundo vemos una transacción enorme consolidada en la parte superior, esta transacción va a una cuenta *fría*, es decir, el equivalente una bóveda segura que protege los fondos de ataques a los servidores *calientes* que están conectados a

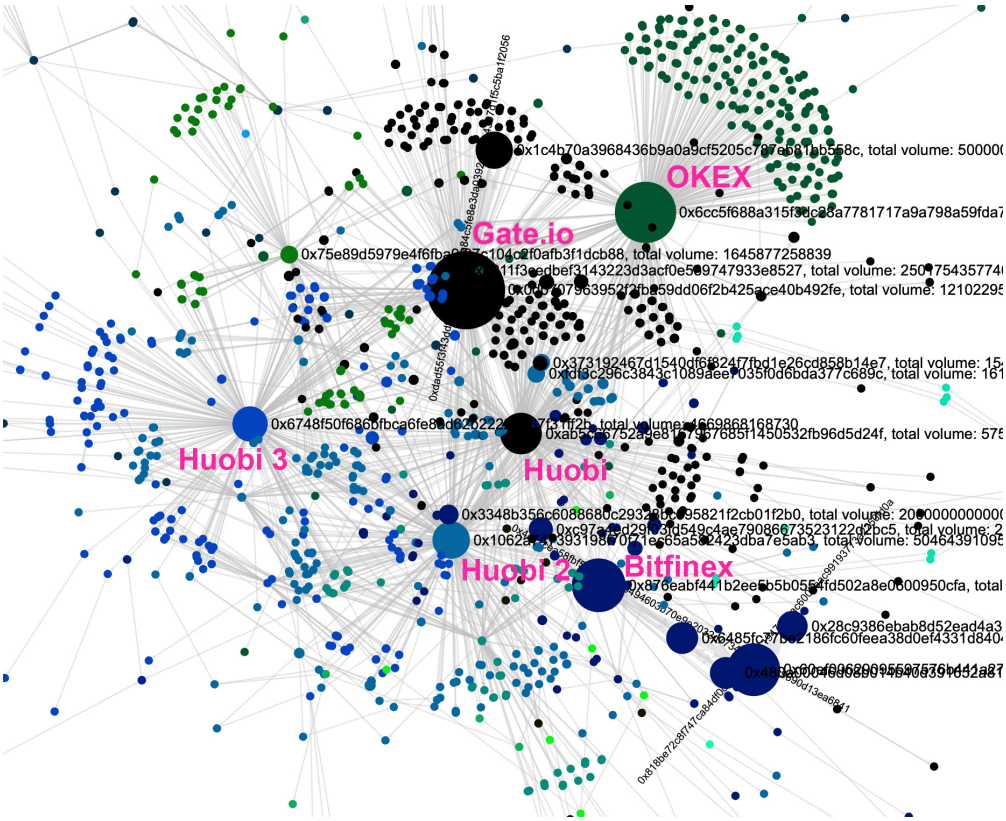


Figura 16: Red de transacciones de contrato inteligente de Tether. Fuente: RI5C, mayo 2019.

internet.

Un acercamiento con aún más detalle en la Figura 18 muestra un sub-conjunto de transacciones y nodos que se encuentran entre los clusters de Huobi y Gate.io. Estos nodos representan cuentas o carteras que han retirado fondos de ambas casas de cambio, muy probablemente alguna casa de cambio o usuario experimentado.

Por último, viendo el resto de la red, encontramos una comunidad aislada, una anomalía alejada del resto de los clusters y sin ninguna conexión. Vemos una comunidad de transacciones pequeñas y homogéneas sin ninguna conexión al exterior. Este cluster puede representar la creación o destrucción de Tethers, sin embargo, a simple vista no podemos estar seguros.

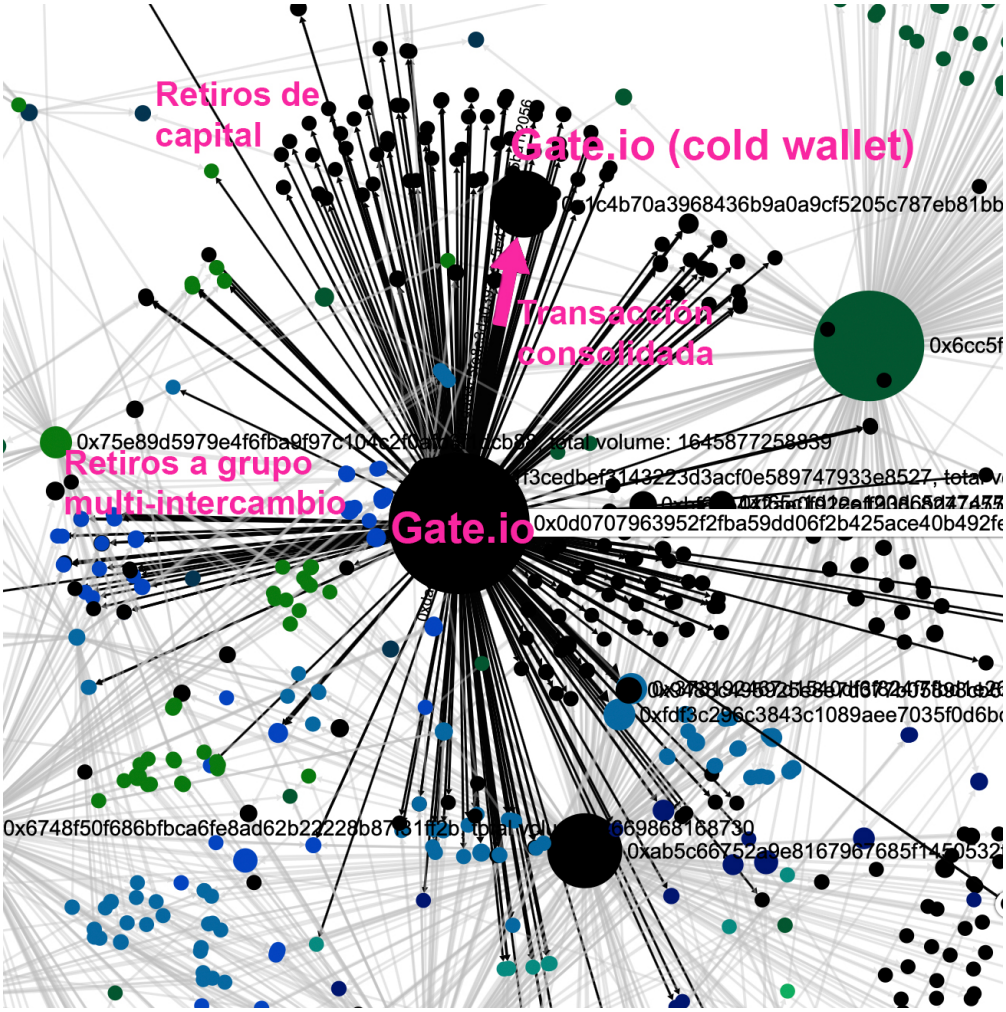


Figura 17: Acercamiento a transacciones de Gate.io dentro de sistema de transacciones de contrato inteligente de Tether. Fuente: RI5C, mayo 2019.

Utilizando RI5C, con una simple inspección visual queda claro que existe una anomalía, y que la comunidad está aislada.

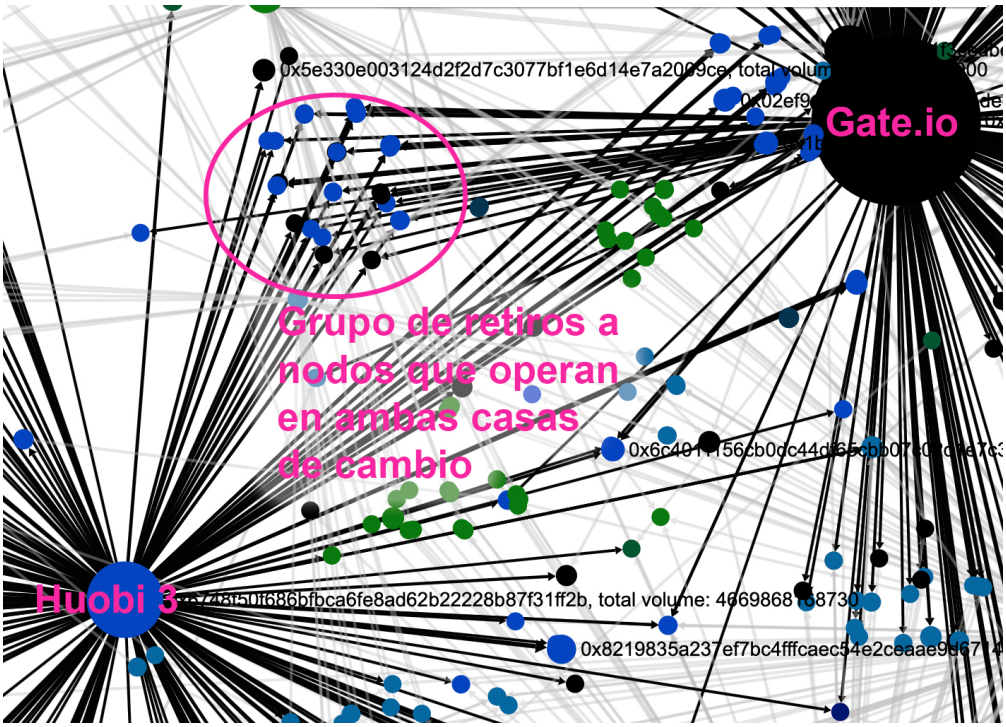


Figura 18: Acercamiento a transacciones de Gate.io y Huobi 3 dentro de sistema de transacciones de contrato inteligente de Tether, mostrando retiros a nodos en común. Fuente: RI5C, mayo 2019.

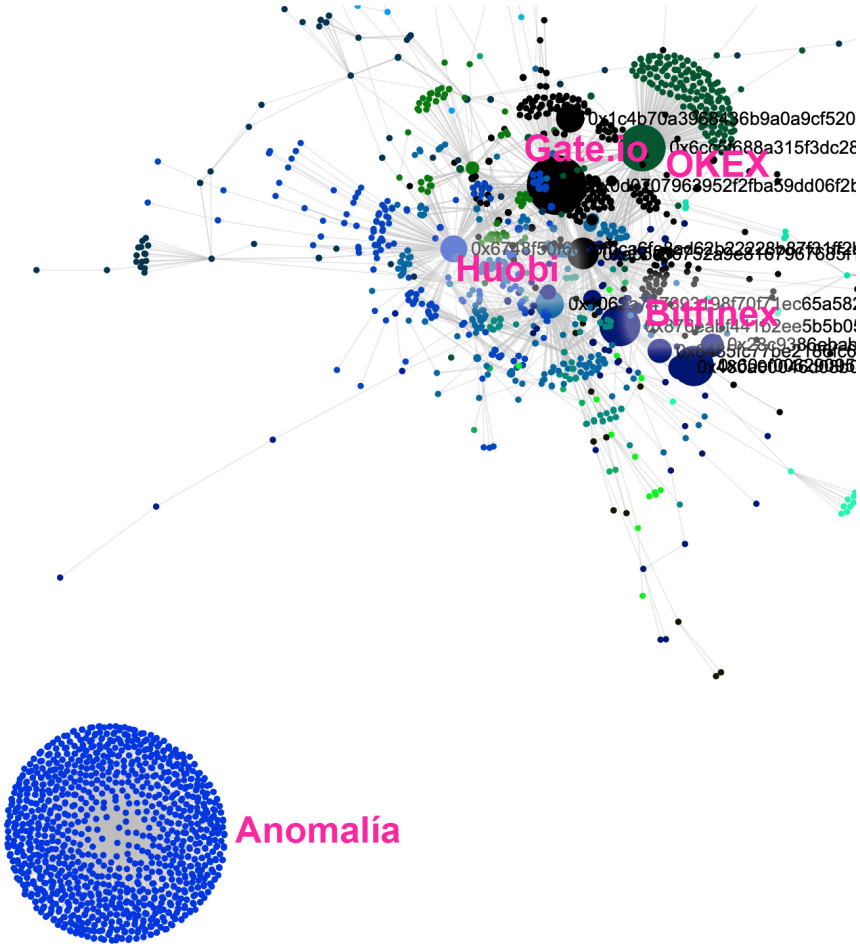


Figura 19: Acercamiento a cluster de transacciones de dentro de sistema de transacciones de contrato inteligente de Tether, mostrando un conjunto separado de el resto de la red. Fuente: RI5C, mayo 2019.

6.1.2. Ejemplo de Contrato Inteligente no-Financiero ERC-721

La red de Cryptokitties es un buen ejemplo de una red sana, y una cuantificación simple de transacciones posiciona este contrato como uno de los más utilizados. El activo digital de Cryptokitties *no* es un activo financiero, de hecho, de acuerdo a la clasificación FINMA es un token utilitario, que técnicamente cumple con la especificación de ERC-721 para tokens no-fungibles, es decir, activos digitales únicos que no se pueden mezclar entre si.

Cryptokitties se entiende como un juego de artículos coleccionables en la cadena de bloques, sin embargo los colecccionables son activos digitales, *criptogatitos* si se traduce del inglés directo al español. Los usuarios de la red puede comprar los coleccionables directamente de ellos o a través de una serie de casas de subastas, y una vez que tienen los activos, los pueden *cruzar* con otros dueños para obtener nuevos activos provenientes de un *padre* y *madre* únicos. Para buscar parejas, pueden dejar a sus activos en consignación en una casa de subastas especial.

Análisis dibujado con Maplotlib: El primer análisis que se hizo de la red de Cryptokitties fue con una versión preliminar de RI5C que sólo generaba dibujos de redes no pesadas y no direccionadas. La Figura 20 es el resultado del primer esfuerzo. Como se puede ver, es fácil identificar los clusters, sin embargo hay poca información acerca del flujo de las transacciones y no es fácil buscar información de terceras partes para entender mejor cómo se utiliza la red.

- Nombre: CryptoKitties
- Dirección del contrato: 0x06012c8cf97bead5deae237070f9587f8e7a266d
- Límite de Transacciones: 3,000
- Número de nodos: 1625
- Número de aristas: 1936
- Grado promedio: 2.3828

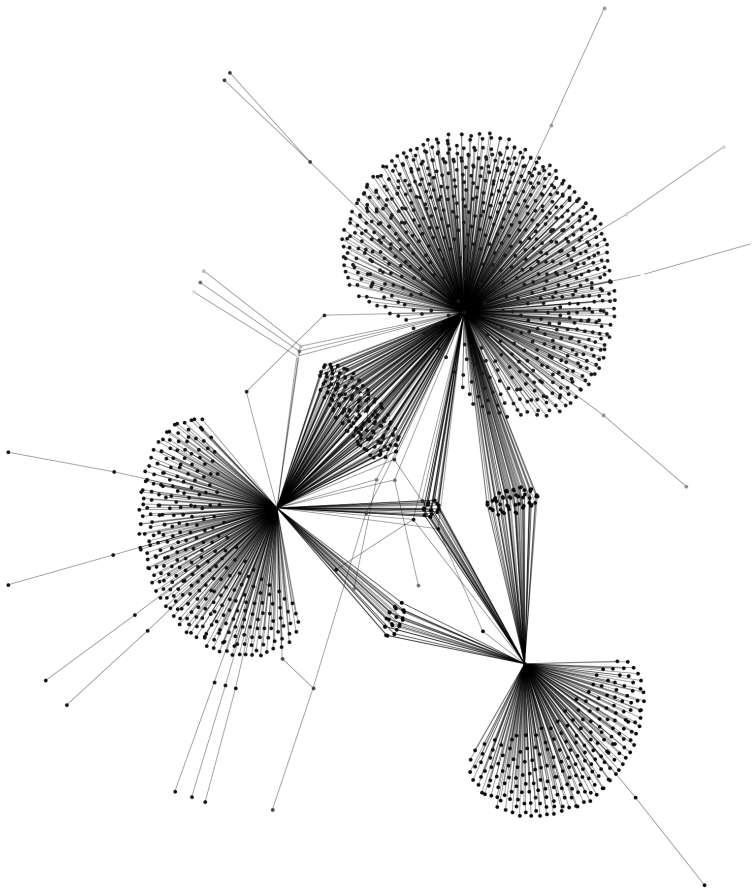


Figura 20: Red de transacciones de contrato inteligente de CryptoKitties. Fuente, Generación propia con software RI5C en marzo 2019.

Análisis con RI5C actualizado: Un análisis con el software final de RI5C, que permite accesar información contextual de fuentes externa a la cadena de bloques, como lo es el navegador de Etherscan permitió identificar fácilmente los diferentes clusters como se puede ver en la Figura 21.

- Nombre: CryptoKitties

- Dirección del contrato: 0x06012c8cf97bead5deae237070f9587f8e7a266d
- Límite de Transacciones: 4,000
- Número de nodos: 178
- Número de aristas: 234
- Grado promedio: 2.6292134831460676
- Densidad promedio: 0.014854313464102075

Es importante ver que a través de RI5C podemos ver cómo los usuarios interactúan con diferentes clusters, tales como el contrato génesis, que muestra los eventos de generación accionados por algún administrador de la red, las ventas directas a través de subastas y la subasta para interacciones, donde los usuarios dejan en consignación sus Cryptokitties para buscar una pareja y acceder a la funcionalidad de cruzarse con otro Cryptokittie. Con un poco más detalle, logramos identificar una casa de subastas secundaria llamada Auctioncity, como lo muestra la Figura 22. Este es un buen ejemplo, de cómo se puede utilizar RI5C para validar que un sistema de criptodivisas se esté utilizando de acuerdo a sus parámetros de diseño.

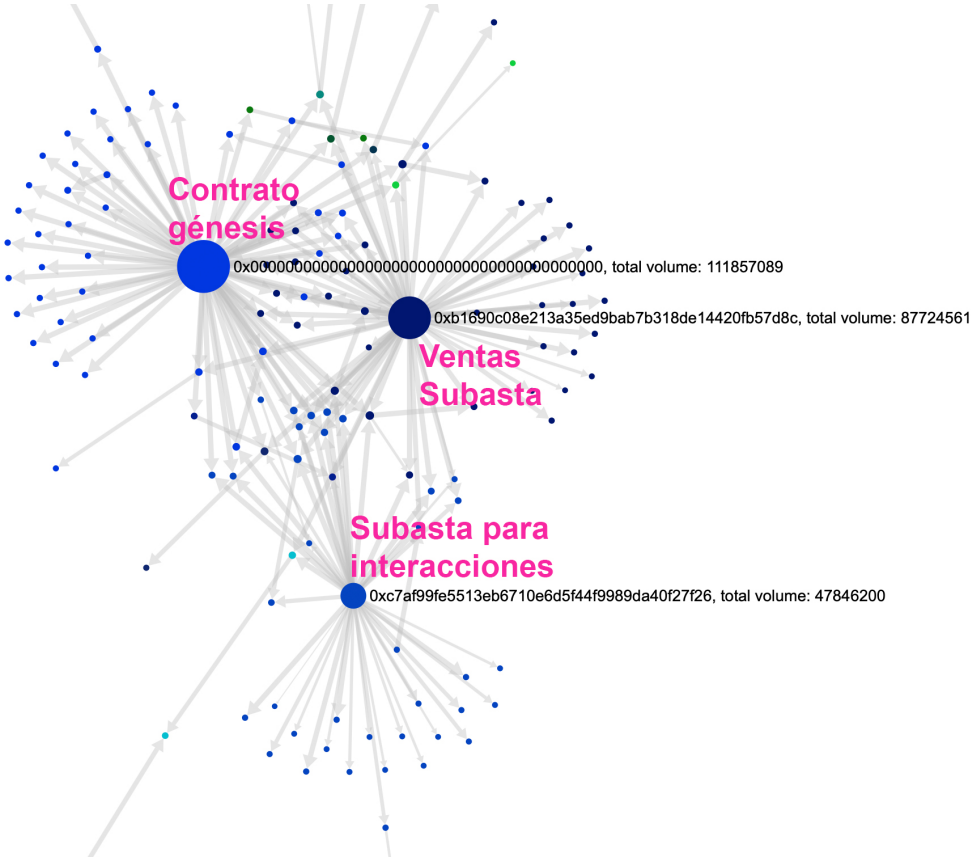


Figura 21: Red de transacciones de contrato inteligente de CryptoKitties. Fuente: RI5C en marzo 2019.

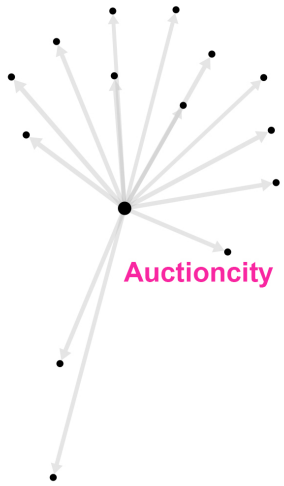


Figura 22: Acercamiento a cluster de transacciones aislado de CryptoKitties, identificado como el mercado secundario *Auctioncity*. Fuente: RI5C, mayo 2019.

6.1.3. Análisis Forense de Anomalía Cryptopia en 2019

A lo largo de enero y febrero de 2019 la casa de cambio Neozelandesa Cryptopia fue víctima de una serie de ataques. En su momento, las pérdidas se estimaron en alrededor de 16 millones de dólares, a precios de mercado contemporáneos al ataque. Los ladrones o *hackers* se llevaron Ethereum y varias otras criptodivisas. Este ataque fue particular en tanto que Cryptopia perdió acceso a más de 76,000 cuentas de Ethereum y criptodivisas. Para efectos de entender un poco cómo funcionó el ataque, nos enfocamos en el periodo específico del ataque, analizando el contrato inteligente de Dentacoin, que fue parte del ataque: los hackers se llevaron casi 2.5 millones de dólares en Dentacoin. Galka (2019)

Para este análisis, se modificó el query estándar de RI5C y se limitaron los resultados a un momento en específico cuando se sabía que había sucedido el robo. Las condiciones fueron las siguientes:

- Nombre: Dentacoin
- Dirección del contrato: 0x08d32b0da63e2C3bcF8019c9c5d849d7a9d791e6
- Límite de Transacciones: 4,000 (no se llegó al límite)
- Número de nodos: 268
- Número de aristas: 274
- Grado promedio: 2.044776119402985
- Densidad promedio: 0.007658337525853876
- Ventana de tiempo: Entre las 5:00 hrs del 28 de febrero de 2019 y las 23:00 hrs del 28 de febrero de 2019.

En la Figura 23 vemos la estructura de la red de Dentacoin durante las 18 horas de la ventana de tiempo que se está analizando. En esa ventana de tiempo vemos transacciones en tres casas de cambio fundamentales: Ether Delta, Hit BTC y CoinExchange, además de un cluster que presenta ordenamiento de casa de cambio pero no logramos identificar. La casa de cambio Cryptopia brilla por su ausencia, pues en estos días había cerrado operaciones.

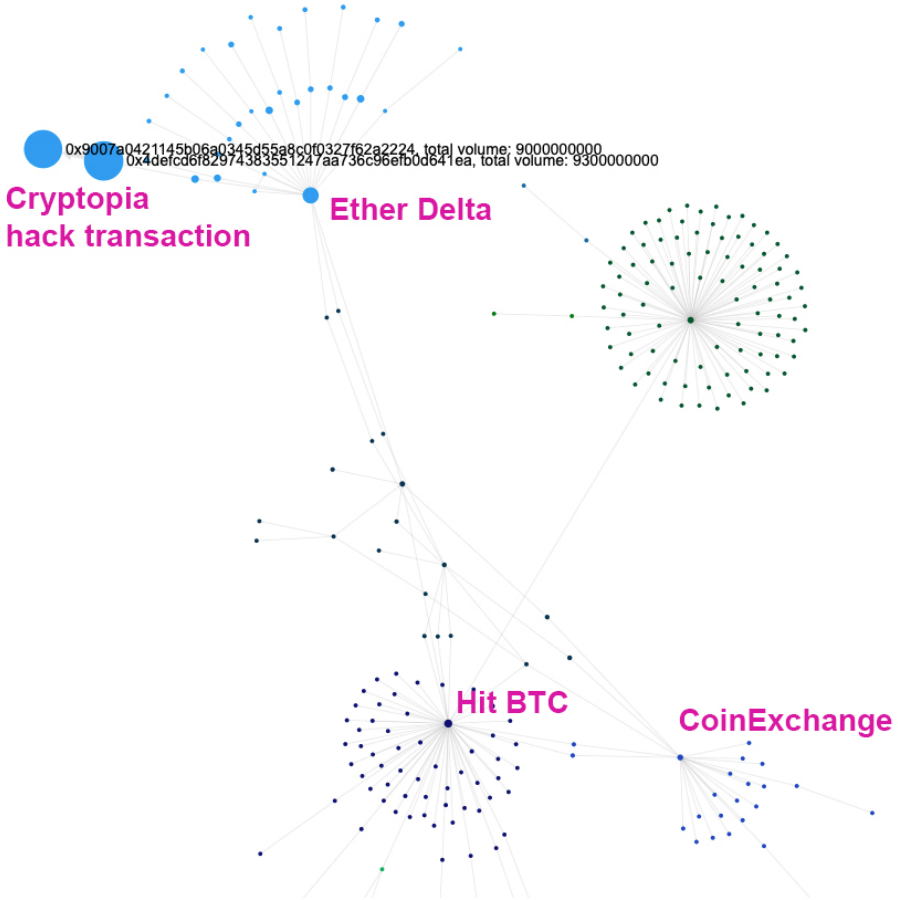


Figura 23: Red de transacciones de contrato Dentacoin entre el 28 de febrero 2019 y el 1 de marzo del 2019. Fuente: RI5C, mayo 2019.

Viendo los volúmenes relativos, hay una anomalía notoria en la esquina superior izquierda, que analizamos a detalle en la Figura 24.

En la Figura 24 podemos rastrear el origen de los fondos a EtherDelta, evidencia que el Hacker liquidó una posición de Dentacoin con un valor equivalente de alrededor de 388,297.80 USD en esa transacción. En la Figura 25 podemos ver las etiquetas que Etherscan agrega a la

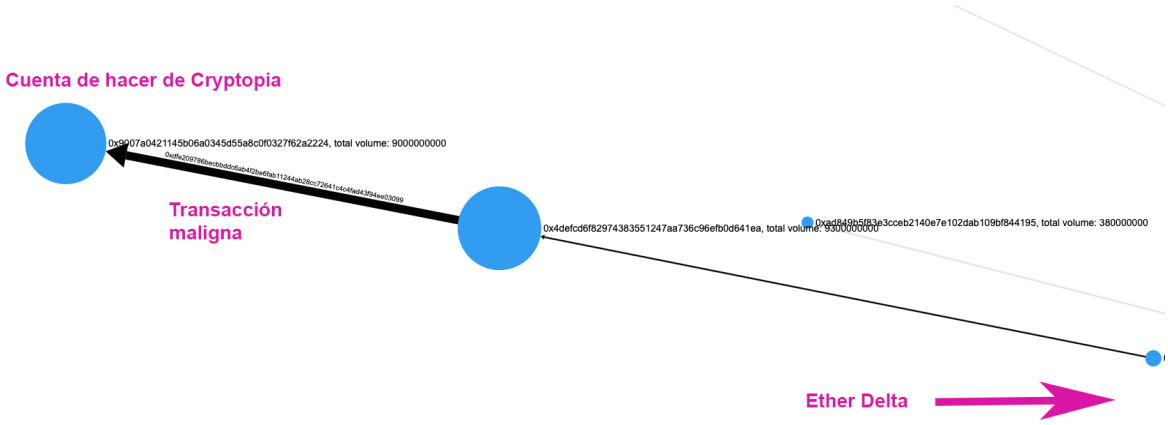


Figura 24: Acercamiento a transacción luego del robo de Cryptopia en la red de transacciones de contrato Dentacoin entre el 28 de febrero 2019 y el 1 de marzo del 2019. Fuente: RI5C, mayo 2019.

transacción. La transacción proviene de Etherdelta, una casa de cambio descentralizada que opera a través de un contrato inteligente y por ende no tiene ningún control de anti-lavado de dinero. Muy posiblemente esta transacción haya sido parte de un esfuerzo de ocultar el origen de fondos relacionados al ataque.

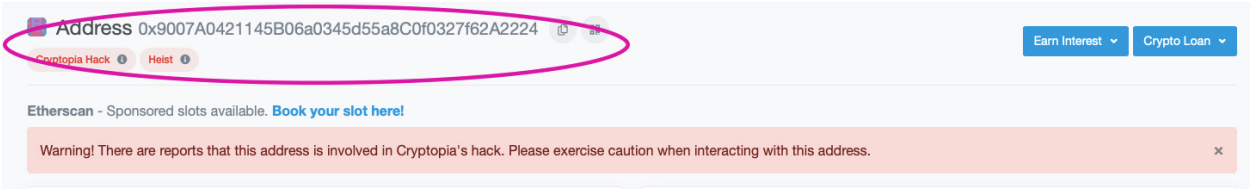


Figura 25: Mensaje en Etherscan identificando cuenta relacionada con robo de Cryptopia. Fuente: Etherscan, mayo 2019.

6.2. Resumen de Topologías en Sistemas de Criptodivisas

En el interés de ayudar a identificar los patrones más comunes y agilizar la lectura utilizando la herramienta de RI5C, hemos descrito algunos patrones con algunas características, utilizando el lenguaje de análisis de redes.

6.2.1. Red Libre de Escala

Todas los sistemas de criptodivisas activos, se describen como una red libre de escala, con una estructura de comunidades traslapadas e interconectadas entre si, y algunas comunidades aisladas, un ejemplo visual en la Figura 26.

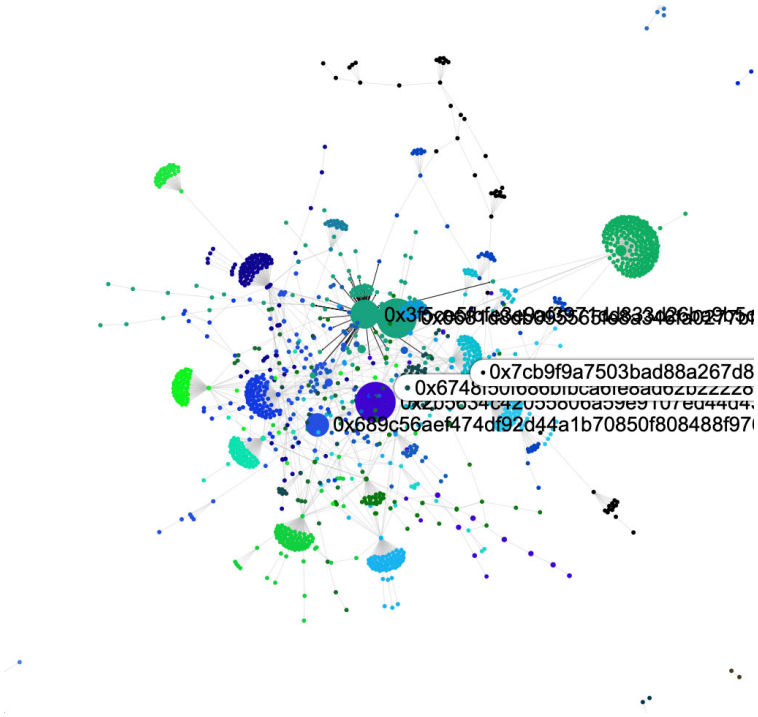


Figura 26: Visualización de la red-interconectada del contrato inteligente de Tether en RI5C. Fuente: RI5C, octubre 2019.

6.2.2. Transacciones Aisladas

Debido a limitantes en la adquisición y procesamiento de datos, existe un número finito de transacciones que se pueden procesar en un mismo momento y no todas se visualizan como parte de las comunidades principales. En estricto sentido, algunas pueden ser conjuntos de transacciones realmente aisladas, como divisas que aún no están en circulación, sin embargo en la mayoría de los casos, estas transacciones aisladas están conectadas con la estructura de comunidades en un punto en la historia fuera de los datos recabados por RI5C. Las

comunidades aisladas se distinguen por ser nodos y transacciones aparentemente sin aristas a las comunidades principales, como se ven en la Figura 27.

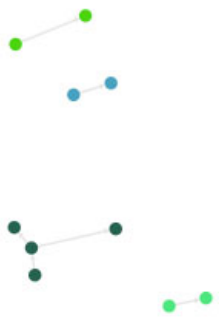


Figura 27: Visualización de transacciones aisladas del contrato inteligente de Tether en RI5C. Fuente: RI5C, octubre 2019.

6.2.3. Cluster

Dentro de la estructura de comunidades, el nodo concentrador, claramente identificado en la Figura 17 y 28, se identifica como un cluster y se define como un mismo nodo que tiene un número grande de aristas.

En los sistemas de criptodivisas, los clusters representan nodos que por diversas razones de diseño u emergentes, terminan siendo parte de la infraestructura básica de la red. Algunos ejemplos de clusters:

- **Casa de cambio:** Naturalmente, las casas de cambio o de subasta, representan clusters al ser servicios que por definición son usados por un número importante de nodos.

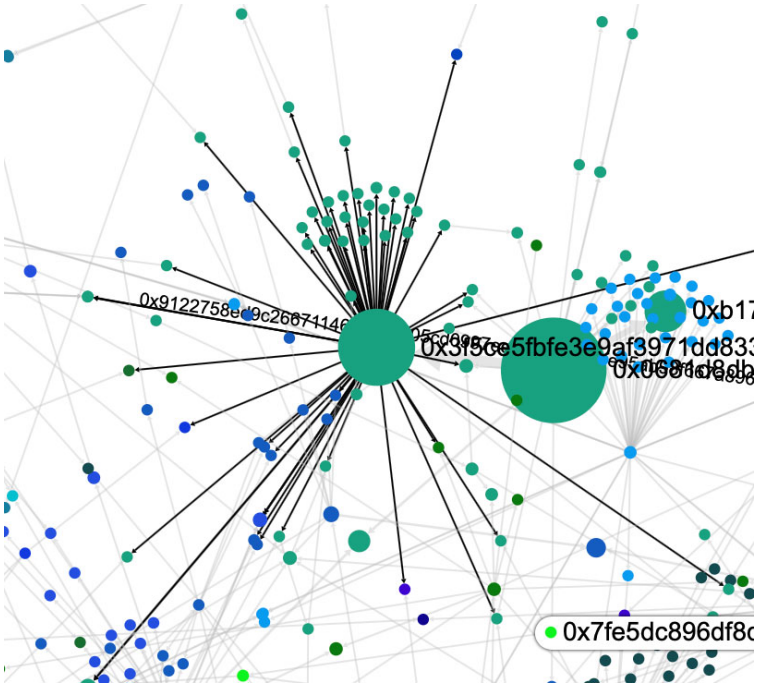


Figura 28: Un cluster en la visualización de RI5C del contrato inteligente de Tether. Fuente: RI5C, octubre 2019.

- **Contrato inteligente:** Algo muy semejante sucede con los contratos inteligentes, que también se representan como un cluster.
- **Servicios:** Un término más general que casa de cambio y contratos inteligentes, en general cualquier servicio público puede verso como un cluster. Ejemplos de servicios puede ser un negocio que recoja pagos en criptodivisas, una casa de subasta (como los vistos en los ejemplos de Cryptokitties).

Utilizando los servicios de información contextual *off-chain* de RI5C, se puede hacer investigación para entender cuál es la naturaleza del servicio, y para identificar clusters.

6.2.4. Super Cluster

Un super cluster se define como un nodo que concentra más del 51 % de las transacciones de una red. En estos casos, es claro que los servicios están concentrados y esto tiene

repercusiones significativas en la estructura de la red, ya que apunta a una concentración importante.

6.2.5. Comunidades Traslapadas

Cuando se presentan varios comunidades, es común que encontremos nodos que interactúan con varias de ellas, representan evidencia de que la red está funcionando como debe y hay usuarios que utilizan varios de los servicios.

6.2.6. Comunidades Aisladas

También es común que observemos mini-comunidades aisladas de la red principal. Estos clusters aislados pueden estar conectados a la red principal a través de transacciones más antiguas, y representan servicios más pequeños, o grupo cerras de personas que pueden estar intercambiando entre sí por diversas razones. Por ejemplo, un usuario que está vendiendo varias porciones de una criptodivisa en un sitio de subasta directa como LocalBitcoins, una tanda o quiniela informal, etc.

7. Conclusiones

La implementación del software de RI5C en algunos contratos inteligentes de la red de Ethereum apunta a las siguientes conclusiones:

1. La conclusión principal es que se puede evaluar un sistema de criptodivisas utilizando la metodología y herramienta de RI5C. Esta metodología, acompañada de la herramienta original RI5C avanza la ciencia de la administración en materia de criptodivisas para los siguientes actores:

    - **Investigador:** El mayor impacto para el investigador es sin duda el código fuente abierto de RI5C, que le permite validar y replicar las hipótesis presentadas en este trabajo, así como re-utilizar el código de manera completa o parcial para empujar la ciencia en nuevas direcciones. El investigador puede hacer uso de RI5C de tres modos fundamentales: a) puede utilizar el servicio web para hacer estudiar

la topología de un sistema existente; b) puede utilizar las funciones de RI5C para adquirir data y hacer el tratamiento final fuera de RI5C y finalmente; c) puede generar una versión mejorada de RI5C o utilizarlo como componente para herramientas más potentes.

- **Regulador, policía cibernética y autoridad fiscal:** Quizás uno de los jugadores cuyo beneficio sea más directo, es el regulador, a quien RI5C le presenta una herramienta práctica y útil para el entendimiento de estos sistemas, de cómo se están utilizando y del comportamiento de los usuarios de un sistema de criptodivisas: es decir, RI5C le representa una herramienta auxiliar potente para la evaluación de estos sistemas en el ámbito de administración pública.
- **Inversionista:** RI5C presenta una herramienta exploratoria útil para el inversionista privado o institucional, para quien tener un entendimiento de la estructura de comunidades, distribución, concentración de capital y actividad proveen información que puede ser útil para mitigar riesgos operativos y algunos riesgos de mercado. Tener un entendimiento del sistema y sus partes pueden validar una hipótesis de inversión. Por ejemplo, en la Sección 3.3.3 vimos el parámetro NVT, que relaciona el volumen de transacciones de la cadena de bloques como una medida de valoración del sistema; utilizando RI5C se puede analizar a detalle la estructura de estas transacciones y llegar a un entendimiento superior. Un ejemplo, ¿están sucediendo transacciones en una misma comunidad o entre comunidades? ¿en pocas transacciones o distribuídas uniformemente? Respuestas a estas preguntas, dejan ver información de alta utilidad.
- **Emprendedor:** Para el emprendedor, RI5C es una herramienta de investigación y de administración. De investigación ya que previo al diseño o a la implementación de un sistema de criptodivisas le puede ayudar a investigar el estado de la tecnología. Una vez implementado un sistema de criptodivisas o cadena de bloques, RI5C le da información valiosa para la correcta administración de su sistema. Para el emprendedor, la posibilidad de evaluar un sistema tercero o propio utilizando RI5C, es la clave para la correcta administración de diversos factores operativos y de riesgo en sus interacciones.

2. Sí se puede modelar un sistema de criptodivisas como una red de transacciones para complementar su entendimiento. La abstracción de transacciones como aristas y carteras como nodos para generar una red direccional pesada, así como el algoritmo para detectar comunidades y demás parámetros definidos en RI5C son adecuados para cumplir los objetivos planteados. Tal vez más importantemente, la suite de herramientas interactivas de RI5C, ha permitido identificar varias características de alto nivel de un sistema de criptodivisas y al mismo tiempo provee herramientas útiles para profundizar. Todo esto, se pudo validar con detalle en la Sección 6.1.1.

3. El uso de herramientas tecnológicas de visualización e interacción de datos masivos ayuda enormemente al entendimiento de un sistema complejo, como es el caso de un sistema de criptodivisas. La visualización, interacción, evaluación y entendimiento de un sistema de criptodivisas a través de RI5C, provee información valiosa para la evaluación del riesgo. En particular para gente no familiarizada con los componentes estructurales técnicos de un sistema de criptodivisas.

La metodología y herramienta original RI5C es de utilidad para evaluar un sistema de criptodivisas en diversos modos: a) es útil para evaluar comportamiento generalizado, como interacción con una casa de cambio, manipulación del mercado y/o un robo, b) es valioso para explicar cómo funciona un sistema de criptodivisas, c) puede ser utilizado para evaluar visualmente el uso de un sistema de criptodivisas. Es importante que debido a la naturaleza pública del código y del servicio, estos resultados son repetibles y verificables.

En conclusión, RI5C se muestra como una metodología adecuada para evaluar un sistema de criptodivisas, tan útil para una inspección visual rápida de un sistema, como para investigar a fondo detalles de interacciones y tendencias generales. RI5C es útil para evaluar riesgos operativos y de implementación, y para obtener información complementaria a riesgos de mercado, sin embargo varios riesgos permanecen externos al comportamiento de la cadena de bloques. Se puede utilizar para auditar el funcionamiento de un contrato inteligente, para validar la promesa de un director de comenzar a vender activos, para validar noticias de un ciber-crimen o estudiar un evento histórico, como un robo, cambios en las condiciones fundamentales de los sistemas o anomalías del mercado.

7.1. Siguientes Líneas de Investigación

Pese a su gran utilidad, RI5C está enfocado en contratos inteligentes, relativamente ligado a la arquitectura de Ethereum y tiene grandes oportunidades de mejora en la visualización.

7.1.1. Estudio y Validación con otras Criptodivisas y Cadenas de Bloques

Hace falta ampliar el uso de la herramienta para el análisis de cadenas de bloques diferentes a Ethereum, como lo son Bitcoin, Ripple, Tether y cualquier otra criptodivisa. Algunas de estas cadenas de bloques pudieran tener un comportamiento materialmente diferente a Ethereum.

7.1.2. Generación de Índice Útil para Cuantificar Evaluación del Riesgo

Las medidas de centralidad y densidad son útiles para entender la estructura del sistema de criptodivisas, sin embargo, no es suficiente obtenerlas para validar su utilidad. Es necesario buscar correlaciones y patrones contra el comportamiento externo como precio y volumen transaccional, para entender correctamente su utilidad. Estas medidas se podrían correlacionar a la volatilidad y podrían tener cualidades de valor para cuantificar estas características. En este rubro, se ha tratado de evaluar cualidades, como la decentralización utilizando el Coeficiente de Gini[19], utilizando el modelo de redes de RI5C se podrían evaluar características semejantes con mayor profundidad.

7.1.3. Interpretación y Búsqueda de Patrones

Tal vez la línea de investigación más importante es la aplicación de la metodología RI5C para la búsqueda de patrones correlacionados a precio y volumen de transacciones, así como a otros fenómenos que pudieren suceder fuera de la cadena de bloques. Se sugiere generar gráficos con cierto nivel de interactividad, utilizando alguna de las herramientas disponibles para generar gráficos con los cuales se pueda interactuar.

[19] En términos económicos, el coeficiente de Gini es una medida de la dispersión estadística diseñado para representar distribución de riqueza. Fue publicado por Corrado Gini en el artículo de 1912 *Variabilità e mutabilità*

7.1.4. Estudio de Variaciones a Través del Tiempo

Una de las posibles aplicaciones útiles de RI5C es utilizarlo para notar cambios en la estructura de una red, que pudieran proveer un mayor entendimiento de factores internos y externos al sistema. Una posibilidad interesante, sería ver el arreglo de nodos y aristas cambiar a través del tiempo, para ello habría que hacer una animación entre dos o más estados de los nodos. Para lograr exitosamente esto habría que cambiar la estructura de los datos y modificar extensamente el tratamiento y generación de una red. Sin embargo, las herramientas existentes y métodos de adquisición y limpieza de datos serían aplicables directamente.

7.1.5. Modelos Predictivos con Inteligencia Artificial

Utilizando los datos obtenidos a través de RI5C, sería de alto interés para la evaluación de estos sistemas que se pudiera hacer un modelo predictivo para la estructura de la red basado en inteligencia artificial. Es viable que la posibilidad de predecir la estructura futura de una red pudiera llevarnos a predecir su volatilidad.

Apéndices

A. Glosario de términos y nombres

- API: del inglés *Application Program Interface*, una API es la interfaz de programación de aplicaciones, un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

- Activo digital: un instrumento financiero intercambiable. Se refiere a cualquier forma de instrumento financiero, cuya definición legal específica puede variar de acuerdo a la jurisdicción. Algunos tokens se consideran activo digitales.

- Bitcoin: la primer criptodivisa, desarrollada en 2008 basada en el documento escrito por Satoshi Nakamoto Nakamoto (2008). Bitcoin introdujo el concepto de Blockchain (Cadena de Bloques) como un registro descentralizado con un algoritmo de consenso utilizado para validar sus transacciones. En esta investigación,se utiliza la palabra *Bitcoin*, capitalizada, para referirnos al sistema y la propia red, e.g., "El sistema de Bitcoin ha resistido varios ataques" y utilizamos la palabra *bitcoin*, sin capitalizar, para referirnos a la unidad de cuenta, e.g., "Alicia le ha enviado un par de bitcoins a Bob".

- Capital de Riesgo: el capital riesgo o capital emprendedor es una nomenclatura financiera para denominar capital financiero aplicado a empresas startup con elevado potencial y riesgo en fase de crecimiento.

- Compañía Holding: un holding, también conocida como sociedad tenedora o simplemente tenedora, es una sociedad comercial cuya principal o única función es la de tener o administrar la propiedad de otras sociedades o compañías.

- Ecosistema de startups: el conjunto de empresas, inversionistas, emprendedores, entidades regulatorias, bancarias y comerciales que influyen e interactúan en el ciclo de vida de una startup.

- Empresa Gacela: una empresa que crece rápidamente, no está correlacionada con el ecosistema de inversión de riesgo ni con el mercado de fusiones y adquisiciones tradicionales de una startup.
- Friends, Fools and Family (FFF): el nombre coloquial para tontos, amigos y familia, la primera y más común opción de fondeo para muchas startups.
- ICO: del inglés *Initial Coin Offering*, se refiere a la colocación primaria de tokens en el mercado. Normalmente, un evento de generación de tokens para el levantamiento de capital Sehra (2017). Parecido al modelo de fondeo comunitario Bolt (2016), pero ligado a un token que se puede intercambiar fácilmente en mercados de compra y venta Ametrano (2017). Terminología usada a finales de 2017 y principios del 2018, normalmente se buscaba una aplicación utilitaria para evitar regulación de la SEC.
- Key Performance Indicator (KPI): un indicador estratégico diseñado para medir el desempeño de alguna cualidad de interés.
- Ronda de capital semilla: una oferta para inversionistas, normalmente a través de seguridades, notas convertibles o capital para obtener una posición de capital. El término seed proviene de *semilla* en inglés y se refiere a la etapa de la compañía.
- STO: del inglés *Security Token Offering*, evento semejante a un ICO, pero con tokens que explícitamente representan un activo.
- Silicon Valley (SV): es el nombre que recibe la zona sur del área de la Bahía de San Francisco, en el norte de California, Estados Unidos. Aloja muchas de las mayores corporaciones de tecnología del mundo y miles de pequeñas empresas en formación (startups). Originalmente la denominación se relacionaba con el gran número de innovadores y fabricantes de chips de silicio fabricados allí.
- Startup: una empresa con tres características importantes: ambición, producto escalable y crecimiento rápido. Se diferencia de una PyME (Pequeñas y Medianas Empresas) o MiPyME (Micro, Pequeñas y Medianas Empresas) por su enfoque en crecimiento rápido y por ofrecer un producto disruptivo o innovador. Las startups son MiPyMEs, pero no todas las MiPyMES son startups.

- Token: en el contexto de una ICO, un token Foundation (2017) es la llave de acceso a una funcionalidad de una cadena de bloques, muy parecido a las llaves de acceso de una API. En algunos casos, se puede considerar como un instrumento financiero.
- Unicornio: una empresa, que haya empezado como startup, valuada en más de mil millones de Dólares.
- Ángel Inversionista: un inversionista que invierte capital privado y propio, a diferencia de un fondo de capital de riesgo, que invierte con responsabilidad fiduciaria de fondos ajenos.

B. Código Fuente de RI5C

B.1. Rutinas Básicas

A continuación se muestran las rutinas básicas para la generación de la red, se puede dividir en tres partes fundamentales:

- **La obtención de los datos**, con la función $get_contract$, que obtiene los datos de un respaldo de la cadena de bloques de Ethereum en un repositorio de Google BigQuery.
- **La generación del grafo**, utilizando la rutina de $create_graph$. Recibe datos estructurados y regresa un grafo generado por NetworkX.
- **Graficación de la red**, utilizando la función $draw_graph$ para dibujar una red no-pesada, no-direccionada utilizando Maplotlib y almacenarlo en un archivo tipo .png, o utilizando $generate_sigma_network$, que genera una red direccionada y pesada con información contextual y lo almacena en la notación de objeto estándar de javascript (JSON) que puede ser interpretado por SigmaJS.

A continuación, las rutinas principales en pseudo-código. Cabe resaltar que todo el código está protegino por una licencia APACHE, de acuerdo a: https://github.com/ebarojas/RI5C/blob/master/LICENSE

```
def get_contract(contract_address, limit=1000):

    contract_address = contract_address.lower()
    print ("Getting query...")
    test_query = """
        #standardSQL
        SELECT
          *
        FROM
          `bigquery-public-data.ethereum_blockchain.
             token_transfers`
        WHERE
          token_address='%s'
        LIMIT
          %s
    """ %(contract_address, limit)

    # === Generate credentials and connect to BigQuery

    print ("Finished getting data")
    # This returns a simple dataset that can be used and tested
    return rows

def create_graph(contract):
    # Create graph
    print ("Creating a simple graph...")
    G = nx.Graph()
    # Pandas dataframe TODO: this method should be extracted
```

```
    sorted_list = [u'token_address', u'from_address', u'
        to_address', u'value', u'transaction_hash', u'log_index' ,u
        'block_timestamp', u'block_number', u'block_hash']
    data=[list(x.values()) for x in contract]

    df = pd.DataFrame(data=data, columns=sorted_list)

    G = nx.from_pandas_edgelist(df, source='from_address', target=
        'to_address', edge_attr=["value", "transaction_hash"])

    print ("Graph created.")
    print(nx.info(G))

    # Get Avg Degree for graph_data
    nnodes = G.number_of_nodes()
    s=sum(dict(G.degree()).values())
    avg_degree = (float(s)/float(nnodes))
    graph_data = {"density": nx.density(G), "degree": avg_degree,
        "nodes": nnodes, "edges": G.number_of_edges() }


def draw_graph(graph, filename='network.png', x=100, y=100):
    print ("Starting to draw...")
    G = graph
    #first compute the best partition
    partition = community.best_partition(G)
    plt.figure(figsize=(x,y))
    #drawing
    size = float(len(set(partition.values())))
    pos = nx.spring_layout(G)
    count = 0.0
    for com in set(partition.values()) :
```

```
            count = count + 1.
            list_nodes = [nodes for nodes in partition.keys()
                                        if partition[nodes] == com]
            nx.draw_networkx_nodes(G, pos, list_nodes, node_size = 20,
                                        node_color = str(count / size)
                                           )

    # Draw
    nx.draw_networkx_edges(G, pos, alpha=0.5)

    print ("And now, let's save it in", filename)
    pylab.savefig('network.png')

def generate_sigma_network(graph):
    '''
    NOTE: G should include edge_attr="value" ie: G2 = nx.
       from_pandas_edgelist(df, source='from_address', target='
       to_address', edge_attr="value")
    This method should generate a JSON with sigmajs readable
       format
    It should integrate Nodes, Edges and positions
    '''
    print ("Starting to generate sigma.js compatible graph...")

    G = graph
    # POSITION: First compute the best partition and get positions
    partition = community.best_partition(G)
    pos = nx.spring_layout(G) # should try other layouts

    # COLOR - using louvain, should work on this more, colors are
       unnappealing and weird
    colors = {}
```

```
for node in G.nodes():
    colors[node] = '{0:06X}'.format(partition.get(node)+70000)

# NODE SIZE - Calculate node size
node_size = {}
for node in G.nodes():
    ne = G.edges(node, data=True)
    value = 0
    for v in ne:
        value += int(v[2]["value"])
    node_size[node] = value # Should add a log or something

# Weights
weights = []
for e in dict(G.edges).values():
    if float(e['value']) != 0.0:
        weights.append(float(e['value']))
    else:
        weights.append(0.0)

# txids
txids = []
for e in dict(G.edges).values():
    txids.append(e['transaction_hash'])

# Init JSON
data ={ 'nodes': [], 'edges': [] }

# Nodes
for n in G.nodes:
    data['nodes'].append({
            "id": n,
```

```
            "label": n+", total volume: "+ str(node_size[n]),
            "x": pos[n][0],
            "y": pos[n][1],
            "size": node_size[n],
            "color": "#"+colors[n]
        })

    # Edges
    for i, e in enumerate(G.edges):
        data['edges'].append({
            "id": "e" + str(i),
            "label": txids[i],
            "source": e[0],
            "target": e[1],
            "color": "rgba(190,190,190,0.4)", # Last digit is
                transparency
            "type": 'arrow',
            "size": weights[i]
        })

    print ("Finally, let's return data :)")

    return json.dumps(data)
```

C. Fuentes de Inversión privadas en México

Un estudio reciente de la Organización para la Cooperación y el Desarrollo Económico (OCDE) acerca de las nuevas empresas basadas en el conocimiento en México afirma que su escaso desarrollo, se explica por dos características importantes: OCDE (2010)

- Mercados financieros poco desarrollados. La aversión local al riesgo del sistema bancario tradicional agravada por un desarrollo débil del mercado de capital semilla, y la reducida capacidad y experiencia para evaluar el potencial de nuevas empresas innovadoras

basadas en el desarrollo científico o tecnológico, ha dejado a la mayoría de los posibles nuevos emprendedores sin recursos para financiar las etapas iniciales de sus empresas. Por otra parte, el tamaño y el alcance limitados del mercado de capital de riesgo en México es un problema que afecta la sostenibilidad financiera de nuevos emprendimientos a mediano y largo plazos, lo que obliga a estos negocios a su eventual venta o bien su afiliación a una empresa más grande para obtener líquidez y que los inversionistas obtengan retorno en su inversión.

- Desarrollo bajo y poca valoración de los activos tecnológicos intangibles. La cultura de los derechos de propiedad intelectual se ha difundido lentamente en México. Las solicitudes de patente basadas en los resultados de actividades científicas y tecnológicas, que promueve la acumulación de activos intangibles y facilita el acceso al capital semilla, está muy poco desarrollada, tanto en las empresas como en las instituciones públicas de investigación. Esta situación está mejorando gracias a las iniciativas emprendidas por el CONACYT, el Instituto Mexicano de la Propiedad Industrial y, más recientemente, por la Secretaria de Economía OCDE (2010).

Inversionistas Ángeles:

Además de la Asociación Mexicana De Capital Privado (AMEXCAP), existen varios clubes de inversionistas ángeles en México. Sin embargo, este mercado está poco desarrollado a comparación de economías más avanzadas. El estudio de la OCDE de 2012 menciona dos dificultades básicas que enfrenta este segmento:

- En primer lugar, no existe un plan de incentivos para los inversionistas de capital ángel en ninguna entidad pública (ni fiscales para los inversionistas, ni para el apoyo a redes).

- En segundo, hay cuestiones de regulación no resueltas, como que en México los grupos de capital ángel no pueden organizarse como entidades de responsabilidad limitada y, por ello, deben registrarse en el extranjero para asegurar la protección de sus accionistas minoritarios (principalmente en Canadá o en EUA) OCDE (2010).

Entre esos clubes de inversión, Angel Ventures México ocupa un lugar destacado. Busca apoyar a emprendedores para conseguir capital de los inversionistas ángeles de su red. En sus palabras: “Para presentar proyectos ante inversionistas, se debe de pasar por distintos filtros, que implican desde un plan bien pensado, hasta el hecho de tener inversionistas de nuestra

red interesados en la industria en particular. En caso de haber interés por parte de nuestros inversionistas, Angel Ventures apoya en la estructuración de la transacción, y se queda como socio en una parte minoritaria de cada proyecto. Esto lo hace para apoyar a la Administración a maximizar las posibilidades de éxito en una etapa crítica de las empresas, con miras a crecer el negocio, y eventualmente salirse de la empresa, vendiendo su participación accionaria" Angel Ventures (2014).

Al 2015, Angel Ventures ha participado en la inversión de 14 mdd en 100 negocios nuevos. "Han sido revisados 2500 proyectos. En 2011, Angel Ventures abrió oficinas privadas de inversión en los estados de Puebla y Yucatán y, actualmente, la oficina de la ciudad de México cuenta con 140 inversionistas potenciales OCDE (2010).

Otros grupos de inversionistas ángeles son Start Up Factory, Ángeles Inversionistas, Fundación E, Innovateur (en realidad un fondo de capital de riesgo) y los clubes ubicados en diversas ciudades. Una desventaja es que no reciben proyectos del Sistema Nacional de Incubadoras. Esto implica que no hay un seguimiento de los proyectos de inversión para búsqueda de financiamiento entre los recursos públicos y los potenciales inversionistas privados. Esta situación también puede significar que los proyectos desarrollados dentro de una incubadora tienen un riesgo más alto de morir Chelén and Bello (2014), o que el universo de los proyectos que revisa el comité de inversión ángel se constituye de buenas ideas pero no de proyectos bien desarrollados y orientados hacia el mercado.

Fondo multilateral de inversiones (FOMIN):

FOMIN ha apoyado a instituciones en México para fomentar el apoyo de empresas innovadoras con capital de riesgo. Tres ejemplos concretos de participación del FOMIN en fondos de innovación en México son:

- En el Fondo de Fondos NAFIN
- En el FONLIN de Nuevo León
- En Angel Ventures México

Asimismo, en 2011 el Banco Interamericano de Desarrollo aprobó una inversión de capital privado por 4 mdd que operará Angel Ventures México. Enfocada a las empresas pequeñas que tienen necesidades de capital de 200 mil a 2 millones de pesos (capital semilla), principalmente innovadoras.

En definitiva ha quedado claro que el capital de riesgo privado en México es reducido y orientado hacia actividades en etapas avanzadas y por ello en desventaja para la innovación.

D. Incorporación de Capital de Riesgo en programas gubernamentales

Programa Nacional de Innovación (PNI): Este programa lanzado en 2011 por el Comité Intersectorial para la Innovación (CII) es más explícito acerca de la importancia de desarrollar instrumentos de política pública en apoyo a las empresas innovadoras.

En sus palabras: "con el uso de varios tipos de programas e instrumentos de apoyo, el Gobierno debería garantizar la disponibilidad de fuentes de financiamiento de proyectos innovadores a través de sus etapas de desarrollo. Se pone especial énfasis en la necesidad de apoyar el desarrollo de las fuentes de capital semilla y subraya acertadamente la importancia de asociar el capital privado a las iniciativas gubernamentales" OCDE (2010).

INADEM:
El INADEM es un órgano administrativo desconcentrado de la Secretaria de Economía, cuyo objetivo es instrumentar, ejecutar y coordinar la política nacional de apoyo incluyente a emprendedores y a micro, pequeñas y medianas empresas, impulsando su innovación, competitividad y proyección en los mercados nacional e internacional para aumentar su contribución al desarrollo económico y bienestar social. Además se propone impulsar el desarrollo de políticas de cultura y productividad empresarial INADEM (2014). Entre sus funciones se encuentra acercar los esquemas de financiamiento a la actividad productiva para que llegue a quienes lo requieran.

Sus cuatro estrategias oficiales son:

- Apoyar la inserción exitosa de las MiPyMEs.
- Detonar proyectos productivos.
- Inculcar una nueva cultura nacional emprendedora y empresarial.
- Fortalecer el ecosistema de financiamiento.

Nacional Financiera (NAFIN):
Este banco de desarrollo apoya a las empresas innovadoras, a través de su Programa de Capital de Riesgo. NAFIN es el fiduciario del Fondo de Fondos que canaliza recursos a fondos de capital privado y de capital de riesgo. El Fondo de Fondos se integra por aportaciones de varios Bancos de Desarrollo y de la Secretaría de Economía. Uno de los objetivos de este programa es hacer llegar a startups innovadoras recursos a través de inversiones y apoyar las etapas iniciales y de expansión.

Para esto, el Fondo de Fondos creo un programa, llamado Mexico Venture, que tiene cuatro componentes:

- Mexico Venture One, un fondo con un presupuesto programado de 100 mdd que aporta recursos públicos y capital de inversión de instituciones internacionales en fondos de capital privado para invertir en operaciones de capital privado y de capital de riesgo. El tamaño promedio de cada fondo va de 15 a 20 mdd y la participación pública de cada uno de los fondos no debe superar 35 % del total.
- Desarrollo de programas de capacitación para los administradores de fondos en colaboración con instituciones privadas.
- Otorgar asistencia técnica y asesoría a empresarios sobre los requerimientos para el desarrollo de proyectos y para atraer fondos de capital ángel y de riesgo.
- Desarrollo de la red de capital ángel y de capital de riesgo para fortalecer los componentes de financiamiento público y privado del ecosistema de innovación.

La Secretaría de Economía ha destinado 70 mdd a NAFIN, de los cuales 20 mdd ya están asignados a empresas y fondos en México, 25 mdd están comprometidos y aún se

encuentran disponibles 25 mdd para las empresas o fondos que estén interesados en este programa. El apoyo depende del proyecto y el tipo de empresa o fondo, pero hay un interés mayor en los sectores que tienen una mejor perspectiva innovadora y comercial en los mercados nacionales e internacionales.

E. Estructuras corporativa

En México, la Ley de Sociedades Mercantiles rige el comercio y provee varias personalidades jurídicas para los emprendedores. Sin entrar en detalle en un tema que desvié del interés principal, podemos analizar principlalmente la Sociedad Anónima Promotora de Inversión de Capital Variable, o S.A.P.I. de C.V. Una sociedad mercantil cuyos titulares lo son en virtud de una participación en el capital social a través de títulos o acciones. Esta es la estructura más adecuada, simple y eficiente para poder recibir inversión externa, adjuntar socios o diferentes privilegios vinculados a las acciones.

Varias compañías optan por tener una Compañía Holding (ver Glosario) en EUA a modo de una Delaware C corporation, o una entidad en las Islas Cayman, esto por razones fiscales, de seguridad de datos o para facilitar recibir fondos de fuentes extranjeras y facilitar una adquisición, merger o para lograr un gobierno corporativo unificado cuando se opera en varios países.

F. Breve conclusión: inversión en México

Los fondos de inversión públicas proveen al emprendedor una fuente de ingreso accesible con muy poco riesgo, sin embargo, su rango de aplicaciones es muy limitado; no se puede usar para pagar sueldos ni rentas, y estos son los principales gastos para empresas de desarrollo tecnológico (ver Fig: 29). Por otro lado, obtener dichos fondos está sujeto a un proceso burocrático prohibitivo para un emprendedor y por ello, muchos favorecen obtener fondos de inversión privada, ángeles o familiares. A causa de esto, muchísimos fondos gubernamentales terminan en manos de empresas que no son tecnológicas ni están en fase de arranque.

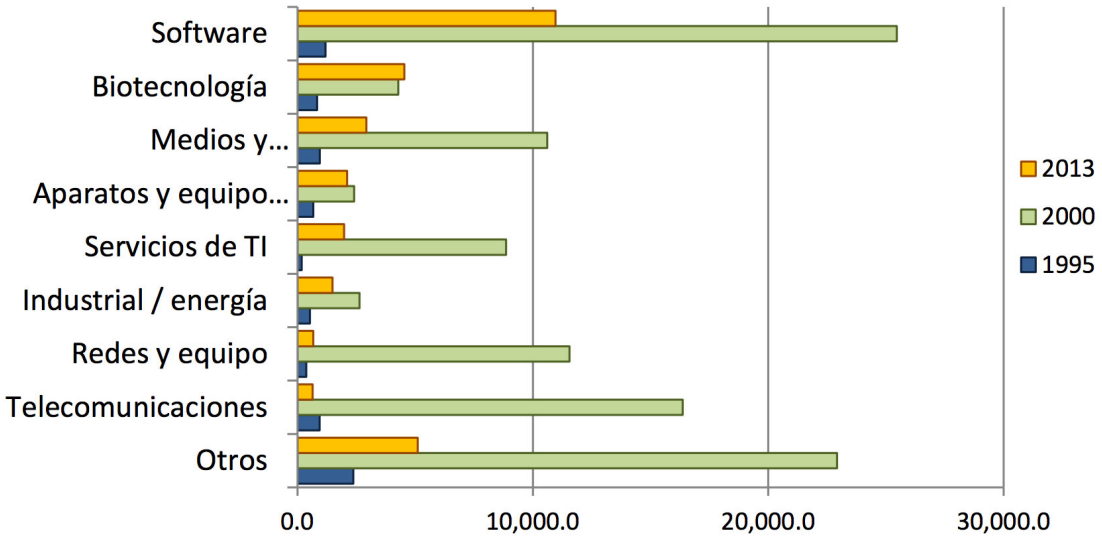


Figura 29: Mercado de startups en el mundo, fuente: PricewaterhouseCoopers/National Venture Capital Association MoneyTree

G. Rondas de Inversión

Normalmente las startups obtienen financiamiento que se divide naturalmente en rondas, que comienzan con una ronda de capital semilla o pre-semilla y continúan con una ronda A, B, C y así consecuentemente. Comunmente la valuación de la compañía y tamaño de la ronda aumentan a la par.

En rondas seed o pre-seed, normalmente se busca aplazar la valuación de la compañía hasta que contratos y propiedad intelectual se encuentren bien establecidos y se puede hacer un análisis más estricto por un tercero imparcial. La ronda A se refiere a la primer ronda donde la empresa recibe financiamiento considerable, normalmente una startup recibe su primer valuación oficial durante el proceso de levantamiento de la ronda A. En EUA es común que las startups levanten rondas C, D, E y F, sin embargo en México normalmente se vuelven profitable, quiebran o se logra una adquisición después de la serie B.

Las letras de las rondas están relacionadas al tipo de acciones que se emiten en la respectiva ronda. Es de importancia notar que en México el tamaño promedio de las rondas es de un 25 % del tamaño de rondas semejantes americanas.

De acuerdo con Amorós and Bosma (2015), el acceso a capital es el principal cuello de botella para startups en México. El capital de riesgo está en sus primeros pasos y el 80 % de los emprendedores Chelén and Bello (2014) deben buscar métodos de fondeo alternativos Angela Cois (2015). Algunas fuentes de financiación aún son muy conservadoras para invertir en empresas de alto riesgo Chelén and Bello (2014), lo cual genera una oportunidad para fuentes que puedan medir y asumir este riesgo correctamente. Es por ello que el objetivo de esta tesis sea de interés para las entidades **bancarias y financieras**.

Referencias

Aite (2017). Is blockchain a good fit?: A disciplined approach in post-trade.

Alastair Darling (2008). Statement by the chancellor on financial stability. https://web.archive.org/web/20081011062730/http://www.hm-treasury.gov.uk/statement_chx_081008.htm.

Ametrano, F. M. (2017). Bitcoin, blockchain, and distributed ledgers: Between hype and reality.

Amorós, J. E. and Bosma, N. (2015). *Global Entrepreneurship Monitor: 2015 Global Report*. Babson College, Universidad del Desarrollo, and Universiti Tun Abdul Razak.

Andersen, N. (2016). Blockchain technology: A game changer in accounting?

Angel Ventures (2014). Angel ventures. http://www.angelventuresmexico.com.

Angela Cois (2015). A Not So Glamorous Startup Life in Mexico. https://medium.com/@angiecois/a-not-so-glamorous-startup-life-in-mexico-4974961d0e4b#.u55it8t2u.

Auger, C. (1975). *Use of Reports Literature*. London Butterworth.

Banco Mundial (2015). Capitalización en el mercado de las compañías que cotizan en bolsa. http://datos.bancomundial.org/indicador/CM.MKT.LCAP.CD?order=wbapi_data_value_2009+wbapi_data_value+wbapi_data_value-last&sort=desc.

Baur, D. G. and Lucey, B. M. (2010). Is gold a hedge or a safe haven? an analysis of stocks, bonds and gold. *The Financial Review*.

Baur, D. G. and McDermott, T. (2010). Is gold a safe haven? international evidence. *Journal of Banking and Finance*.

Baur, D. G. and McDermott, T. (2016). Why is gold a safe haven? *Journal of Behavioral and Experimental Finance*.

Beecroft, N. (2015). Bitcoin: Risk factors for insurance. *Lloyd's Emerging Risk Report*.

Bevir, M. (2013). *TGovernance: A very short introduction*. Oxford, UK.

Biggs, N., Lloyd, E., and Wilson, R. (1986). *Graph Theory, 1736-1936*. Oxford University Press.

Bitcoin-Talk (2010). Re: Switch to gpl. https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/211/.

Bitcoinity (2017). Bitcoin price.

Black and Fischer (1973). The pricing of commodity contracts. *Journal of Financial Economics*.

Blank, S. (2013). Why the lean start-up changes everything. *Harvard Business Review*, 91(5):63–73.

Bolt, W. (2016). On the value of virtual currencies (april 20, 2016). bank of canada working paper no. 2016-42.

Bravelas, A. (1950). Communication patterns in task-oriented groups. *J. Acoust. Soc. Am.*, pages 725–730.

Brown, T. (2017). Real use cases for blockchain and distributed ledger technologies in the asset management sector.

Buchholz, M., Delaney, J., and Warren, J. (2012). Bits and bets: Informacion, price volatility, and demand for bitcoin. https://www.reed.edu/economics/parker/s12/312/finalproj/Bitcoin.pdf.

Buterin, V. (2014). Ethereum.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric.

Casey, M. J. and Vigna, P. (2018). In blockchain we trust. *American Educational Research Journal*, 121(3).

CB Insights, G. S. (2017). The pace of ico fundraising has now surpassed angel & seed stage internet vc funding globally. https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html.

Chelén, R. and Bello, G. G. (2014). *Capital de Riesgo para el Desarrollo de Empresas Innovadoras*. Foro Consultivo Científico y Tecnológico, A.C.

Clayton, J. (2018). Testimony on "virtual currencies: The oversight role of the u.s. securities and exchange commission and the u.s. commodity futures trading commission" by jay clayton chairman, u.s. securities and exchange commission before the committee on banking, housing, and urban affairs united states senate february 6, 2018. https://www.banking.senate.gov/public/index.cfm/2018/2/virtual-currencies-the-oversight-role-of-the-u-s-securities-/and-exchange-commission-and-the-u-s-commodity-futures-trading-commission.

Coinmarketcap (2018). Cryptocurrency market capitalizations. https://coinmarketcap.com/charts/.

Coinschedule (2017). Cryptocurrency ico stats 2017.

Coronavirus Bailouts (2020). Bbc news. https://www.bbc.com/news/business-52450958.

Coronavirus disease (COVID-2019) situation reports (2020). World health organization. https://fred.stlouisfed.org/series/UNRATE8.

COVID-19 Pandemic (2020). Unemployment rate. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports/.

Crawford and Meadows (2017). Blockchain technology as a platform for digitization.

Davidson, L. (1990). *Financial Markets and Williamson's Theory of Governance: Efficiency Versus Concentration Versus Power*, pages 324–338. Palgrave Macmillan UK, London.

Diemers and Koster (2016). Five propositions to transform the financial services sector.

DOF-09-03-2018 (2018). Ley para regular las instituciones de tecnología financiera. **?**.

Duca, J. V., Muellbauer, J., and Murphy, A. (2011). House prices and credt constraints: Making sense of the us experience. *The Economic Journal*.

Emergency Economic Stabilization Act (2008). Library of congress draft. https://www.govtrack.us/congress/bills/110/hr1424/text.

FINMA (2018). Guidelines for enquiries regarding the regulatory framework for initial coin offerings (icos) published 16 february 2018. https://www.iosco.org/library/ico-statements/Switzerland%20-%20FINMA%20-%20ICO%20Guidelines.pdf.

Fjordback Søndergaard, T., Andersen, J., and Hjørland, B. (2003). Documents and the communication of scientific and scholarly information. *Journal of Documentaiton*, pages 278–320.

Foundation, E. (2017). Erc20 token standard.

Freeman, L. (1977). A set of measures of centrality based betweenness. *Sociometry*, pages 35–41.

Frunza, M.-C. (2017). *Solving Modern Crime in Financial Markets: Analytics and Case Studies*. Academic Press.

Galka, M. (2019). Some overdue transparency into the cryptopia exchange hack. https://elementus.io/blog/cryptopia-hack-transparency/.

Ghoshal, S. (2005). Bad management theories are destroying good management practices.

Griffin, J. M. and Shams, A. (2018). Is bitcoin really un-tethered? *White Paper*, 3(1).

Haun, K. (2013). Usa vs ross ulbricth. https://archive.org/details/pdfy-6s57o3H70B1vH6bF.

Hearn, M. (2016). Corda: A distributed ledger.

House Bill No. HB0185 (2019). State of wyoming. https://www.wyoleg.gov/2019/Introduced/HB0185.pdf.

Hubbard, D. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It.* John Wiley & Sons.

INADEM (2014). Instituto nacional del emprendedor. https://www.inadem.gob.mx/.

Karpeles, M. (2014). Announcement regarding the balance of bitcoin held by the company. https://www.mtgox.com/img/pdf/20140320-btc-announce.pdf.

Katz, L. (1953). A new status index derived from sociometric analysis. *Psychometrika*, pages 39–43.

Kolte, A. and Wagh, P. (2019). Analyzing punjab national bank scam. 6:585–592.

Markowitz, H. (1952). Portfolio selection. *The Journal of Finance*, pages 77–91.

Minniti, M. and Lévesque, M. (2010). Entrepreneurial types and economic growth. *Journal of Business Venturing*, 25(3):312.

Mochizuki, T. (2015). Japanese police arrest mark karpeles of collapsed bitcoin exchange mt-gox. https://www.wsj.com/articles/japanese-police-arrest-mark-karpeles-of/-collapsed-bitcoin-exchange-mt-gox-1438393669.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nanotech Excitement Boosts Wrong Stock (2003). Nanotech Excitement Boosts Wrong Stock. https://www.techdirt.com/articles/20031204/0824235.shtml.

Needham, T. (1993). A visual explanation of jensen's inequality. *American Mathematical Monthly*, page 768–71.

Newman, M. (2009). The mathematics of networks.

Nilsson, K. (2015). The missing mtgox bitcoins. https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html.

OCDE (2010). *Estándares de Calidad para la Evaluación del Desarrollo*. OCDE, primera edition.

Perron, O. (1907). Zur theorie der matrices. *Mathematische Annalen*, pages 248–263.

Ries, E. (2011). *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*. Crown Publishing.

Sabidussi, G. (1966). The centrality index of a graph. *Psychometrika*, pages 581–603.

Sampieri Hernández, R., Collado Fernandez, C., and Lucio Baptista, P. (2003). *Metodología de la Investigación*. Mc Graw-Hill Interamericana.

Schembri, S. (2018). *The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act.* Parliamentary Secretariat for Financial Services, Digital Economy for Innovation, Office of the Prime Minister.

Schumpeter, J. A. (1942). Capitalism, socialism and democracy. *Routledge*, pages 82–83.

Schwab Advisor Service News (2015). Ria merger and acquisition deals pick up pace and size according to latest data. Technical report, Schwab Advisor Services.

Seale, J. A. (2014). *Mexico Mergers and Acquisitions Update*. Seale and Associates.

Sehra, D. A. (2017). Economics of initial coin offerings.

Senor, D. and Singer, S. (2009). *Startup Nation*. Hachette Book Group.

Smith, A. (2013). *Totally Wired: On the Trail of the Great Dotcom Swindle*. Bloomsbury Books.

Startup Etymology (2015). Quora. https://www.quora.com/What-is-the-etymology-of-the-term-startup.

Stavroyiannis, S. (2018). Value-at-risk and related measures for the bitcoin. *The Journal of Risk Finance*.

Taleb, N. N. (2012). *Antifragile*. Penguin Books.

Tasca, P., Hayes, A., and Liu, S. (2017). The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. *The Journal of Risk Finance*.

The World Bank (2020). Mexico gdp data. https://data.worldbank.org/country/mexico?most_recent_value_desc=true.

Toby Lewis (2013). Corporate venturing participants near 1,000. www.globalcorporateventuring.com/article.php/6001/corporate-venturing-participantsnear-1000.

Woo, W. (2019). Nvt ratio. https://charts.woobull.com/bitcoin-nvt-ratio/.