Universidad de San Andrés

Departamento de Economía

Licenciatura en Economía

Desarmando Bloques: Un enfoque de costos de transacción y Blockchain sobre estructuras de organización óptimas

Autor: Alexander Coleman

Legajo: 16043

Mentor de Tesis: Daniel Friel

Buenos Aires, Octubre de 2018

Universidad de San Andrés

Departamento

Licenciatura en Economía

Desarmando Bloques: Un enfoque de costos de transacción y Blockchain sobre estructuras de organización óptimas

Autor: Alexander Coleman

Legajo: 16043

Mentor: Daniel Friel

Buenos Aires, Octubre 2018

Contenido

ABSTRACT

Este trabajo tiene como objetivo enmarcar la tecnología de Blockchain dentro de la teoría de costos de transacción. Para abordar este análisis, se ahondará en los mecanismos técnicos de Blockchain que aseguran sus propiedades fundamentales de inmutabilidad y transparencia, así como los incentivos que motivan a los agentes a participar en su funcionamiento. Estas propiedades se aplican a las distintas áreas propuestas por la economía de costos de transacción y en particular el análisis comparativo propuesto por Williamson (1991), para comprender cómo afecta la elección de estructuras de gobernanza óptimas. Se encuentra que la transparencia e inalterabilidad de transacciones que promete esta tecnología reduce el riesgo de oportunismo, mediante una difusión más rápida de información, un menor riesgo de expropiación de derechos de propiedad, la posibilidad de ejecutar contratos sin intermediarios, y la reducción de requerimientos reputacionales para interactuar entre agentes en una economía. Con menor riesgo de oportunismo, y menores costos de transacción asociados, se concluye que las estructuras de gobernanza óptimas se alejan de las estructuras jerárquicas, hacia estructuras híbridas o de mercado. Este análisis se aplica a la industria agrícola de Argentina, para demostrar cómo la utilización de esta tecnología puede motivar a la existencia de redes de producción con menor necesidad de coordinación centralizada.

1. Introducción

1.1 Blockchain y Satoshi Nakamoto

En el año 2008, un autor bajo el seudónimo *Satoshi Nakamoto*, publicó un artículo describiendo un protocolo para efectuar pagos de manera digital de manera descentralizada y segura. Bitcoin, como decide llamarlo, busca resolver un problema común en las plataformas digitales llamado "doble gasto", sin la necesidad de un intermediario que garantice la seguridad de la transacción entre dos individuos.

Nakamoto (2008) sugiere que la intervención de un tercero que garantice las condiciones de pago entre dos partes eleva los costos de la operación, lo cual hace que pagos electrónicos de menor monto no sean posibles de manera digital. En particular, propone extraer al garante de confianza en la transacción, y trasladar las transacciones a un sistema donde el sistema en sí provea la seguridad del intercambio. A este sistema, lo llamó Blockchain, debido a su arquitectura de registros encadenados entre sí.

En el año 2010, el autor detrás del seudónimo Satoshi Nakamoto abandonó las publicaciones, y no se supo más de él. Existen múltiples especulaciones acerca de su identidad, pero ninguna confirmada. Sin embargo, su creación, la plataforma Bitcoin, creció en usuarios y en valor nominal gracias a la cooperación de múltiples desarrolladores.

La evolución de Bitcoin es una historia más que interesante (que involucra hacks millonarios, su uso como medio de pago en plataformas ilegales en la Dark Web, y múltiples fluctuaciones en el mercado), pero el foco de este trabajo es ahondar en el mecanismo subyacente, Blockchain, y su promesa de reducción de costos existentes en las transacciones entre individuos.

Como se describirá en detalle en este trabajo, lo que se conoce como Blockchain es una serie de programas e instrumentos tecnológicos que permiten el mantenimiento de un registro históricos de activos y transacciones, que puede mantenerse de manera descentralizada, sin necesidad de depositar confianza en una única autoridad que verifique la información. En su forma más pura, todos los participantes pueden ver y validar todas las transacciones ocurriendo en una misma red, por ende las transacciones no pueden ser modificadas, evitando los costos y desventajas asociadas a tener un organismo central que sea dueño de la verificación de la información

Al momento de escribir este trabajo, existen innumerables criptomonedas, empresas y negocios vinculados a esta tecnología emergente. Asimismo, hay incontables noticias que surgen alabando la tecnología, o prediciendo su caída. Sin embargo, falta un entendimiento general de las bases sobre las que funciona esta herramienta, así como también un análisis estructural que permita entender cuan factible es la promesa de Blockchain, y dónde realmente se puede esperar ver un impacto, más allá de las fluctuaciones en valor de los múltiples activos financieros comúnmente asociados a la tecnología.

1.2 Costos de Transacción: Un Marco Teórico

Este análisis requiere de un marco teórico establecido que permita una crítica real y pragmática de su potencial. Dado que Nakamoto buscaba reducir los costos de las transacciones, y descentralizar el intercambio entre individuos, un buen punto de partida teórico es el análisis económico de los costos de transacción.

El prestigioso economista Ronald Coase, en su trabajo *The Nature of the Firm* (1937) es el primero en presentar el concepto de costos de transacción. En el artículo, plantea una crítica a la economía neoclásica, al buscar entender por qué en algunos casos, la asignación de recursos no se hace a través del mercado (vía el mecanismo de precios). Coase observa que en la realidad también existen las empresas (o un emprendedor-coordinador) que asignan los recursos acorde a otros motivos. Coase sugiere que la razón por la cual existen las empresas es porque existen costos al utilizar el mecanismo de precios para coordinar agentes en una economía.

Coase no usa el término "costos de transacción" específicamente, pero impulsa una línea de investigación que se separa de la existente en ese momento, formalizada por autores como Douglass North y Oliver Williamson, que busca entender por qué ciertas organizaciones crecen y aparecen y como interactúan éstas con la economía, poniendo foco en las instituciones y transacciones como foco de análisis. A esta escuela se la llama Nueva Economía Institucional, o NIE por sus siglas en inglés, y de ella desprende un análisis comúnmente denominado economía de costos de transacción (TCE por sus siglas en inglés) que sugiere que las elecciones de los agentes en una economía muchas veces buscan economizar en estos costos, formando estructuras de organización que se alejan del mercado.

Oliver Williamson, sugiere que uno de los objetivos principales de la economía de costos de transacción es entender qué parámetros influyen en la elección de las organizaciones para agruparse de cierta manera, partiendo de la pregunta original de Coase, que es entender

por qué las empresas se integran verticalmente en lugar de interactuar de manera descentralizada (Williamson 1998).

Williamson (1998) plantea que, dada la existencia de racionalidad limitada (otro concepto que aleja esta escuela de la economía neoclásica) los arreglos contractuales con los que los participantes de una economía se regulan entre sí es importante. El autor sugiere que, en interacciones complejas, surgen instancias en las que alguno de los participantes puede aprovecharse del otro. Dada esta realidad, las elecciones de sistemas de organización que reduzcan las posibilidades de oportunismo es relevante, ya que es se torna un instrumento que permite asegurar transacciones seguras y eficientes en una economía. Su conclusión, que es punto de partida para muchos otros economistas, es que existen tres grandes estructuras de organización: el mercado clásico, las empresas que se integran verticalmente (estructuras jerárquicas) y las estructuras híbridas, que son intermedios entre el mercado y las empresas, y que incluyen organizaciones como consorcios, cooperativas, franquicias, sociedades, etc.

1.3 Objetivos y guía de lectura

Dada la promesa de Blockchain de permitir un sistema de que reduzca el oportunismo, y considerando que la economía de costos de transacción analiza las estructuras óptimas que lo reducen, se espera que este enfoque permita entender dónde esperar cambios, y en particular ver si la tecnología de Blockchain permite alguna actualización a la investigación vigente en la disciplina. En particular, este trabajo busca entender si las estructuras óptimas se modifican de alguna manera dado el cambio de parámetros que propone esta nueva plataforma. Una vez que definamos el potencial impacto sobre estructuras de gobernanza, proponemos aplicar este análisis a una industria específica (la industria agrícola en Argentina) para entender que implicancias existen, en particular en una industria que depende fuertemente de la generación de reputación para reducir el oportunismo.

Este trabajo toma conceptos de múltiples disciplinas, tales como las ciencias de computación y economía, y como tal, requiere una descripción a nivel detallada de los conceptos que serán utilizados en el documento. En esta línea, una de las contribuciones de este trabajo es dar una explicación detallada de los principios sobre los que opera Blockchain. Esta descripción detallada cumple dos funciones relevantes. Por un lado, al presentar Blockchain de manera simple, pero demostrando que los conceptos sobre los que opera son conceptos probados de la ciencia de la computación, permite tener una discusión que permite la crítica y la comprensión de las distintas partes del funcionamiento de Blockchain. Esto

permite poder teorizar acerca de las distintas modificaciones al protocolo que son posibles, de manera tal que permita investigar aplicaciones en la economía real. Es importante aclarar que no se busca anticipar la vigencia de la tecnología hacia el futuro, sino más bien explorar la promesa de Blockchain como facilitador de descentralización utilizando disciplinas de investigación establecidas. El segundo punto que se busca con esta descripción es reducir las criptomonedas (mucho más publicitadas) a una pequeña parte del funcionamiento de la tecnología, y en particular ver su rol como incentivo para mantener integridad en un sistema, en lugar de activo de especulación financiera. Dado este objetivo, el capítulo 2 de este trabajo es una descripción escalonada de los conceptos computacionales y su interacción en la suite Blockchain. El foco es la presentación modular de las distintas aplicaciones, empezando por la generación de transacciones, y avanzando a través del armado de contratos inteligentes y los casos de uso empresariales.

El capítulo de Blockchain requiere una aclaración acerca de la bibliografía, que contiene particularidades que serán más importantes en el futuro a medida que nuevas tecnologías se sigan promoviendo. Debido a que la suite de software englobada por Blockchain es de código abierto (de libre utilización y modificación), existe una multitud de aplicaciones distintas, y sus propiedades cambian dependiendo de la aplicación puntual que tengan (hay muchos Blockchain, ninguno es igual entre sí). Dada esta particularidad, la literatura acerca de su funcionamiento es heterogénea, y está basada en White papers, documentación técnica versionada (GitHub, Wikis), y papers académicos (aunque la literatura académica es menos numerosa). Para hacer más simple el análisis, este trabajo buscará ser agnóstico y describir los mecanismos más utilizados, en su formato original.

El tercer capítulo sirve para presentar otro de los objetivos de este trabajo, que es presentar los fundamentos básicos del análisis de costos de transacción. Aquí se presentarán las investigaciones de Ronald Coase, Oliver Williamson y los demás precursores de la nueva economía institucional, pero buscando enfocar el análisis en los hallazgos relacionados con los incentivos detrás del armado de estructuras de mercado, híbridas y jerárquicas. Lamentablemente no se ahondará en las críticas a esta línea de investigación y a su defensa, pero se revisarán diversas fuentes y autores para mostrar cómo el análisis fue evolucionando a través del tiempo.

Una vez finalizada la presentación de economía de costos de transacción, el capítulo 4 presenta un análisis utilizando los modelos semi formales de costos de transacción, tal como son propuestos por los autores citados en el capítulo 3. En particular se propondrá entender

cómo Blockchain afecta el conjunto de parámetros institucionales que incide en la elección de estructuras de governance óptimas para cada tipo de transacción. Este análisis busca basarse en modelos teóricos formales, pero también plantea una discusión de tipo especulativo, que sirva de base de futuras investigaciones. Dada la naturaleza incipiente de la tecnología de Blockchain, y su carácter dinámico e inmutable, se persigue este enfoque para arrancar la conversación, pero queda abierto a críticas y mejoras.

El capítulo 5 presenta un pequeño análisis de la industria agrícola en Argentina, y cómo Blockchain podría afectar la manera en la que interactúan los agentes económicos en su estructura. Este escenario es de particular interés, porque como fue mencionado previamente, la industria agrícola en Argentina es un ejemplo claro de coordinación vía redes, donde la generación de reputación actúa como un mecanismo para asegurar la interacción entre participantes de la industria. En estos casos, la confianza en un organismo coordinador, y el compartir recursos entre productores asegura la apropiación de rentas. En este escenario, introducir Blockchain, para reducir la dependencia de un ente coordinador, puede resultar en una estructura de organización más descentralizada. Cabe aclarar que el análisis será a nivel teórico, enfocando en estructuras de organización, y una aplicación de capa superior de la tecnología, no se ahondará en casos de uso concretos de la tecnología en el campo.

El capítulo 6 resume las conclusiones, críticas y sugerencias de investigación futura.

2. Blockchain

2.1 ¿Qué es Blockchain?

Un problema recurrente en plataformas de pagos digitales es evitar el *doble gasto*. El doble gasto es el escenario en el que un participante en una transacción intercambia bienes, pagando con un activo, y al mismo tiempo, interactúa con otro participante pagando con el mismo activo. En sistemas *descentralizados*, no hay un regulador con visión de ambas transacciones, y la transacción no puede evitarse, permitiendo fraude y oportunismo. La solución suele ser intercambiar bienes a través de un intermediario, que pueda garantizar que la transacción se ejecute correctamente, reemplazando la confianza entre actores, por una confianza en el intermediario, que suelen ser bancos, plataformas de e-commerce, o tarjetas de crédito.

A medida que el comercio se vuelve más dependiente de estos intermediarios, los servicios que proveen los intermediarios se hacen más costosos. Sin embargo son necesarios para poder seguir comerciando.

En el año 2008, un autor bajo el seudónimo Satoshi Nakamoto, planteó una solución a este problema[1]. Su solución busca reemplazar la confianza en los intermediarios, con una plataforma digital entre pares que tenga un protocolo de validación que permita reemplazar la necesidad de confianza entre pares, por un sistema lógico descentralizado. En esencia, Nakamoto buscó implementar un modelo en el que la confianza entre pares no fuera necesaria entre los participantes de una transacción, porque los participantes confían en el modelo subyacente sobre el que están operando, o más bien, tienen incentivos para asegurar la integridad de la plataforma. La plataforma de pagos propuesta fue llamada *Bitcoin*.

Nakamoto no fue el primero en atacar este problema, ni el primero en proponer una solución, pero su contribución es la introducción de un mecanismo de validación y verificación que fue refinado por múltiples autores. Este mecanismo toma conceptos probados de *criptografía* y *arquitectura de sistemas*, y los fusiona en un sistema de incentivos que permita el registro de transacciones sin la participación de una autoridad central. Esta tecnología, llamada *Blockchain*, permitió la creación de múltiples capas de aplicación distintas, que se desarrollarán en este trabajo.

En este trabajo, siguiendo la sugerencia de Drescher (2017) se define a Blockchain como una suite de tecnología que permite la *integridad de transacciones* en una arquitectura de software *distribuida*, mediante un mecanismo de *interacción entre pares*. Se le llama Blockchain, porque consiste en una cadena de *bloques secuenciales en el tiempo*, que contienen información acerca de las transacciones entre pares en esa base de datos. Esta cadena de bloques actúa como un *libro mayor* de registros, que registra todas las transacciones históricas, ayudando a definir quien es dueño de qué en cada momento. Para garantizar esta integridad, hay mecanismos de seguridad que garantizan la *inmutabilidad* de los registros históricos, así como también existen incentivos para que los participantes se comporten de manera honesta.

Esta definición no incorpora conceptos de activos o criptomonedas, que suelen ser las aplicaciones más conocidas de la tecnología. Esto es intencional, dado que se busca ahondar en el mecanismo subyacente de la tecnología, para entender el potencial de uso de la tecnología más allá del sistema financiero. En pos de este objetivo, las siguientes secciones serán una

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

introducción a conceptos técnicos que son relevantes para entender esta tecnología correctamente.

2.2 Un sistema descentralizado

En un sistema de software centralizado, los componentes (que pueden compartir funciones, o no) están conectados a través de un componente central que coordina las actividades.

En un sistema distribuido, los componentes están todos conectados sin un punto central que coordine o controle el resto de los componentes. Cada dispositivo que transfiere información (se denominan *nodos*) coordinan sus actividades pasándose mensajes entre sí. Es importante notar que no necesariamente cada nodo está conectado entre sí, pero sí que cada nodo esté conectado con otro de forma indirecta (o sea, a través de otro nodo).[2]

Figura 2.2-1: Modelo distribuido vs Centralizado

Las ventajas de un sistema distribuido son la reducción de puntos de falla, el poder computacional incrementado con cada participante, y el potencial para crecer de manera orgánica. Una de sus mayores desventajas, es la complejidad para mantener integridad entre todos los nodos participantes. Esto ocurre dado que no todos los mensajes se reciben en cada nodo al mismo tiempo.

En estos modelos de arquitectura, generalmente los nodos son proveedores de servicios (se los denomina servidores), o demandantes (se los denomina clientes). A este modelo de arquitectura se lo denomina arquitectura cliente-servidor.

[2] Coulouris, G. F., Dollimore, J., & Kindberg, T. (2005). Distributed systems: concepts and design. pearson education.

Una variante a este modelo, dentro de las arquitecturas descentralizadas, es el modelo P2P (por sus siglas en inglés Peer-to-Peer o entre pares). En este modelo, cada nodo es una computadora, que participa de la red, sumando sus recursos computacionales, pero donde es servidor y cliente a la vez. O sea, donde todos los roles son iguales y pueden cumplir las mismas funciones.

Couloris et. Al (2005) sugieren que los modelos P2P permiten mayor escalabilidad, dado que los recursos de los clientes son al mismo tiempo utilizados para soportar el servicio, por ende a mayor cantidad de participantes, mayor el poder de procesamiento. Según los autores, los modelos P2P tienen las siguientes características:

- Su diseño asegura que todos los participantes contribuyan al sistema
- Aunque los nodos difieran en la cantidad de recursos que proveen a la red, todos comparten las mismas capacidades y responsabilidades.
- Su funcionamiento no depende de un sistema central.
- Pueden ser diseñadas para dar cierto grado de anonimato a sus participantes
- El componente más importante es la elección de un algoritmo que distribuya la carga operativa entre nodos de manera eficiente.

Ejemplos conocidos de la arquitectura P2P son el programa Napster, que permitía compartir archivos multimedia entre usuarios, y el protocolo BitTorrent, que permite transferir archivos de gran tamaño mediante la descarga y replicación del archivo dividido en pequeñas partes a través de los nodos en las redes.

Esta introducción a arquitectura de software será relevante para este trabajo porque como se verá más adelante, Blockchain es una plataforma de información distribuida, que utiliza interacción P2P. Su contribución más importante en este aspecto, sin embargo, es el diseño de un modelo de comunicación que resuelva la dificultad de mantener la información actualizada en todos los nodos. Esto es, Blockchain propone un mecanismo para mantener integridad de información sin necesidad de un mecanismo coordinador.

2.3 Funciones Hash

Como se explicará más adelante, Blockchain permite mantener registros de manera inmutable, y de manera segura. Para lograr esto, utiliza lo que se denominan *funciones hash*.

Las funciones hash de una dirección son funciones que permiten convertir un valor, en un nuevo valor de una longitud fija, pero donde es prácticamente imposible poder derivar el valor original a partir del nuevo valor.

Utilizando la nomenclatura de Coulouris et al (2005) se define una función hash $h = H(M)$ tal que:

- Conociendo *M*, sea fácil encontrar el valor *h*
- Conociendo *h*, sea difícil encontrar el valor *M*
- Conociendo *M*, sea difícil encontrar un valor alternativo *M'* donde *H(M) = H(M')*

Drescher (2017) agrega que las funciones hash son *pseudoaleatorias*, dado que cuando el valor *M* difiere de *M'* mínimamente, el valor *h* calculado de ambas funciones diferirá de forma impredecible.

En la figura 2.3-1, se puede evidenciar como textos de distinta longitud, se convierten en bloques de texto de igual longitud una vez procesados por una función hash.

Valor Entrada	Valor Salida
Tesis	B1F97931ADF9E1CBEDF5C45E47B1F28E59473203D05B032D247A7106B79F0217
Economía	A3DBA4AD43B1E7E0B84995ACC19C1277758D5527EA50C9C3E263BA72BD2965F7
Blockchain	625DA44E4EAF58D61CF048D168AA6F5E492DEA166D8BB54EC06C30DE07DB57E1
¡Hola Mundo!	239BDFAAD79AFDF9220349DDCCD67B1E801AA275D757AC90C3977AC2F0A1F9E4

Figura 2.3-1: Valores hash calculados utilizando función hash SHA-256[3]

Las funciones hash son utilizadas en criptografía para asegurar *integridad* en bloques de datos. Al comprimir largos bloques de información en segmentos más cortos de información, distintos conjuntos de información pueden ser comparados entre sí para ver si hubo modificaciones. Por ejemplo, un contrato de 20 páginas de longitud puede ser comprimido en un valor hash, y compararlo con otro valor hash generado para un contrato supuestamente igual. Si una letra cambia en alguna parte del contrato, los valores hash van a

[3] El valor 256 refiere a la cantidad de bits que tendrá el bloque de información. Cuanto más largo el bloque de información más improbable es encontrar un valor igual, pero requiere mayor poder de procesamiento computacional.

diferir por ende es evidencia de manipulación. La figura 2.3-2 muestra un ejemplo donde un simple carácter cambiado, genera un resultado completamente distinto al anterior.

Valor Entrada	Valor Salida
Esto es un contrato establecido entre las dos individuos para acordar la comercialización de un producto con determinados términos y condiciones.	C643F54278A225B75AE2E4744D56130AB2041A8FEB481B35D56E6C9BF7F5BD0C
Esto es un contrato establecido entre las dos individuos, para acordar la comercialización de un producto con determinados términos y condiciones.	A5CE5659B830B9573592ED2A838F377ED73C63C4040CBCF88310DD72E1D8B74F

Figura 2.3-2: el agregado de una coma (,) luego de la palabra 'individuos' genera un valor de salida completamente distintos, demostrando que los valores originales no son idénticos.

Otro tipo de uso para las funciones hash, que es de particular uso en Blockchain, es su utilización para generar *costos computacionales*. Esto se refiere a situaciones donde al computar la solución a una función hash se le agregan *restricciones* que hacen más dificultosa su resolución, por ende el esfuerzo de procesar la solución es mayor y requiere mayores recursos computacionales.

A este uso de funciones hash para generar costos de procesamiento se lo denomina *sistema de Prueba de Trabajo (Proof of Work)*[4], y fue establecido para evitar que los recursos computacionales de servidores de internet sean atacados por un acceso no autorizado. [5]

Adam Back (2002) propuso la utilización de funciones hash como mecanismos criptográficos para proteger de ataques. Partiendo de la función propuesta por Coulouris et al (2005) donde una función hash puede ser definida como:

$$h = H(M)$$

Back sugiere que el problema computacional sea identificar M tal que el resultado hash resultante sea igual a un valor conocido previamente. Como se mencionó en la definición de

[4] Jakobsson, M., & Juels, A. (1999). Proofs of work and bread pudding protocols.
[5] El objetivo es que, cuando se detecta un ataque, el servidor presente problemas criptográficos al cliente, que tiene que resolver para poder acceder a la información (la evidencia de esta solución es lo que se llama Prueba de Trabajo o Proof of Work). Esto logra que el trabajo computacional sea mayor con cada acceso, y el ataque sea menos redituable para el nodo que ataca al servidor.

Coulouris et al (2005), una de las propiedades de las funciones hash es que encontrar el valor de *M* conociendo *h* es difícil, dado que las funciones hash son pseudoaleatorias.

Nakamoto (2008) propone utilizar este mecanismo para generar procesamiento computacional utilizando una *restricción de dificultad*. En el caso de Bitcoin, la restricción está dada por la cantidad de valores iguales a cero con el que empieza el valor hash a encontrar, donde a mayor cantidad de ceros, más difícil es el ejercicio computacional.

Para entender como funciona este mecanismo, es de utilidad ver un ejemplo. Drescher (2017) propone un ejercicio ilustrativo muy simple, que se presenta debajo recalculando los valores. En este ejemplo, el texto original es "Hola Mundo" y el objetivo es encontrar el valor (se le denomina *nonce)* tal que, concatenado al texto original, su valor hash sea igual a un valor determinado con una restricción definida (por ejemplo, la cantidad de ceros que preceden al valor hash).

En un escenario de dificultad 3 el objetivo es encontrar un valor hash que comience con 3 ceros consecutivos:

$$h = H(M)$$

$$x = nonce$$

$$h = 000....$$

$$M = Hola\ Mundo\ ++\ x$$

El objetivo es encontrar x tal que $H(Hola\ Mundo\ ++\ x) = 000....$

Dado que las funciones hash son pseudoaleatorias, no es posible derivar de manera lógica cual valor corresponde a x, por ende *la resolución al ejercicio computacional requiere ir probando valores* hasta encontrar el valor determinado. En este caso, utilizando una función hash simplificada, con una restricción de 3 a 7, se identifican las siguientes soluciones (marcadas en verde):

Texto Original	Nonce	M	h	Tiempo (segundos)	Restricción
Hola Mundo	0	Hola Mundo0	985cb35f0f789491dc00e600ab5792f6391b1220dca0791de1e1330cdccb71ea		
Hola Mundo	1	Hola Mundo1	3971a7418d11536a77ec58bff49c91fe69c6697266460bfaabc9dc7467323ef5		
Hola Mundo	2	Hola Mundo2	e135e55eba7e7bd1874aa254f234939afd43b6c8e012822af5dd61ac33a53828		
Hola Mundo	3	Hola Mundo3	b3d8679669bacfb4a41106425736f52e030e37733df540b1e6178f3fc2a2f80d		
...					
Hola Mundo	1198	Hola Mundo1198	**000**c4766b5f065749824e501f3bf1afe91088ff78af17afa1538e217d5ee0766	0.0057259	3 (tres ceros)
...					
...					
Hola Mundo	41641	Hola Mundo41641	**0000**3c153b578793dadef5413b67d5416708805a527c1acf4548956bcba47b4c	0.2014642	4 (cuatro ceros)
...					
...					
Hola Mundo	469110	Hola Mundo469110	**00000**8879e84a0aaede36631cfc84a307d32da61c84be2b93a05375cd4f7c85d	2.3373811	5 (cinco ceros)
...					
...					
Hola Mundo	23952407	Hola Mundo23952407	**000000**7730e8c956162bcb5ab69fddb22812edfa83dc73828f5848024b11069b	121.51289	6 (seis ceros)
...					
...					
Hola Mundo	224334166	Hola Mundo224334166	**0000000**63be8b39ab47ba0d10d9b06bd078ee0e9947fcc12cc8ff0edda9dc73e	1007.938	7 (siete ceros)

Figura 2.3-3

Como se ve, a medida que la dificultad se incrementa, crecen de manera exponencial la cantidad de intentos necesarios y la cantidad de tiempo necesario para llegar a un resultado.[6]

Un atributo importante de las funciones hash es que conociendo M es fácil verificar el resultado h. Tomando los ejemplos de arriba, se puede verificar de manera veloz que el resultado es correcto para la solución con dificultad 7:[7]

$$h = H(M)$$

$$M = Hola\ Mundo224334166$$

$$h = 000000063be8b39ab47ba0d10d9b06bd078ee0e9947fcc12cc8ff0edda9dc73e$$

$$tiempo\ de\ procesamiento\ para\ verificar\ resultado = 0.000151157\ segundos$$

$$tiempo\ de\ procesamiento\ para\ encontrar\ resultado = 1000.99\ segundos$$

[6] El código en Python utilizado para calcular los valores está incluido en el anexo
[7] El código para la verificación de los valores hash está incluido en el anexo

Como se ve arriba, *una vez se conoce la solución, la verificación es más simple* y *requiere menor cantidad de procesamiento.*

Como se verá en más detalle más adelante, cl concepto de funciones hash tiene múltiples aplicaciones en Blockchain. Por un lado, se utiliza para verificar que información guardada en los registros compartidos no sea modificada. Esto se hace mediante la verificación de valores hash. Otra función, es la de utilizar la resolución de problemas hash como condición previa a la publicación de nuevos registros. Esto permite la generación de manera controlada, permitiendo tiempo para su verificación y validación. Por último, como se verá en la siguiente sección, la posibilidad de convertir valores a valores hash es una parte importante de las firmas digitales, un mecanismo criptográfico que asegura la seguridad de las transacciones en Blockchain.

2.4 Criptografía Asimétrica y Firmas Digitales

El área de la criptografía busca proteger información de acceso no autorizado. Mediante la utilización de una *clave de encriptación*, un bloque de texto puede ser *encriptado*, de manera tal que se genere un conjunto de información sinsentido (*texto cifrado*), pero que pueda ser reconvertido a su valor original mediante una llave que permita *descifrar* el texto cifrado.

En la criptografía *simétrica*, la misma clave de encriptado puede ser utilizada para descifrar la información.

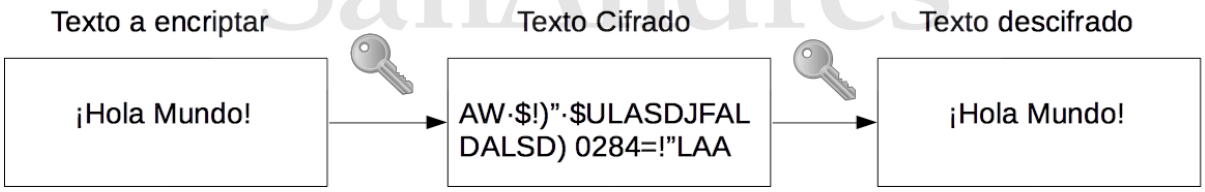

Figura 2.4-1: En la criptografía simétrica, la misma clave sirve para encriptar y descifrar la información

El riesgo de la criptografía simétrica es que la clave de encriptación debe ser compartida con el receptor del mensaje, lo cual genera riesgos en caso de que alguien la intercepte y pueda generar mensajes encriptados también.

En la *criptografía asimétrica*, sin embargo, se utilizan *dos llaves complementarias*, para encriptar y descifrar el texto cifrado.

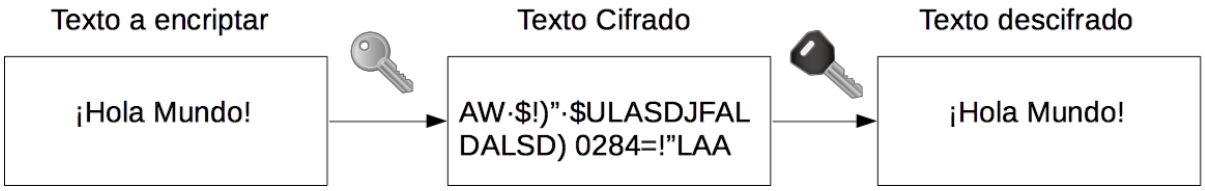

Figura 2.4-2: En la criptografía asimétrica, se utilizan claves complementarias para encriptar y descifrar la información

Esto permite mantener las claves separadas, proveyendo al sistema de mayor seguridad.

Además de ser utilizadas para proteger información de lectores no autorizados, las técnicas de criptografía asimétrica (y también las funciones hash) son de utilidad para la utilización de *firmas digitales*. Las firmas digitales son utilizadas para verificar que un documento ha sido firmado por la persona firmante y que no hubo modificaciones posteriores.

En las firmas digitales, el emisor utiliza su llave privada para encriptar el hash de un documento. Al mismo tiempo, incluye también el documento en su versión original. La persona que recibe el documento puede luego descifrar el texto cifrado usando la llave pública del emisor, y comparar el resultado con la ejecución del documento a través de la función hash. Si los valores son iguales, el documento no ha sido modificado.[8]

La utilización de criptografía asimétrica, y firmas digitales, se utiliza en Blockchain para *identificar participantes* de manera inequívoca (esto es, verificar que nadie se haga pasar por otro para recibir transacciones) y también para *autorizar transacciones* (que solamente el dueño de un activo pueda transferirlo).

2.5 ¿Cómo funciona Blockchain?

En la introducción a Blockchain, se definió a Blockchain como una suite de tecnología que permite integridad de transacciones entre pares, que consiste en bloques secuenciales en el tiempo con la información de transacciones, que además es seguro e inmutable. Luego se planteó una introducción a conceptos de arquitecturas de software distribuidas, funciones hash y criptografía asimétrica, prometiendo que estos conceptos eran relevantes para entender el funcionamiento de la tecnología. Es momento de explicar como estos conceptos interactúan y permiten la operación del sistema.

i. Estructura de Blockchain

[8] En el anexo se incluye un ejemplo gráfico que facilita el entendimiento de firmas digitales.

La información histórica de transacciones en Blockchain se registra en grupos denominados *bloques.* Cada bloque es parte de una cadena de bloques secuenciales, donde cada bloque contiene una referencia al bloque anterior. El objetivo es mantener un registro digital de interacción y transacciones entre pares, que sea inalterable en el tiempo, pero que pueda ser mantenido por todos los nodos, sin la necesidad de un centralizador.

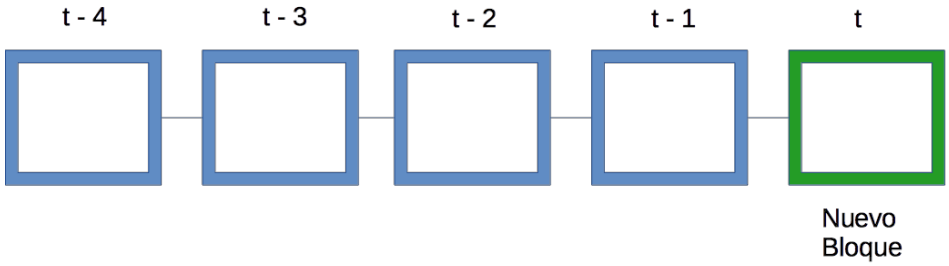

Figura 2.5-1: Cada nuevo bloque de transacciones se añade a la cadena existente

ii. Generación de Transacciones

Para participar, y generar transacciones (se define transacción como la transferencia de un activo a otro), cada nodo instala el software correspondiente, donde se conecta al resto de los participantes (dado que es un sistema P2P) y descarga un estado actualizado de los registros de transacción existentes.

Para poder generar transacciones con otros pares en la plataforma, necesita poder acceder a sus activos de manera personal. Para esto, se utilizan los mecanismos de criptografía asimétrica que fueron presentados anteriormente. En Blockchain, cada usuario, tiene una *llave privada* (utilizada para encriptar transacciones) *y una llave pública* (que sirve a modo de identidad y es visible para todos los participantes).

Cada vez que se ejecuta una transacción entre usuarios, ésta se encripta con la llave privada del nodo que envía la transacción (actuando efectivamente como una firma digital), y se publica al Blockchain con la llave pública del usuario que recibe la transacción.

Esto permite dos garantías de seguridad. Por un lado, al encriptar la información utilizando la llave privada del emisor de la transacción, cualquier otro nodo puede verificar la identidad del emisor utilizando la llave complementaria (llave pública) del emisor para comprobar que efectivamente esta llave descifra la información enviada. Esto actúa como validación de la firma digital y confirma que efectivamente, el emisor es quien dice ser. Por

otro lado, al requerir la llave privada para su encriptación, se asegura que solamente ese usuario puede utilizar los activos. Por ende aunque todo el mundo en la red pueda ver que los activos se están transfiriendo, no pueden utilizarlos. Solo los puede utilizar quien tenga la llave privada de la cuenta a la que se transfieren.[10]

iii. Validación de Transacciones

Cuando la transacción se publica, no se actualiza el registro distribuido inmediatamente. Como se señaló al describir las propiedades de las redes P2P, una de las mayores dificultades es poder actualizar todos los registros al mismo tiempo y asegurando que las transacciones sean correctas. Para poder lograr esto, Blockchain utiliza un mecanismo de *verificación por consenso* entre los nodos participantes para corroborar si las transacciones son correctas.

El objetivo del mecanismo de verificación por consenso es establecer un método en el que los nodos participantes, puedan verificar que las transacciones son correctas, al validar distintos aspectos de la operación. Por ejemplo, verificando que el emisor de la transacción efectivamente tenga los activos que dice tener. Esto es posible de hacer utilizando la llave pública del emisor, y verificando en el histórico de transacciones si adquirió el activo que quiere poder emitir.

Sin embargo no alcanza solamente con validar las transacciones, las transacciones luego deben ser agregadas al registro aceptado. Para agregar un registro a la cadena existente existen distintos mecanismos de validación y publicación de información, pero el más común es el denominado *Prueba de Trabajo*, que se mencionó previamente.

El objetivo de cada nodo validador es poder publicar este bloque de transacciones al final del último bloque activo, y hacer válidas las transacciones. Para poder hacer esto, cada nodo debe, además de validar que las transacciones sean correctas (esto es, verificar que el contenido sea consistente con los bloques anteriores), debe además resolver un problema hash.[11]

[10] Este mecanismo genera una situación interesante en el mundo Bitcoin. Dado que los registros son públicos, es visible para todo el mundo que el creador de Bitcoin, Satoshi Nakamoto, recibió (y minó) aproximadamente 1 millón de Bitcoin, valuados a alrededor de 6 mil millones USD. Sin embargo, Nakamoto desapareció de las redes, junto con su llave privada, por ende esos activos podrían no ser utilizados nunca.

[11] Una descripción más detallada del proceso de minería se describe en el Anexo.

Mientras este ejercicio corre para un nodo, se valida también que las transacciones hayan ocurrido correctamente (por ejemplo, que no estén duplicadas, y que el emisor tenga en su propiedad lo que quiere emitir). Los ejercicios de resolver el problema hash, y verificar la veracidad de las transacciones corren en paralelo. Una vez que algún nodo logra resolver el ejercicio computacional, y consigue la respuesta, puede agrupar todas las transacciones validadas y publicar los registros junto con la resolución computacional en un nuevo bloque, que se agrega a la cadena de bloques anteriores. Lo más importante en este momento, sin embargo, es que la resolución del ejercicio hash, se incluye en el nuevo bloque. Esto cumple dos objetivos: Por un lado, permite que otros nodos validen la respuesta y vea que sea válida. Lo segundo más importante, es que dado que el valor hash contiene la referencia al bloque anterior, crea una secuencia de registros, donde cada bloque esta inequívocamente relacionado con el bloque anterior.

iv. Publicación de Transacciones

Una vez encontrado el nuevo bloque (a este concepto se le llama informalmente "*minería de bloques*"), éste se publica y el resto de los usuarios pueden verificar que este bloque (y la solución propuesta) sea correcta. Este ejercicio de verificación es menos intenso computacionalmente, dado que una vez que se tenga la solución al problema, se puede verificar que sea correcta (como se detalló en la sección dedicada a funciones hash, conociendo M es fácil de verificar h). Al publicar el bloque, las transacciones quedan en el registro general. Una vez que existe un consenso, en que ésta es la solución correcta, los nodos suman ese bloque a sus registros, y deciden resolver el próxima problema para poder minar el próximo bloque.

Es importante aclarar que el problema computacional, busca dos objetivos: Por un lado, busca demorar el ingreso de nuevos bloques, para permitir un crecimiento orgánico, y permite que le resto de los nodos tenga tiempo para verificar la solución antes de que demasiados bloques se hayan sumado a la cadena. Para poder moderar la velocidad de creación de bloques a medida que el poder de procesamiento computacional de cada nodo crece por mejoras tecnológicas, el ejercicio computacional puede hacerse más difícil mediante restricciones adicionales, para mantener estable el crecimiento de la cadena. El otro objetivo de la generación de costos computacionales es que hace que la modificación de algún bloque ya publicado sea costoso para cualquier nodo malicioso, de manera tal que actúa como un mecanismo que desincentiva a participantes deshonestos. Esto se ve en la sección que describe la inmutabilidad de los registros en la cadena.

v. Inmutabilidad de la cadena de Bloques

Una vez consensuada la cadena de registros, el total de bloques contiene la totalidad de todas las transacciones ejecutadas, dado que cada bloque contiene registro de las transacciones validadas, pero también tiene un valor hash creado con la información de su bloque anterior.

Como cada bloque contiene un registro digital de los registros previos, corromper (o falsificar) transacciones en un bloque anterior involucra tener que corromper o falsificar los bloques posteriores para volver a generar su valor hash. Volviendo al concepto de hash y la solución verificable, es simple para cualquier nodo verificar que la cadena relacional no se haya corrompido, pero al mismo tiempo, volver a generar la relación y el valor hash correcto para valores corruptos es un ejercicio complejo, por ende, cuanto más atrás en la cadena se quieran modificar los datos, mayor cantidad de costo computacional es necesario para hacerlo. El costo se hace cada vez más alto y resulta un mecanismo detractor para cualquier nodo deshonesto que quiera modificar los registros.

2.6 Propiedades de Blockchain

Habiendo descripto a nivel general cómo funciona en la práctica un registro mayor descentralizado con la tecnología de Blockchain, cabe aclarar que hay múltiples aplicaciones de esta tecnología, que difieren en algunos aspectos.

Xu, et al (2017), sugieren cinco propiedades fundamentales de Blockchain: Debido al esfuerzo requerido para modificar bloques previos, afectando a los registros de transacciones, es *inmutable.* Gracias a los mecanismo de criptografía asimétrica, un nodo emisor no puede negar de manera creíble que haya firmado una transacción, por ende es *no-repudiable.* Los Blockchain tienen *integridad* debido a que los mecanismos de validación están instalados en la lógica del software, que mantienen integridad a nivel transacción y por ende a nivel histórico, y tiene un mecanismo de incentivos para mantener esta integridad. El acceso de todos los nodos a las transacciones provee *transparencia* al sistema, y el sistema P2P permite *igualdad de permisos* entre los nodos participantes.

Drescher (2017) también busca definir propiedades de Blockchain, y separa en propiedades funcionales (lo que la tecnología busca hacer) y los no-funcionales (los aspectos que permiten que se alcancen las propiedades funcionales). Define propiedades funcionales que son la *clarificación de la propiedad*: quién es dueño de qué y en qué momento, y la *transferencia de propiedad*. Para lograr esto tiene las propiedades no-funcionales de *disponibilidad,* dado que no tiene interrupciones. Es *incensurable,* ya que no hay un individuo

que pueda apagar el sistema. *Confiabilidad,* dado que si el mecanismo funciona, no hay errores. Es *abierto* dado que todos los participantes pueden interactuar. Es *pseudónimo,* dado que identifica a sus participantes pero no revela su identidad real. Es *seguro* a nivel transacción y a nivel sistema, gracias a los mecanismos criptográficos y de hashing. Es *resiliente*, dado que puede soportar cierto grado de ataques de nodos maliciosos. Según el autor, los registros históricos son *eventualmente consistentes* una vez que los participantes logran un consenso en el registro establecido, y *mantiene integridad* gracias a su modelo de seguridad a nivel transacción, bloque y sus lógica empotrada en el software.

Más adelante en este trabajo se utilizarán estos conceptos para entender como un sistema con estas características puede afectar la manera de interactuar entre agentes en una economía.

2.7 Activos, Criptomonedas e Incentivos

Una de las maneras de generar incentivos para la participación en una red de Blockchain, es la generación de *activos*.

Una manera de emitir estos activos es durante la generación de bloques. Cada vez que un nodo encuentra un nuevo bloque de transacciones, se le recompensa con una cantidad determinada de la *criptomoneda o "token"* que es particular a la plataforma, por ejemplo, Bitcoin. Este activo se utiliza para operar en la plataforma, y consumir los servicios que se ofrezcan en la red.

Distintos Blockchain tienen distintas reglas acerca de cómo adjudicarse los activos. Los mecanismos de validación, emisión de activos, y cómo asignar votos al mecanismo de consenso son únicos para cada plataforma, y están definidos en la capa de lógica del sistema en sí. Algunos Blockchain no utilizan activos, otros tienen una cantidad máxima de activos que emiten, y otros donde el sistema de asignación de activos es distinto. Cada Blockchain contiene sus propios parámetros y reglas, que actúan como incentivos para que los participantes elijan ese sistema, y participen en su mantenimiento.

Catallini y Gans (2017) sugieren que Blockchain reduce los costos de networking y adopción que se notan en dos etapas:

i. Bootstrapping

Al comienzo de la existencia de un Blockchain, hay pocos participantes, y por ende el incentivo a participantes de adoptar la tecnología viene de la expectativa de que al utilizarse

más, van a poder derivar mayor valor de utilizarla (esto es, como método alternativo a alguno existente, o por el alza de valor del activo inherente al Blockchain).

Para financiar estos proyectos públicos, se suele recurrir a una subasta inicial de activos llamada *ICO (Initial Coin Offering).* De esta manera se asignan los primeros activos, que luego son comúnmente utilizados para interactuar en la plataforma. Esto genera financiación, además de sumar participación en la red, y evita costos adicionales de los métodos más tradicionales de financiación (Adhami, Giudici, Martinazzi, 2018). Según el sitio coinschedule.com, en el 2017 se recaudó un total de 6.3 billones de dólares mediante estas subastas[12]. Este año, ese mismo monto se había recaudado ya en abril (a comienzos de octubre el monto total es de 20 billones de dólares)[13].

Sin embargo dada la laxa o nula regulación existente para las criptomonedas, existe un riesgo de que la operación y el proyecto no se completen, ya sea por alguna falla, o porque el proyecto sea un engaño (o sea percibido por los inversores como un engaño) (Adhami et al, 2018)

ii. Operación

En esta etapa, los usuarios eligen participar de la red, en busca de incentivos para mejorar sus negocios o reducir costos de transacción existentes. Además, al permitir un proceso donde no hay incentivo a centralizar información, las barreras de entrada se hacen menores y esto hace más fácil la adopción de una tecnología a medida que más usuarios se involucren.

Catallini et al (2017) también sugieren que aquellos nodos que participen de la minería (o sea, el proceso de agregar más bloques a la cadena) tienen el incentivo de hacerlo siempre y cuando la recompensa por hacerlo, la moneda, sea mayor al costo de encontrarlo (costo computacional o electricidad). Al mismo tiempo, los participantes en la cadena eligen participar siempre y cuando la integridad de los registros se mantenga intacta. A medida que la cantidad de participantes crece, y la cantidad de bloques crece, el esfuerzo y costo computacional de modificar bloques anteriores crece, y hace más costoso querer aprovecharse del sistema. Por ende a mayor participación y a mayor cantidad de bloques creados, más estable

[12] "Coinschedule - Cryptocurrency ICO Statistics." Coinschedule.com, Coinschedule, https://www.coinschedule.com/stats.html?year=2017

[13] "Coinschedule - Cryptocurrency ICO Statistics." Coinschedule.com, Coinschedule, https://www.coinschedule.com/stats.html?year=2018

es el sistema y mejor la integridad, incentivando a más usuarios a seguir participando de la plataforma.

Relacionado a los incentivos de los participantes a operar en una red de Blockchain, es el concepto de *bifurcaciones* (fork en inglés). Dado que el código de los Blockchain públicos es de código abierto, es de visualización para todos los participantes. En algunos casos, si una mayoría de los participantes decide armar un Blockchain nuevo, con nuevas reglas, puede copiar los registros a una nueva cadena, y operar bajo un protocolo nuevo. La ventaja, en estos casos, es que los activos y el registro histórico se mantienen sin costos de transferencia.

Abadi y Brunnermeier (2018) prepararon un modelo de teoría de juegos en el que buscan analizar los incentivos de los participantes a quedarse en un Blockchain o pasarse a uno nuevo, y concluyen que dado los costos reducidos de cambiarse, los creadores de un Blockchain públicos se ven incentivados a armar reglas que sean beneficiosos para la mayoría de los participantes, en lugar de armar reglas que beneficien a unos pocos. En particular, la utilización de Blockchain permite evitar un escenario donde los participantes necesite mantenerse en un registro que no lo beneficie solamente porque es el único que tiene todas las transacciones históricas.

2.8 Contratos Inteligentes

Hasta aquí se mencionaron distintas funcionalidades que son parte de Blockchain, pero enfocados en la operación de transacciones entre dos partes. Las tecnologías de Blockchain permiten transacciones más complejas, que son programables en lo que se denominan "contratos inteligentes" (*Smart Contracts* en inglés).

Ethereum, una plataforma de Blockchain creada en 2013, fue creada específicamente con el objetivo de permitir un ecosistema digital autónomo en el que los participantes pueden preparar sus propios "contratos" (en realidad programas de reglas por eventos) de manera simple. Esto permite armar arquitecturas de procedimientos visibles y transparentes para todos los participantes, mediante el código utilizado para armar las transacciones.

Estos programas, permiten la ejecución en tiempo real de arreglos entre participantes, sin la necesidad de un ejecutor de la transacción. Los nodos de contratos inteligentes actúan como un nodo adicional, que contiene ciertos términos y condiciones programados en su lógica. Dos o más participantes pueden elegir interactuar entre sí y utilizar este contrato para ejecutar sus condiciones. Por ende utilizan ponen un monto de sus activos en el nodo del contrato inteligente, y el contrato se ejecuta de manera automática. Un ejemplo muy utilizado

para describir este funcionamiento es de las máquinas expendedoras, donde uno sabe exactamente lo que va a recibir una vez inserte el dinero correspondiente.

Estos programas funcionan con una lógica de programación simple, de "si esto entonces aquello" (IFTTT por sus siglas en inglés: "If this then that") y se ejecutan directamente cuando una de las condiciones se cumple. Como todas las partes entran a este contrato de común acuerdo, el programa se ejecuta directamente al interpretar que alguna de las condiciones se cumple, sin necesidad de que un tercero ingrese y obligue a una de las partes a ejecutar lo acordado. El programa siempre es visible para los participantes pero no puede ser modificado por ninguno, por ende actúa como un juez imparcial que solamente ejecuta el resultado cuando una de las condiciones definidas en su programa se cumple.

Un ejemplo simple es un sistema de apuestas, donde los participantes ponen su dinero en el contrato inteligente hasta que el juego sobre el que se apuesta se cumple. Una vez que hay un ganador, los activos se transfieren del nodo del contrato, al nodo ganador, sin que haya una autoridad central que distribuya el monto ni que se lleve un porcentaje de las ganancias. Otro ejemplo puede ser asignar dinero a una garantía. En general, cualquier transacción que tenga reglas claras y simples es candidata a ser programa en un contrato inteligente, reduciendo el costo administrativo o las tarifas adicionales de un intermediario. Una limitación de estos programas es que sólo pueden considerar contingencias conocidas, que puedan ser programadas en su lógica. Esto será útil de entender cuando se detallen los conceptos de contratos completos e incompletos en la teoría económica de costos de transacción.

2.9 Blockchain Públicos, Privados y de consorcio

En los ejemplos mencionados anteriormente, se habla de Blockchain públicos. Esto es, una red, donde los nodos no se conocen entre sí, y cualquier agente puede participar, generando transacciones, y viendo los registros de transacciones de todos los pares.

Sin embargo, existen variantes a este modelo, dependiendo de si todos los participantes pueden participar mediante la generación de transacciones (*permisos de escritura*) o si tienen disponibilidad a ver todos los registros históricos de la cadena (*permisos de lectura*).

En los *Blockchain de consorcio*, existe una restricción a los participantes en alguno de estos dos puntos. Por ejemplo, una red de logística de proveedores, competidores y reguladores puede tener distintos permisos para cada uno, donde los reguladores pueden ver todas las transacciones pero aquellos proveedores que son competidores entre sí no pueden ver las

transacciones hechas por otros proveedores. Esto es, tienen distintos permisos de escritura o de lectura dependiendo de su rol en la red.

Otro ejemplo son los Blockchain privados, que son redes que actúan dentro de una misma empresa.

Estos modelos esconden una tendencia a la centralización, dado que para poder participar en los Blockchain de consorcio, necesitan primero ser autorizados para ser parte de la red. Esta autorización en general está dada por un nodo o grupo de nodos, que todavía mantienen un poder adicional por poder elegir quienes participan y quienes no.

Al alejarse de las estructuras de Blockchain públicas, la utilización de activos y criptomonedas es menor. En su lugar, los incentivos a participar son la generación de información en redes que permita asegurarse mayores beneficios al interactuar con clientes, proveedores y socios, así como también reducir los costos de transmitir información entre participantes en una red logística. Abadi et al (2018) modelizan esta situación y sugieren que en Blockchain de consorcio, la menor competencia de otros Blockchain, y la menor posibilidad de la generación de una bifurcación, generan incentivos menores para que los creadores de reglas diseñen un modelo que beneficie a la mayoría de los participantes.

2.10 Consenso en Blockchain Privados y de Consorcio

Los mecanismos de consenso también difieren de los mecanismos públicos. Dado que los participantes tienen mayor conocimiento de sus pares en la red, no es necesario un consenso de voto mayoritario.

En su lugar, se definen nodos "validadores" confiables que son los que reciben las transacciones hechas por los pares, y las envían a nodos de contratos inteligentes para validar que las transacciones se hayan ejecutado correctamente. Una vez validadas, se añaden a la cadena.

Lo más importante a considerar en estos casos, es que aunque todas las transacciones existen en la red, no todas son visibles para todos los participantes en un principio. Cada nodo tiene visualización de ciertas transacciones, pero al confiar en el mecanismo de validación, puede confiar en que las transacciones son reales. Esto se logra mediante la utilización de canales de información, que permiten a cada nodo suscribirse a ciertas actualizaciones de registros, de manera tal que vean solo la información pertinente y para la cual tienen permisos.

Al tener menor cantidad de nodos validadores, y tener confianza en esos nodos, el esfuerzo de propagación y validación de los registros es más rápido que en los Blockchain públicos, lo cual permite mayor escalabilidad y uso empresarial. En particular, los sistemas que regulan los tiempos de validación de transacciones tales como prueba de trabajo, dejan de ser necesarios al tener menos nodos desconocidos en la red. *Al requerir menos validaciones, la publicación de información es más rápida* y mayor cantidad de registros pueden ser añadidos a la cadena. Sin embargo, participar de una red de este tipo conlleva una decisión adicional, que es tener confianza en el resto de los nodos como aprobadores, y también en el organismo que diseña las reglas de la red (tales como las reglas de certificación). Al depender de las reglas de un organismo u organismo centrales, no hay un sistema completamente descentralizado, por ende algunas posibilidades de oportunismo todavía pueden existir.

2.11 Riesgos y Limitaciones

Blockchain, siendo una tecnología naciente, tiene todavía una serie de limitaciones, que deben ser superadas antes de que la tecnología pueda ser implementada de manera masiva.

Uno de los temas que se mencionaron previamente, es la velocidad de verificación de información. De la velocidad de verificación y validación depende que las transacciones efectivamente se confirmen. Dado que las transacciones se publican en bloques, el tiempo que tarde en minarse un bloque es el mínimo de tiempo que puede tardar en confirmarse una transacción. Sin embargo, las transacciones todavía pueden ser rechazadas en caso de que el bloque sea rechazado. Esto hace que las transacciones tomen tiempo en validarse. Además, la cantidad de transacciones en un bloque está definida por el tamaño del bloque permitido, así como también la cantidad de transacciones que pueden ser validadas en un tiempo específico.

Acorde a un reporte institucional de VISA, a agosto 2017 VISA tiene la capacidad de procesar más de 65 mil transacciones por segundo[27]. Al momento de escribir este trabajo, el promedio de transacciones por segundo de Bitcoin, en los últimos 180 días es de 2 transacciones[28], y el máximo histórico fue el 3 de enero de 2018 con 5 transacciones por segundo[29]. Distintos Blockchain buscan resolver esta limitación de distintas maneras, pero la

[27] https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

[28] https://www.blockchain.com/charts/n-transactions?timespan=180days

[29] https://www.blockchain.com/charts/n-transactions?timespan=all

escalabilidad sigue siendo un problema vigente. Sin embargo, la utilización de Blockchain de consorcio o públicos evita este problema, dado que no tiene las mismas necesidades de validación que los Blockchain públicos.

Otros de los puntos que suele mencionarse es que la minería (y en particular los protocolos de prueba de trabajo) consumen recursos energéticos de manera masiva. Al momento de escribir este trabajo (octubre 2018) se estima que el consumo estimado de electricidad de Bitcoin es de 73.12 TWh (Tera vatio-horas) que es mayor al consumo total de electricidad de Austria.[30] Un artículo publicado en The Economist en septiembre 2018 investiga que la mayoría de los servidores más grandes de pools de minería están ubicados en China, que produce energía pero no prioriza métodos ecológicos, por lo cual esto genera impacto adicional[31]. Este problema empeora al combinarlo con los problemas de escalabilidad de Blockchain.

Una rama de investigación que busca resolver el problema del consumo energético es la utilización de distintos algoritmos de consenso. Uno de los más utilizados es el mecanismo denominado Proof-of-Stake, que busca darle votos y prioridad de minería a aquellos nodos que depositan activos para ser nodos validadores. [32]Ethereum, por ejemplo utiliza este mecanismo.

Otro de los puntos a mejorar es la interoperabilidad entre distintos Blockchain. Dado que existen distintos Blockchain y cada uno mantiene su propios activos nativos, existe dificultad para transferir activos de un Blockchain a otro, dado que funcionan como un ecosistema propio. Por ende es necesario convertir estos activos a valor monetario fuera de la red de Blockchain y volver a adquirir activos en el nuevo Blockchain. Una de las soluciones que se está investigando es la posibilidad de utilizar *Sidechains* (Back et al 2014) que permitan un registro que funcione como interconector entre distintos Blockchain, sin embargo requiere que los distintos Blockchain tengan protocolos distintos y existe competencia entre estos Sidechains.

Dado el mecanismo de los Blockchain públicos requiere un consenso de los nodos participantes, en caso de que alguna entidad logre controlar una mayoría de los nodos, se corre el riesgo de que este nodo control efectivamente los registros de la cadena. A esto se lo

[30] https://digiconomist.net/bitcoin-energy-consumption#validation

[31] (2018, Septiembre). A Voracious Apetite. *The Economist – Techonology Quarterly*, Volumen 428 Número 9107 p. 8

[32] Ethereum. "Ethereum/Wiki." *GitHub*, github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake.

denomina un *ataque de 51%* . El riesgo es más alto cuanto menor sea el tamaño de la red, y cuanto más poder computacional controlen los servidores de minería.

Otro problema que existe es común a muchos sistemas de información, y es la dificultad de ingresar información correcta en un sistema. Si la información que se ingresa es incorrecta, cualquier proceso que se base en esa información traerá resultados que no tienen utilidad. A este problema se lo llama "GIGO" (por sus siglas en inglés: "Garbage In, Garbage Out"). Una de las maneras que se busca resolver esto, es mediante la utilización de sensores IoT, que sirven para capturar información sin la necesidad de un usuario que ingrese la información manualmente. Sin embargo, existe un costo adicional, e implica que cada dato debe tener sensores determinados, por ende es difícil de escalar. Al mismo tiempo, confiar en estos dispositivos involucra confiar en el organismo que instala o monitorea los artefactos, por ende involucra resignar cierto grado de control.

Por último, se cita frecuentemente la dificultad de regulación en el área. En particular con las criptomonedas tales como Bitcoin, los gobiernos identifican situaciones que hace que Blockchain sea considerado un sistema lo suficientemente distintivo, como para que las leyes actuales alcancen para regular el mercado. También, dada su naturaleza descentralizada, se hace difícil ejecutar cualquier tipo de condición sobre la plataforma, dado que no existe un único punto de falla. Dada esta situación, una de las áreas que suele ser objetivo de regulación, son los intermediarios que convierten moneda real, en criptomonedas (comúnmente llamadas "billeteras virtuales"). Sin embargo, al haber regulaciones en ciertas jurisdicciones, las empresas que empujan los proyectos de Blockchain o billeteras virtuales se mueven a jurisdicciones con menor regulación (Böhme et al 2015). Un ejemplo concreto es la ciudad de Zug, en Suiza, comúnmente llamado el "Cripto Valle", donde, según un reporte de la revista The Economist, se albergan 4 de los 10 ICO más de mayor valor en el año 201733. Böhme et al (2015) sugieren, que dada esta posibilidad de arbitraje entre jurisdicciones, una potencial solución es definir reglas globales de regulación.

[33] Tales from the crypto-nation. (2018, February 24). *The Economist*, *426*(9080), 65-65.

3. Costos de transacción

3.1 Nueva Economía Institucional

Mediante su arquitectura distribuida, Blockchain busca articular una manera de poder ejecutar transacciones sin que un intermediario asegure su funcionamiento. Nakamoto (2008) hace referencia al concepto de *costos de transacción* al sugerir que al generar pagos mediante intermediarios, se incurre en costos adicionales para poder mediar disputas. Sin embargo, antes de que Nakamoto diseñara este sistema, el estudio de costos de transacción había comenzado en la economía.

Uno de los objetivos de este trabajo es enmarcar el funcionamiento de Blockchain y sus posibilidades dentro de la teoría económica. Para lograr esto se busca encontrar un modelo que pueda ser actualizado con los recientes avances en Blockchain. Este trabajo sugiere que la literatura de la Nueva Economía Institucional (NIE por sus siglas en inglés), provee este marco teórico necesario, dado que estudia los distintos factores que afectan los modos en los que agentes económicos interactúan entre sí.

En su artículo pionero de 1937, *The Nature of the Firm,* el laureado economista Ronald Coase plantea la necesidad de entender por qué en una economía, las empresas surgen como centralizadoras de transacciones en lugar de permitir la libre interacción mediante el mecanismo de precios. Según Coase, esto era necesario dado que la teoría económica establecida en ese momento no planteaba una definición de las empresas que se asemejara a la realidad.

Coase (1998), sugiere que el término NIE fue utilizado por primera vez por Oliver Williamson, en búsqueda de establecer este nuevo foco en el análisis de la economía real como una rama de investigación que buscara volver a analizar casos concretos de mercado, en lugar de la abstracción teórica más común en ese momento.

Según Williamson (2000) la NIE propone cambiar el foco de análisis de la microeconomía de un análisis centrado en la elección entre recursos limitados, para presentar un nuevo foco en el cual el objetivo de estudio es el sistema económico en sí. El autor sugiere que hay dos ramas de investigación relevantes: el ambiente institucional a nivel formal e informal (las reglas de juego), y las estructuras de governance tales como mercado, empresas y consorcios. Williamson sugiere que el análisis de costos de transacción presentado originalmente por Ronald Coase se enfoca en el segundo nivel.

Según Williamson (2000) esta rama de estudio tuvo múltiples dificultades para ser aceptada, dado que difiere con el estudio ortodoxo en varios puntos: (1) propone el análisis de la empresa no solamente como una curva de producción tecnológica, sino que también incorpora las formas organizacionales y contractuales; (2) define los contratos como fundamentalmente incompletos (la teoría neoclásica asume que todos los agentes conocen todas las contingencias); y (3) analiza la organización en un mercado, donde el análisis ortodoxo analizaba los mercados de manera descentralizada y enfocaba el análisis en las decisiones de los agentes económicos individuales.

Coase (1937) sugiere que si las empresas eligen agruparse verticalmente, entonces participar del mecanismo de precios implica incurrir en costos que son mejor internalizados por un organismo centralizador. Coase argumenta que una empresa absorberá mayor cantidad de transacciones cuando (1) los costos son reducidos o crecen de manera no proporcional con la cantidad de transacciones, (2) a medida que la empresa es más eficiente y comete menos errores, (3) los costos de producción sean menores para empresas grandes; y a medida que la empresa internalice mayor cantidad de transacciones, su tamaño crecerá.

El estudio de la economía de costos de transacción luego profundiza estas ideas, al buscar formalizar las estructuras más eficientes para internalizar los costos de transacción, analizando las propiedades de las transacciones en sí y el marco regulatorio (instituciones) disponibles para posibilitar las transacciones.

3.2 Costos de Transacción

Como se mencionó previamente, Coase (1937) presentó un análisis inicial acerca del funcionamiento de las empresas, planteando la existencia de costos que se materializan al hacer transacciones bajo un sistema de precios. A estos costos se los denomina comúnmente *costos de transacción*. Dada la existencia de estos costos, puede ser beneficioso para alguna de las partes en elegir un modo alternativo de llevar a cabo esta transacción que le permita reducir estos costos y substituirlos por otros menores. Coase menciona costos tales como el costo involucrado en identificar los precios relativos para poder participar del mercado y el esfuerzo que requiere el armado y ejecución de contratos.

El enfoque de análisis de costos de transacción, como su nombre indica, analiza a la transacción como unidad de actividad. Williamson (1981) propone que el objetivo del área es encontrar estructuras de organización que reduzcan los costos de intercambiar bienes y

servicios, considerando las limitaciones existentes. Dentro de estas limitaciones existentes, hay algunas que conviene analizar en detalle.

Según Williamson (1998, 2000) el enfoque de costos de transacción acentúa tres propiedades del comportamiento de los participantes en una economía: (1) su habilidad cognitiva, (2) su interés en su beneficio personal y (3) su capacidad de mirar al futuro. Estas tres propiedades se agrupan bajo el supuesto de racionalidad limitada, que aplicado a la economía, sugiere que los agentes económicos tienen la intención de actuar de manera racional (y buscando beneficio propio) dada la información que poseen.

Williamson sugiere que la economía de costos de transacción suscribe en particular al supuesto de racionalidad limitada en su estudio de contratos. Dado que los participantes en una transacción no pueden conocer de antemano todas las contingencias, necesitan recurrir a definir contratos incompletos (o sea, que no consideran todas las contingencias posibles) para poder intercambiar.

De aquí sale otro concepto importante, que es el oportunismo. Dado que hay contratos incompletos, los agentes pueden aprovechar información asimétrica acerca de las transacciones para apropiar beneficios en detrimento del otro. Esto es una fuente importante de fricción y de costos adicionales a la transacción.

Dado este escenario de potencial oportunismo, y bajo los supuestos de racionalidad limitada, Williamson sugiere que el foco de la economía de costos de transacción es identificar estructuras óptimas de governance, que, sujeto a las características de las transacciones que busca agrupar, permitan atenuar las posibilidades de oportunismo, reduciendo los costos de transacción. Para esto, es necesario analizar cuales son las estructuras organizacionales posibles, sus propiedades, e identificar las más apropiadas para cada tipo de transacción.

3.3 Estructuras de organización

Williamson (1991) sugiere un análisis comparativo discreto, que difiere de los análisis de equilibro a través de variables continuas. El autor sugiere distintas formas organizacionales, que tienen distintas modalidad de ejecución y atributos, que están mejor adaptadas a cierto tipo de transacciones.

Los atributos que Williamson utiliza para identificar las estructuras posibles son (1) el grado de autonomía para ajustar precios acorde a la oferta y demanda, (2) el grado de coordinación y velocidad que se puede lograr entre agentes para definir una acción concreta y

eficiente, (3) intensidad de incentivos y posibilidad de renta para ajustarse rápidamente, (4) la cantidad de controles administrativos y costos internos, que en general atentan contra la posibilidad de capturar incentivos, y (5) como organizan y ejecutan sus contratos.

Esta definición de atributos le permite al autor definir tres tipos de organización para analizar transacciones:

Estructuras de Mercado

Por un lado, existe el sistema de mercado descentralizado, que organiza transacciones mediante los mecanismos de oferta y demanda, y utiliza el sistema de precios para auto-regularse. En estos casos los participantes no necesitan ingresar en contratos particulares entre sí, sino que se rigen bajo sistemas de contratos clásicos con reglas claras preestablecidas. Los participantes no pueden tomar su experiencia propia para evitar oportunismo de las otras partes, pero tienen posibilidades de elegir distintas alternativas para salvaguardarse de ser víctimas de oportunismos. La identidad de las partes no es relevante para la transacción porque al no existir una relación beneficiosa a largo plazo (dada la poca especificidad de los activos que se intercambian), la relación en sí no está valuada por los participantes (Williamson 1979).

La autonomía dada por la posibilidad de actuar sin dependencias con otros ni bajo procesos administrativos costosos, le da al agente participante del mercado descentralizado mayores incentivos a ajustar rápidamente sus precios acorde a shocks de demanda, dada la posibilidad de capturar rentas adicionales en un mercado competitivo (grado de intensidad de incentivos altas).

Según Williamson, cuando las transacciones se rigen por el mercado, el marco contractual que asegura que las condiciones se cumplan es la teoría de contratos clásica, donde las reglas son establecidas previamente y las reglas claras y formales prevalecen sobre interpretaciones posteriores. Dado este foco en formalidad, se evita la participación de terceros que hagan de intermediarios en las disputas.

Estructuras Jerárquicas

En el otro extremo del espectro, se encuentran las estructuras jerárquicas o empresas que habían sido punto de partida para Coase en 1937. Coase sugería que una empresa era un sistema en el que la dirección de los recursos estaba dada por el emprendedor (Coase 1937). Sin embargo no aclara qué tipo de transacciones afectan la decisión de organizarse como empresa, sino que sugiere que la empresa surge para reducir los costos adicionales que aparecen al querer interactuar en un sistema descentralizado.

Williamson sugiere que en estos casos, dado que el costo de definir contratos para las interacciones es más alto, resulta más conveniente integrar estas transacciones dentro de una misma empresa que permita reducir el costo adicional de cada nuevo contrato. Williamson (1991) sugiere que a medida que existen más riesgos y se arma una mayor dependencia bilateral, las oportunidades de generar mayores beneficios vía la integración vertical crecen. El autor sugiere que estas posibilidades de capturar renta se dan por una mayor posibilidad de coordinación y flexibilidad, dado que para cambiar modelos de producción o estrategias no es necesario reconvenir con otras empresas para redefinir condiciones contractuales.

Estructuras Híbridas

Williamson (1991) define las estructuras híbridas como aquellas que se sitúan entre los dos polos definidos previamente. Sin embargo, no define subcategorizaciones dentro de la clasificación genérica de híbrido. Según el autor, estos son estados transitivos en los que las organizaciones se sitúan temporalmente. En cuanto a sus características, Williamson las sitúa convenientemente en el medio, dotándolas de autonomía media, grados de coordinación intermedios y costos administrativos intermedios. Dentro de estas estructuras se pueden encontrar formas tales como las franquicias, sociedades, cooperativas, etc.

En formas de organización híbridas, los contratos se regulan mediante lo que Williamson define como marco contractual neoclásico. En estos casos, los contratos no pueden cubrir todas las contingencias posibles, por ende uno de los objetivos de las estructuras híbridas es mantener incentivos acordes para mantener el contrato funcionado, sin generar costos adicionales de renegociación. Dado que no se pueden considerar todas las contingencias, a este tipo de contratos se los denomina *contratos incompletos*.

La descripción propuesta por Williamson para las organizaciones híbridas fue considerada insuficiente por subsecuentes autores, dado que la evidencia empírica demostraba que las organizaciones híbridas no son transitivas, y también que dentro de la clasificación híbrida existe una gran heterogeneidad de maneras de organizarse. Ménard (2004) sugiere las organizaciones híbridas tienen múltiples factores en común que las hace especiales, en particular: (1) sus participantes comparten recursos, (2) utilizan contratos incompletos y (3) sus participantes se mantienen competidores entre sí.

Estos puntos son de particular importancia porque permiten identificar cuales son los problemas base que buscan resolver las estructuras híbridas y que genera tantas variantes de

estructura. Ménard (2004) sugiere que estos factores que las estructuras híbridas tienen en común generan cierto tipo de interrogantes únicas a las organizaciones de este tipo.

El compartir recursos genera una relación de dependencia entre las partes, lo cual implica el riesgo del oportunismo como también indicaba Williamson. En este escenario, generar un sistema de información compartida y elegir correctamente a los participantes en la organización es importante, de manera tal que se pueda mantener la relación a largo plazo de manera económicamente viable.

Este mismo problema se traslada al armado de contratos, dado que existe un beneficio de armar contratos para minimizar el beneficio de una acción oportunista, pero el sistema de información incompleta genera costos altos para poder mantener contratos completos. En estos casos las estructuras híbridas recurren a sistemas de contratos incompletos. Sin embargo en un contexto cambiante estos contratos pueden requerir múltiples renegociaciones. Esto genera que los contratos incompletos sean utilizados como marco, con contratos estandarizados, donde el problema a resolver sea la elección de una estructura híbrida tal que complemente a los contratos de manera tal de reducir los costos de transacción.

Que los participantes se mantengan competitivos y sean autónomos implica una extensión del concepto de racionalidad limitada. Los participantes mantendrán su participación dentro de una estructura organizativa híbrida siempre y cuando tengan ventajas de mantenerlo así. Ménard sugiere que las estructuras híbridas surgen en escenarios donde competidores eligen compartir recursos para minimizar el riesgo de incertidumbre, pero no necesariamente eligen actividades complementarias. Dado este escenario de incentivos, Ménard sugiere que la estructura elegida de governance puede ser inherentemente inestable si es que los participantes eligen cambiar. Por este motivo, y para coordinar y mantener la cooperación bajo los parámetros de competencia, elegir un organismo coordinador o centralizador pasa a ser una de las decisiones necesarias que definen el tipo de estructura híbrida conveniente.

Powell (1990) define estas estructuras como estructuras en red, y sugiere que son ideales en casos donde se necesita información eficiente y confiable, y ésta se consigue mediante la interacción con socios, clientes y proveedores con los que se interactuó en el pasado. En estos casos, la reciprocidad es un factor importante para mantener las relaciones a futuro, y para mantener beneficios mutuos entre participantes. Dada la necesidad de mantener estas relaciones, estas estructuras son más adeptas a la generación de confianza, que permite reducir la complejidad de las transacciones entre pares.

3.4 Estructuras Óptimas de Organización

Para encontrar la estructura óptima para cada tipo de transacción Williamson (1979, 1991) propone clasificar las transacciones acorde a tres condiciones: (1) la incertidumbre acerca de la transacción, (2) la frecuencia con la que las transacciones ocurren y (3) el grado en el cual ocurren inversiones en activos que son específicos a la naturaleza de la transacción.

El autor sugiere que cuanto menos frecuentes sean las transacciones, menos dependencia bilateral se genera entre las partes, por ende una organización más similar al mercado es necesaria. En cuanto a la especificidad de los activos, cuanto mayor sea la inversión necesaria para soportar cierto tipo de transacciones, sugiere que es mayor el costo de reasignar este activo en otras líneas de producción, y por ende existe una necesidad mayor de generar relaciones de dependencia contractuales para proteger los incentivos de las partes. En estos casos, cuanto más específica sea la inversión, Williamson sugiere que las estructuras jerárquicas permiten reducir los costos de transacción.

Para entender la dinámica de elección de estructura óptima Williamson (2000) propone partir de un mecanismo de mercado, donde los productos no son específicos y no se requieren resguardos adicionales a los proporcionados por el mercado. No hay definición de contratos entre las partes porque el comprador tiene la opción de ir a proveedores alternativos. Esto actúa como incentivo para las partes de cumplir con el arreglo.

A medida que aumentan la especificidad de activos, y el riesgo, surge la necesidad de armar contratos (incompletos) que reduzcan el beneficio de alguna de las partes de incumplir el arreglo. A medida que estos contratos se determinan, y la dependencia bilateral se establece, el sistema se aleja de un mecanismo de mercado, dado que requiere la participación de terceros para ejecutar los términos del acuerdo, situándose en un estado híbrido de mercado.

Dados suficientes incentivos para internalizar las transacciones, resulta más conveniente reemplazar los costos de transacción para internalizar las transacciones e invocar costos de administración, y agrupar y organizarse como empresa u organismo público, ejecutando contratos dentro de su misma estructura.

El siguiente modelo describe a niveles generales la interacción entre especificidad de activos y costos de transacción (Williamson 1991):

En este modelo, se definen los costos de transacción con las siguientes funciones:

$$M = M(k, \theta)$$

$$H = H(k, \theta)$$

$$X = X(k, \theta)$$

Donde *M, H, X* son los costos de transacción de una estructura de mercado, jerarquía e híbrido respectivamente. La variable k identifica la especificidad de activos, y el valor θ se utiliza para identificar una serie de parámetros que afectan los costos de transacción totales, que pueden ser factores tecnológicos o institucionales.

Williamson propone que M(0) < X(0) < H(0), lo que es decir que en condiciones donde el grado de especificidad del activo es nulo, los costos serán menores en el mercado y mayores en las estructuras de jerarquía (dada la existencia de costos administrativos). Además sugiere que la rapidez con la que se incrementan los costos a medida que la especificidad es mayor en el mercado y menor en las jerarquías, dado que en mercados el grado de coordinación es menor lo cual se traslada a mayores costos. El diagrama siguiente interpreta estas condiciones de manera gráfica:

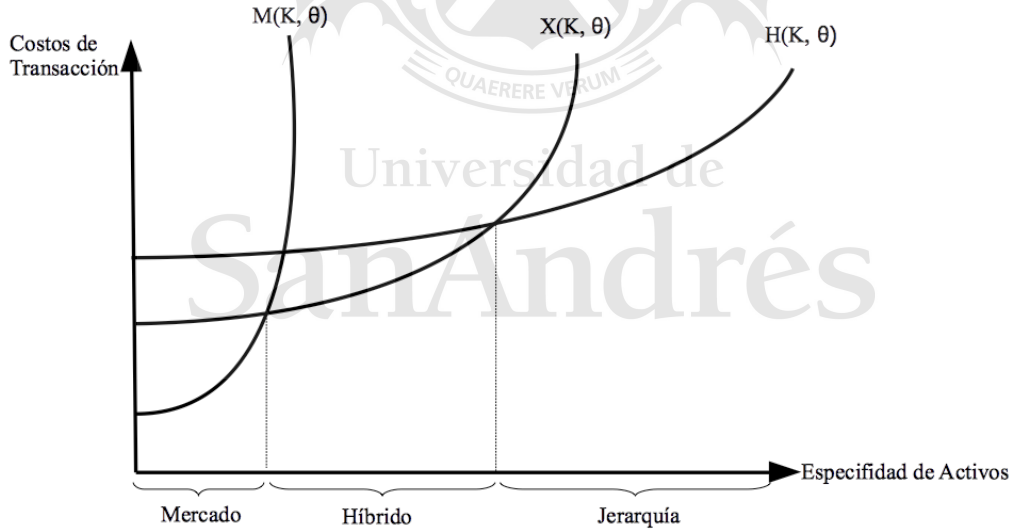

Figura 3.4-1

El análisis comparativo discreto que sugiere Williamson es identificar cómo la convergencia de estas estructuras se adapta cuando los parámetros de la variable θ cambian, por ejemplo distintos grados de apropiación de rentas, cambios estructurales en la manera de ejecutar contratos, o el grado de incertidumbre en el entorno analizado.

Tal como se describe en los párrafos anteriores, Williamson sugiere que la organización como empresa es una organización de última instancia cuando no hay otras alternativas posibles (o donde no sean convenientes). Sin embargo, Williamson no propone una definición concreta de qué tipo de organizaciones componen este estado híbrido, ni propone un mecanismo de convergencia que derive en la elección de estas organizaciones como mejores estructuras para coordinar transacciones.

Ménard (2004) critica esta conclusión y propone un análisis que sugiere distintos tipos de estructuras híbridas dependiendo de la naturaleza de las razones que lleva a los participantes a organizarse de manera cooperativa. Por un lado, los participantes en estructuras híbridas aceptan entablar una relación de dependencia entre sí dado que anticipan que pueden conseguir ventajas en compartir recursos e inversiones. Dependiendo del grado de interdependencia necesaria, existe mayor o menor posibilidad de oportunismo, donde en casos donde hay mayor riesgo de oportunismo, se requieren sistemas híbridos de mayor coordinación centralizada para asegurar que la relación se mantenga. En este escenario, donde se puede controlar con quien entablar relaciones, la elección de socios resulta importante. Otro argumento que propone Ménard es que los híbridos actúan como mitigadora de riesgo para los socios participantes. En aquellos casos donde hay mayor incertidumbre y la mitigación de riesgo es más importante como argumento para la formación de híbridos, la estructura ideal involucra un mayor grado de coordinación centralizada.

Definidos los argumentos que definen el grado de coordinación, Ménard argumenta que hay tres dimensiones que deben ser cubiertas por la estructura híbrida elegida: (1) reducir el grado de oportunismo dado un escenario de contratos incompletos, (2) asegurar que las rentas sean distribuidas de manera transparente, evitando que existan free-riders y (3) el armado de una autoridad de coordinación que permita decidir en casos de conflictos. En todas estas dimensiones el concepto de contratos incompletos actúa como marco, y la elección de socios confiables es de particular importancia.

4. Blockchain y costos de transacción

4.1 Literatura Existente

Mucha de la literatura existente sobre Blockchain pone su lupa en Bitcoin y las criptomonedas y su sistema de emisión controlada. Aquí se sugiere un análisis enfocado en Blockchain, pensado como tecnología que permite reducir la fricción en las transacciones.

Davidson, et al (2016) propone un primer acercamiento a este análisis. Los autores suscriben al análisis de costos de transacción y sugieren que Blockchain es una tecnología que impulsa la descentralización, mediante la eliminación de oportunismo al permitir transacciones en formato de mercado que permitan cumplir con una promesa a futuro de manera indefinida. Los autores toman el análisis de Williamson, acerca de la dicotomía de mercados y empresas, y concluyen que siempre y cuando las estructuras de governance existan para controlar el oportunismo, Blockchain puede reducir considerablemente los costos de transacción, sin embargo en los casos en los que las estructuras de governance existan por otras razones, el impacto será menor. Sin embargo, los autores sugieren que esta tecnología no apoya solamente las organizaciones óptimas tal como era la norma en la escuela de costos de transacción, sino que sugiere que Blockchain, tiene facultades que permiten que actúe como organización propia que compite con empresas y jerarquías. El argumento de los autores es que mediante la definición de normas, reglas de decisión y la introducción de una moneda dentro de la estructura, la plataforma actúa como una organización económica independiente.

En este artículo se busca us expandir este análisis al introducir un aspecto faltante en el análisis de Davidson et. Al, que son las estructuras híbridas y los Blockchain de consorcio o privado. En el análisis de los autores, las opciones son mercado, o empresa, pero como múltiples autores, incluyendo Williamson (1991) y luego Ménard (2004, 2012) sugieren, las organizaciones híbridas muchas veces predominan al analizar la evidencia empírica, y estas comparten múltiples similitudes con los Blockchain de consorcio.

4.2 Análisis Comparativo

Se propone entonces seguir la línea de investigación y analizar cómo la introducción de Blockchain impacta los incentivos y los mecanismos de las estructuras definidas dentro del análisis de costos de transacción, que son el mercado, las estructuras híbridas y las estructuras jerárquicas. En particular, se incorporarán las propiedades que se describieron de Blockchain,

y aquellas funcionalidades adicionales y se buscará entender cómo podrían afectar las estructuras de organización óptimas sugeridas por la literatura de costos de transacción.

Para analizar esto conviene volver al modelo semi-formal propuesto por Williamson (1991) en el que se definen costos de transacción como resultado de una función con parámetros k y θ, que eran la especifidad de activos y los parámetros externos, respectivamente.

Williamson define la intersección de las curvas de mercado e híbridas con el valor $\overline{k}_1$ y la intersección de híbridos y jerarquías con el valor $\overline{k}_2$. Dados los valores de θ, y dado el tipo de transacción, se encuentra el valor óptimo de k que es k^*. Cuando $k^* < \overline{k}_1$ entonces la estructura de organización sugerida es el mercado, y cuando el valor $k^* > \overline{k}_2$ la estructura sugerida es la jerarquía. En los valores intermedios tal que $\overline{k}_1 < k^* < \overline{k}_2$ la estructura óptima es la organización híbrida.

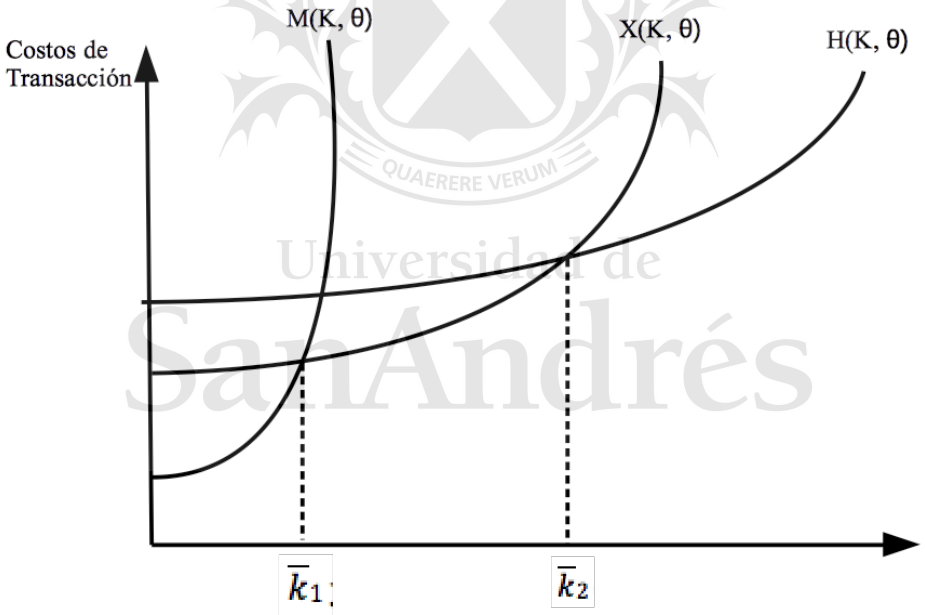

Figura 4.2-1

El análisis comparativo sugerido por Williamson es analizar cambios en los parámetros institucionales, para entender cómo las curvas de costos de transacción cambian para cada organización, para entender si los valores $\overline{k}_1$ y $\overline{k}_2$ cambian de alguna forma, afectando la estructura de organización óptima para valores de especificidad de activos dados (k^*).

En su modelo, Williamson sugiere acomodar las dos áreas de investigación de la economía de las instituciones. Por un lado el ambiente institucional, que establece las reglas de

juegos políticas y sociales que afectan el ecosistema en el que se ejecutan las transacciones, y por el otro lado, los arreglos institucionales que afectan el modo en el que los agentes económicos interactúan entre sí. Williamson analiza cuatro cambios de parámetro distintos: derechos de propiedad, el modo de derecho utilizado para ejecutar arreglos, efectos de reputación y la incertidumbre.

En este trabajo, se tomarán cada una de estas áreas, y suscribiendo al análisis de Williamson, pero tomando los progresos en el análisis de otros economistas en el análisis de costos de transacción, se analizará como Blockchain afecta la estructura de governance óptima para cada tipo de transacción.

4.3 Derechos de Propiedad

Williamson enfoca su análisis de derechos de propiedad en la seguridad de mantenerlos vigentes una vez asignados. En particular considera dos escenarios: (1) la posibilidad de que el gobierno reasigne los derechos de propiedad y (2) la posibilidad de que los derechos de propiedad sean expropiados por el proceso comercial en sí (proveedores, clientes, rivales).

Sobre el primer punto, la expropiación de parte del gobierno, el autor sugiere que ante un escenario donde hay una probabilidad creciente de que el gobierno expropie parte de las rentas de los agentes del mercado, los participantes van a elegir invertir menos en activos específicos y no específicos. Además, las inversiones se van a concentrar en áreas donde los activos se puedan reasignar en otros países. Su conclusión es que en caso de que haya posibilidades de expropiación de parte del gobierno, todas las estructuras de organización tienen costos de transacción más elevados, que incorporan dentro de sus curvas de costos, por ende los valores $\overline{k}_1$ y $\overline{k}_2$ no se ven afectados, por ende las preferencias de estructuras de organización óptimas tampoco cambian.

Si se inserta Blockchain en este análisis, hay varios matices a considerar. Por un lado, la utilización de Blockchain permite distribuir la información de manera de manera tal que se reducen los nodos centralizados de información traducidos en poder adicional. Además, en un sistema descentralizado los agentes pueden interactuar entre sí, sin necesidad de un permiso o intermediarios adicionales. Tomando el caso de Bitcoin, el uso de las criptomonedas quita poder regulatorio a los gobiernos dado que no hay un nodo central que se pueda ajustar en pos de un objetivo concreto, por ende el gobierno como agente centralizador pierde poder regulatorio.

Allen (2017) sugiere dos tipos de implementación de Blockchain en la economía con relación a la interacción con el gobierno: (1) una implementación dentro de las áreas empresariales, pero manteniendo las capas de protección de instituciones públicas (sistema legal, gobierno, etc.) y (2) una aplicación donde los agentes económicos salgan del sistema institucional existente para armar sus propias redes institucionales privadas, por ende actuando bajo un sistema separado de gobiernos, formando sus propias jurisdicciones.

El análisis se torna más complejo a medida que se analizan los distintos tipos de Blockchain que pueden aplicarse, en particular si se incorpora el escenario de las redes de consorcio, donde el mismo gobierno puede ser un agente que participe en la red.

Si uno considera un primer escenario, donde el gobierno introduce un sistema de derechos de propiedad regulado en un Blockchain, puede verse que las reglas de juego siguen definidas dentro de los parámetros definidos por el gobierno, pero, dado que el registro de información es público y descentralizado, se reduce el oportunismo potencial. Además, la posibilidad de tener públicos los registros reduce el poder centralizador de información que aprovecha el gobierno, reforzando los derechos de propiedad. Además, como beneficio positivo, mantiene un registro más estable, dadas las reglas de la plataforma, generando una reducción en la necesidad de requerir arbitrajes y costos administrativos para resolver disputas. La utilización de contratos inteligentes también reduce la carga administrativa en la validación de la información, reduciendo los costos. En estos casos, el gobierno igual se apropia de la potestad de poder autorizar activos y agentes para ser introducidos en la red, pero una vez allí permite la libre transacción reduciendo la intervención y asegurando transparencia. Dado que los agentes son validados previamente por el gobierno, se mantiene un cierto poder centralizador y arbitrario, pero reduce los costos de transacción de interactuar en la economía dado que el gobierno no necesita validar todas las transacciones, quitándole poder para apropiarse u obstaculizar las transacciones.

Dado que este sistema reduce las posibilidades de oportunismo y prioriza el mantenimiento de derechos de propiedad a mediano y largo plazo, se puede asumir que el impacto será menor en los tipos de transacciones con mayor especificidad de activos, que requieren mayor soporte legal y administrativo para ejecutarse. De manera complementaria, dado que hay menor riesgo de oportunismo de parte del gobierno, se ve que hay menor incentivo de las organizaciones de integrarse verticalmente para protegerse institucionalmente, por ende mirando las curvas originales se puede decir que hay mayor incentivo para organizarse de manera híbrida y mercados (Figura 4.3-1):

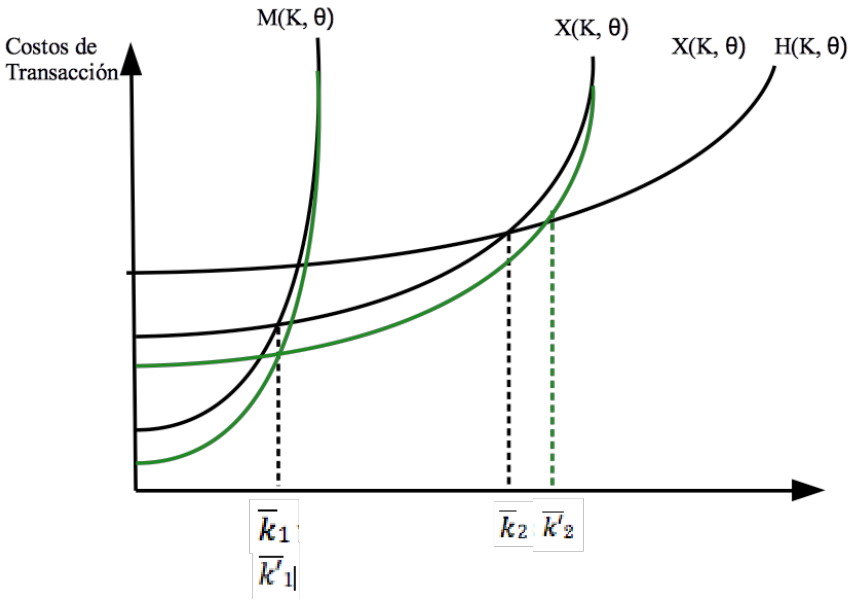

Figura 4.3-1

(Berg, Davidson, Potts 2018) proponen que la decisión del gobierno de incorporar inversión en tecnologías de Blockchain, dependerá de los retornos sociales que pueda conseguir de hacerlo comparado con el costo de hacerlo. Pero, dado que en este tipo de redes reguladas por el gobierno, será éste quien arme las reglas, la adopción de los participantes también dependerá de la confianza que tengan en la institución gubernamental.

Esto genera una alternativa que MacDonald (2015) denomina cripto-secesión, donde los agentes tienen la posibilidad de optar por excluirse de cierta parte de los servicios provistos por el gobierno, para organizarse en una red separada con su propia red de activos públicos, operada sobre Blockchain. Este escenario implica un riesgo nulo de expropiación gubernamental, dado que es un sistema descentralizado. En este escenario, Berg et al (2018) sugieren que ante un escenario donde haya un mayor riesgo de pérdida social mediante expropiación gubernamental existirá un mayor interés en los agentes en organizarse de manera separada, por ende armando sus propias jurisdicciones. A medida que la posibilidad de cripto-secesión sea mayor, entonces el gobierno necesita reducir su autoridad central para evitar perder rentas a los agentes que se salen de su jurisdicción. Volviendo al modelo de competencia entre Blockchain sugerido por Abadi et al (2018), si el Blockchain de consorcio tiene competencia con un Blockchain público, entonces los que armen las reglas del Blockchain de consorcio tendrá la necesidad de adaptar sus reglas para ser más atractivo para los participantes,

y no arriesgar que se salgan de la red. Esta competencia entre jurisdicciones también empuja los costos de transacción hacia abajo.

Con respecto a la posibilidad de que clientes o proveedores se adueñen de derechos de propiedad, Williamson (1991) sugiere que si las inversiones en conocimiento que generan rentas no pueden ser apropiadas de manera efectiva por el organismo que invirtió, entonces los incentivos a invertir ex ante se reducen, así como también se incrementa el incentivo a armar estructuras de governance que protejan estas inversiones, empujando la estructura óptima a una de mayor centralización, en detrimento de las estructuras de mercado e híbridos.

Ménard (2012) apoya esta idea al sugerir que los mecanismos de control necesarios para reducir los free-riders en una relación exceden los contratos incompletos, y requieren estructuras de control que pueden empujar las estructuras óptimas de mercado a unas de cuasi-integración. Ménard (2004) sugiere que hay distintos sistemas que pueden ayudar a reducir los riesgos de expropiación de cuasi rentas en estructuras híbridas: (1) la generación de reputación entre los agentes, (2) la existencia de formas de negociación y (3) la definición de una autoridad formal que pueda decidir ante cualquier disputa. Además, sugiere que reducir la información asimétrica entre participantes y elegir participantes correctamente para participar en la red son formas de reducir los costos de transacción en híbridos.

Debido a su esquema de registros inmutables, Blockchain provee una manera de listar las transacciones previas de cada participante en la red, ayudando a formar sistemas de reputación más transparentes y reforzando los derechos de propiedad dado que es un sistema que muestra el estado de los activos a través del tiempo de manera inmodificable. En un esquema de Blockchain de consorcio, un participante podría elegir mostrar todos sus registros previos con otros participantes a una entidad bancaria para poder acceder a un beneficio, de manera simple y transparente, dado que la entidad bancaria confía en el sistema de registros. Ménard (2012) sugiere que la reputación puede crecer viniendo de (1) transacciones recurrentes entre socios, (2) familiaridad entre participantes por compartir antecedentes en común, (3) la existencia de información acerca de transacciones con terceros y (4) el compartir redes en común que tengan normas de comportamiento específicas. La utilización de Blockchain facilita estos cuatro puntos, ayudando a los agentes a poder exponer su buen comportamiento de manera más transparente. Esto permite la generación de sociedades donde se requieren menos mecanismos de control adicionales. También debido al hecho de que los registros en una red pueden ser hechos públicos y son inmutables, el registro descentralizado de transacciones puede pasar a ser la base por la cual se reparten las cuasi-rentas en una sociedad. En particular

con la utilización de contratos inteligentes la necesidad de una autoridad formal que ejecute estas divisiones pasa a ser menos necesaria, reduciendo los costos de transacción.

Este apoyo tecnológico que permite una mejor distribución de derechos de propiedad en red ayuda a bajar los costos de transacción de las estructuras híbridas con relación a mercados y jerarquías, expresándose en una reducción en la curva de costos para híbridos, y generando un rango mayor de valores de $k*$ para los cuales una estructura híbrida puede resultar atractiva:

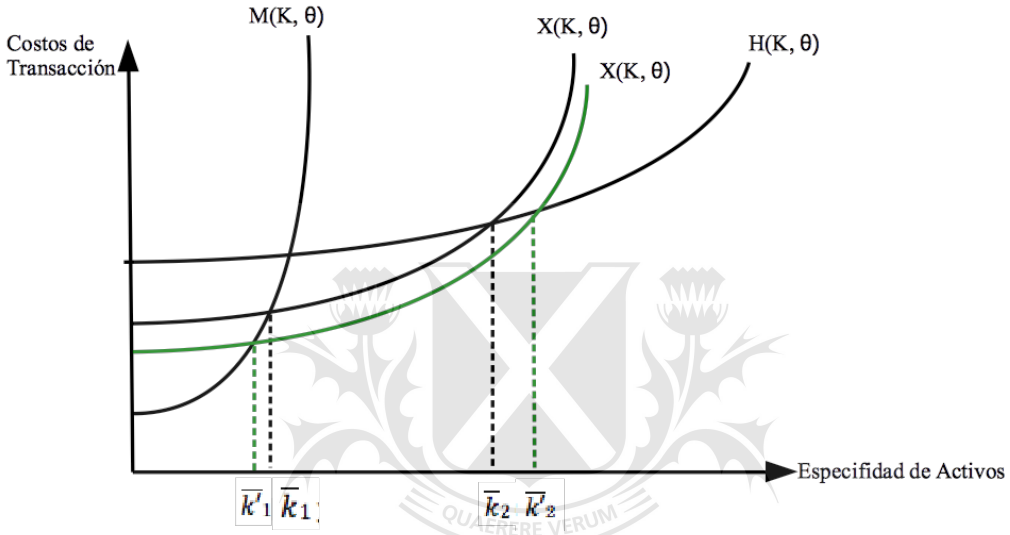

Figura 4.3-2

4.4 Ejecución de Contratos

En su análisis comparativo, Williamson (1991) sugiere que en caso de que haya cambios en doctrinas o maneras de ejecutar contratos, esto también impacta en los costos de transacción y los costos inherentes a las estructuras de organización.

Davidson et al (2017) sugieren que Blockchain es un mundo de contratos completos. Esto es porque los contratos inteligentes cubiertos en el código de la aplicación solamente cubren escenarios conocidos. Con respecto a esto, permiten la ejecución de cláusulas definidas sin intermediación de terceros, muy alineado con el concepto de teoría de contratos clásica que Williamson (1979) sugiere es la más utilizada en las estructuras de mercado, dado que depende de mecanismos formales y reglas autoejecutables. En este escenario se espera que el impacto de Blockchain no sea una reducción en costos de armado de contratos (ya que se asume que no los hay y las reglas formales son similares a las existentes en estructuras de mercado sin la tecnología) pero en su lugar se espera que la utilización de contratos inteligentes, (o la

imposibilidad de ejecutar una transacción ilegítima), reduzca el costo de ejecutar las condiciones del contrato en caso de que alguna de las partes no cumpla.

Con respecto a estructuras híbridas, que utilizan un sistema de contratos neoclásico (contratos incompletos) se espera que las partes más estandarizadas de los contratos también se ejecuten de manera más automatizada, pero dado que las relaciones contractuales abren todavía un abanico de contingencias que no pueden ser contempladas ex ante, la parte incompleta de los contratos no tendrá un beneficio claro con la utilización de Blockchain. Sin embargo, aquellas cláusulas que sí estén consideradas dentro del marco contractual que rige a las estructuras híbridas, podrán ser ejecutadas de manera autónoma e independiente, proveyendo aunque sea una mínima reducción de costos de ejecución de contratos.

En todo caso, el presente trabajo propone que la adopción de Blockchain impacta mayormente a la auto-ejecución de contratos completos en la interacción entre agentes, que es mayormente utilizada en estructuras de mercado. Como potencial resultado de esto, puede concluirse que la utilización de Blockchain sugiere una tendencia hacia la descentralización de transacciones dado que el valor $\overline{k'}_1$ se corre hacia la derecha, generando un escenario más favorable a las estructuras de mercado.

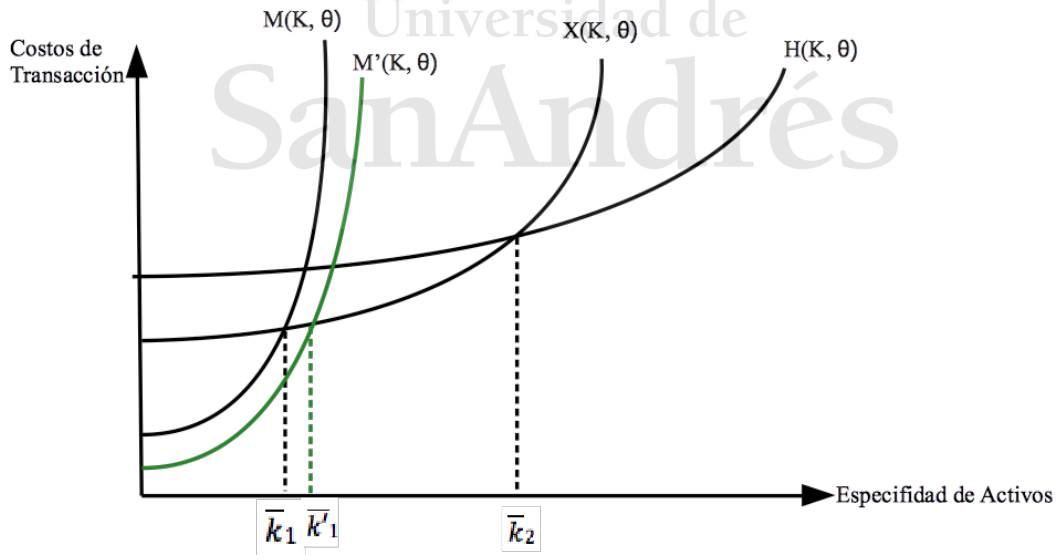

Figura 4.4-1

4.5 Efectos de Reputación

Al analizar los efectos de cambios en reputación en redes y organizaciones, Williamson sugiere analizar cuán rápido se pueden diseminar mejoras de reputación de un participante a otro. Bajo esta perspectiva, Williamson propone que una mejora de los efectos de reputación reduce los riesgos de oportunismo en interacciones entre empresas, por ende contribuye a una mejora de los costos inherentes a las estructuras híbridas. Ménard (2012) sugiere que la reputación es un componente importante para mantener las relaciones entre agentes en una organización híbrida, ayudando a cubrir las áreas que los contratos incompletos no pueden cubrir.

Como se mencionó previamente, el sistema de inmutabilidad y la protección de información, así como su carácter público, hace de Blockchain una manera transparente de promocionar la historia transaccional previa de una empresa. Ménard sugiere que este es uno de los parámetros más importantes para definir reputación. Esta publicación transparente del historial de transacciones hace de la reputación un atributo más medible, que puede luego ser incorporado dentro de los parámetros de elección de socios en estructuras híbridas, reduciendo la incertidumbre y permitiendo sociedades en situaciones donde las organizaciones habrían optado por estructuras jerárquicas.

Williamson (1991) también sugiere que en estructuras jerárquicas, las mejoras de reputación entre departamentos de una empresa reducen los costos transaccionales dado que reduce las oportunidades de oportunismo en transacciones intra-empresa. Blockchain apoya esta reducción de oportunismo dado que reduce la información asimétrica entre participantes, así como también reduce los costos de publicar esa información entre pares.

En cuanto a las estructuras de mercado, Blockchain permite la introducción de sistemas de reputación valuados por usuarios, que no son susceptibles a manipulación de nodos centralizados, por lo cual son más transparente

4.6 Incertidumbre

Williamson (1991) propone dos variantes al considerar el factor incertidumbre en el armado de estructuras organizacionales. Por un lado considera la frecuencia de los cambios que generan incertidumbre, y por el otro lado cuan fuerte es el impacto de cada shock. En ambos casos el autor sugiere que dado que los arreglos institucionales entre los socios de una estructura híbrida necesitan renegociar sus condiciones y llegar a un consenso mutuo, el trabajo extra de coordinación hace que a medida que el impacto o frecuencia de los shocks de

incertidumbre crecen, las estructuras híbridas serán menos favorecidas que las estructuras de mercado o jerarquías. Ménard (2004) tiene una opinión similar, aunque sugiere que en casos de mayor incertidumbre, se favorecerán estructuras híbridas con mayor grado de coordinación centralizada, tales como estructuras con un organismo de control estratégico, de manera tal de poder lidiar con los problemas de coordinación de manera más rápida. Esto también coincide con su opinión de que las estructuras híbridas y sus propiedades que le permiten compartir recursos entre participantes son justamente una herramienta o instrumento para lidiar con la incertidumbre por ende no es necesario alejarse de las estructuras híbridas sino ajustar los parámetros de coordinación inherentes a la estructura en sí (Ménard 2012).

Blockchain no puede reducir la frecuencia de los shocks externos, pero al permitir una difusión de información entre socios, facilita una coordinación un poco más rápida entre los participantes de una estructura híbrida, dado que reduce las ineficiencias de información asimétrica entre participantes (Davidson et al 2016).

4.7 Tipos de Blockchain vs estructuras de organización

Como se describió anteriormente, existen distintos tipos de Blockchain dependiendo de los tipos de participantes. Luego de analizar como Blockchain impacta los tipos de estructura óptima, este trabajo sugiere que existe un paralelismo entre éstos y las estructuras posibles.

Los Blockchain públicos proponen un sistema descentralizado, con participantes desconocidos y sin un organismo que defina reglas. Utilizan contratos completos, ejecutados por los nodos de contratos inteligentes. Los participantes pueden elegir formar parte de otros Blockchain en caso de que exista la competencia. Son transparentes y públicos y hay nula posibilidad de oportunismo entre las partes.

El presente trabajo sugiere que los Blockchain públicos surgen como un mecanismo de soporte en aquellos casos donde las transacciones son de especificidad menor (donde no es relevante la identidad de los participantes) y donde las reglas son claras para todos los participantes. Por ende el mecanismo de Blockchain público es un soporte tecnológico en aquellos casos donde las transacciones ya se organizan como mercado, y reducen los costos de transacción que provienen de intercambiar información entre los participantes, pero agrega también una mejora al no requerir un intermediario para evitar el oportunismo. Blockchain, por ende, facilita la existencia de estructuras de mercado con activos de un grado de especificidad mayor comparado a casos en los que Blockchain no se utilizara, compitiendo de cierta manera con las estructuras híbridas.

Los Blockchain de consorcio, funcionan y son ideales en estructuras donde los participantes se conocen pero no necesariamente confían del todo entre sí. La elección de participar en estas redes depende principalmente de la confianza en el organismo que presenta las reglas y convenciones a utilizar, y también en el beneficio que puedan capturar por compartir recursos para validar transacciones y mantener un registro compartido. En este caso se asemejan a las estructuras híbridas, e igual que éstas, pueden cubrir activos de mayor especificidad, donde es necesario algún organismo que pueda interceder en caso de que los contratos no cubran todas las contingencias. Aquí es donde el organismo u organismos centrales que definen las reglas pueden ir cambiando las reglas de validación acorde a lo que los participantes requieran. En particular se puede considerar que el beneficio mayor en estos casos es la existencia de un histórico de transacciones que permita transparencia al momento de establecer vínculos entre socios, y la reducción de esfuerzo en compartir información. Esta tecnología permite una mejor distribución de información entre participantes, y como tal permite que el oportunismo se reduzca. Blockchain, analizado como un mecanismo de soporte a las estructuras híbridas, permite manejar redes informativas y combinaciones de cooperación y competencia en escenarios donde normalmente las empresas elegirían proteger su rentabilidad integrándose de manera vertical.

Los Blockchain privados tienen menos literatura y casos de uso asociados hasta ahora, pero dado que implican un solo participante, pueden ser asemejados a las estructuras jerárquicas. En estos casos, los Blockchain privados permiten no necesariamente una reducción de costos de transacción, sino más bien una reducción en los costos burocráticos y administrativos de organizar la información dentro de una estructura jerárquica. Sin embargo, más allá de la eficiencia operativa que brindaría Blockchain como mecanismo de información, no es distinto a un sistema de información centralizada, y como tal no se puede concluir que un Blockchain privado provea un beneficio que permita que las estructuras jerárquicas se posicionen como preferibles a las otras estructuras posibles.

5. Blockchain y Agroindustria: Un ejemplo

5.1 Organización de la Agroindustria en Argentina

Un caso interesante de análisis de estructuras organizacionales de mercado es la industria agrícola en Argentina. Según Bisang et al (2008) en Argentina conviven dos escenarios: (1) un modelo de integración vertical donde el agricultor toma decisiones de producción, y (2) un modelo de organización en red donde los distintos agentes comparten recursos para disminuir el riesgo y aprovechar externalidades conjuntas.

Los modelos de integración vertical, que según el autor están disminuyendo, implican aprovechar economías de escala mediante la sistematización de la producción. En estos casos, el dueño de tierras toma decisiones acerca del paquete tecnológico a utilizar, y absorbe todo el riesgo, así como también las rentas disponibles. El autor observa que estas estructuras: (1) interactúan de manera limitada con el resto de la economía al no utilizar servicios ni subcontratar insumos, (2) tienen necesidades medias de capital para operar pero al incorporar maquinaria tienen requerimientos altos para incorporar capital fijo, (3) tienen estructuras de costo internas y (4) mantienen las rentas dentro de la organización que produce.

A partir de la década del 90, el modelo de producción agrícola en Argentina muta a uno que Bisang et al (2008) denomina *esquema de organización en red*. EL autor sugiere que en este modelo, se desdoblan los roles de los participantes en la cadena de valor agroindustrial y tiene las siguientes características: (1) existen múltiples beneficiarios de las actividades agrícolas, no sólo los dueños de tierras, (2) existen empresas que subcontratan insumos y servicios, (3) éstos proveedores de insumos y servicios cobran mayor relevancia, (4) los contratos toman mayor vigencia, (5) la tecnología e innovación pasa a ser de importancia para la competitividad y (6) se demanda mayor variedad de insumos de granos.

En este modelo en red, los autores separan a los *propietarios de tierra* de las *Empresas de Producción Agraria,* donde estos últimos cumplen un rol de coordinación entre las distintas partes de la red agroindustrial y busca optimizar sus inversiones, reducir riesgos y mantenerse competitivo. Además de estos agentes económicos, aparecen los *contratistas*, que son dueños de maquinaria y que subcontratan en aquellos casos donde las empresas de producción agraria no les es rentable adquirir capital propio. Dado que en este nuevo modelo la tecnología aparece como un factor importante para la competitividad de los agentes, aparecen también los *proveedores industriales de insumos* que proveen mayor variedad de productos tales como

herbicidas, semillas y maquinaria. La red la cierran las organizaciones de *transportistas* y los *agentes financieros.*

Este modelo en red genera un ecosistema de relaciones donde el riesgo se distribuye al introducir sistemas de contratos por porcentajes, y que provoca una interacción muy similar a las estructuras híbridas que describía Ménard anteriormente:

> *"(...) A través de este tipo de articulaciones, se da un doble juego: por un lado, cada una de las partes (aún con sus asimetrías estructurales) quiere maximizar ingreso/beneficio, pero, por otro, sus niveles de ingresos/beneficios dependen del desempeño colectivo. De esta forma, y en la medida que los contratos se realicen en base a porcentajes de cosecha y/o rendimientos físicos, la función de beneficio de cada una de las empresas de la red tiene argumentos comunes con la contraparte. Así, la propia estructura de este modelo de producción conlleva el esquema de ganar/ganar y establece las condiciones iniciales hacia una suerte de cooperación para poder competir mejor" (Bisang et al 2008, p. 30-31)*

En línea con esta interpretación, Senesi, Chaddad y Palau (2013) proponen un análisis de las distintas formas de organización híbridas en la industria Argentina. Según los autores, la industria evolucionó en cuatro tipos de estructuras híbridas: (1) estructuras híbridas informales, caracterizadas por contratos de palabra con contratistas, información (2) fideicomisos, donde hay un organismo que actúa como controlador de recursos en beneficio de otros (en general un banco o abogados), (3) Empresas con inversores tradicionales y (4) una "red de redes", que se compone por un organismo que maneja múltiples redes locales con conocimiento particular a cada región.

Al analizar cada una de estas estructuras, los autores suscriben a un análisis de atributos que resulta interesante en base a los modelos teóricos presentados previamente. El análisis se presenta en la figura 5.1-1:

	Estructuras Informales	Fideicomiso	Empresas orientada a Inversores	Red de Redes
Primera Aparición en Argentina	1990	Principios de años 2000	Fines de los '90	1995
Tipo de Contrato	Informales, relacionales	Formal	Formales e informales	Formales e Informales
Duración de Contrato	Corto Plazo (1-3 años)	Corto a mediano plazo	Corto plazo (1 año)	Cortos y largo plazo (+5 años)
Actores involucrados	Agricultor, Proveedores de Servicios	Bancos, abogados, instituciones financieras, coordinadores, proveedores de servicios e insumos	Coordinadores, inversores de capital, abogados, contadores	Coordinador, dueños de tierra, proveedores de servicios, bancos, inversores externos
Fuentes de Financiación	Capital Propio, Crédito de proveedores	Inversores privados e institucionales	Inversores externos	Bancos, Inversores externos, proveedores de insumos
Incertidumbre Organizacional	Mediana	Baja	Baja	Muy baja (importancia de la confianza)
Liderazgo	No importante	Mediana	Baja	Muy importante (coordinador central y gerentes regionales)
Incentivos	Bajos (dada la imposibilidad de tener contratos a largo plazo)	Altos	Altos	Altos (los participantes tienen que cumpir condiciones para recibir rentas)
Activos específicos de la Relación	Bajos (know-how)	Medianos (know-how, reputación de actores)	Medianos (know-how, reputación de actores)	Altos (know-how, reputación de distintos agentes, tecnología)

Figura 5.1-1

Fuente: Senesi, S. I., Palau, H., Chaddad, F. R., & Daziano, M. (2013). The evolution of farming networks in a fragile institutional environment: the case of Argentina

Según los autores, estas estructuras híbridas surgen de la incertidumbre institucional de Argentina, donde los actores buscan mitigar el riesgo y reforzar los derechos de propiedad, mediante la formación de contratos que permitan reducir los costos de transacción, alinear incentivos (de manera tal que todos cumplan con su parte), al mismo tiempo que permiten flexibilidad y autonomía ante cambios institucionales en el país (tales como devaluaciones y la introducción de retenciones a la exportación). Los autores observan que las estructuras de fideicomisos y las empresas orientadas a inversores se reducen a medida que la incertidumbre empuja a los inversores ajenos a la industria hacia afuera, por lo que se mantienen las estructuras informales y la "red de redes".

5.2 Estructuras de organización y mecanismos de coordinación

Al analizar las distintas razones por las que los actores en una economía deciden organizarse como estructuras híbridas, Ménard (2004) sugería que las estructuras podían

diferenciarse por el grado de coordinación centralizada que necesitaran. El autor propone que: (1) a mayor riesgo de apropiación (que crece con la especificidad de activos) la coordinación tiene a ser más centralizada, y (2) a mayores grados de necesidad de adaptarse a incertidumbre, y a mayor necesidad de resguardos contractuales, la coordinación tiende a ser más centralizada.

El autor luego propone cuatro subdivisiones de las estructuras híbridas acorde a su mecanismo de coordinación: (1) Las estructuras híbridas que dependen principalmente de la confianza entre actores, con gran descentralización, (2) redes relacionales, basadas en convenciones sociales y reglas que vienen de costumbre, (3) redes basadas en liderazgo, donde un organismo coordinador controla de manera más cercana las acciones de cada participante, y (4) gobiernos formales, donde los agentes están restringidos en sus acciones por un organismo central.

Ménard expande el modelo original de análisis propuesto por Williamson (1991) al incorporar estas estructuras dentro del análisis de estructuras óptimas. El modelo sugerido por el autor se muestra en la figura 5.2-1

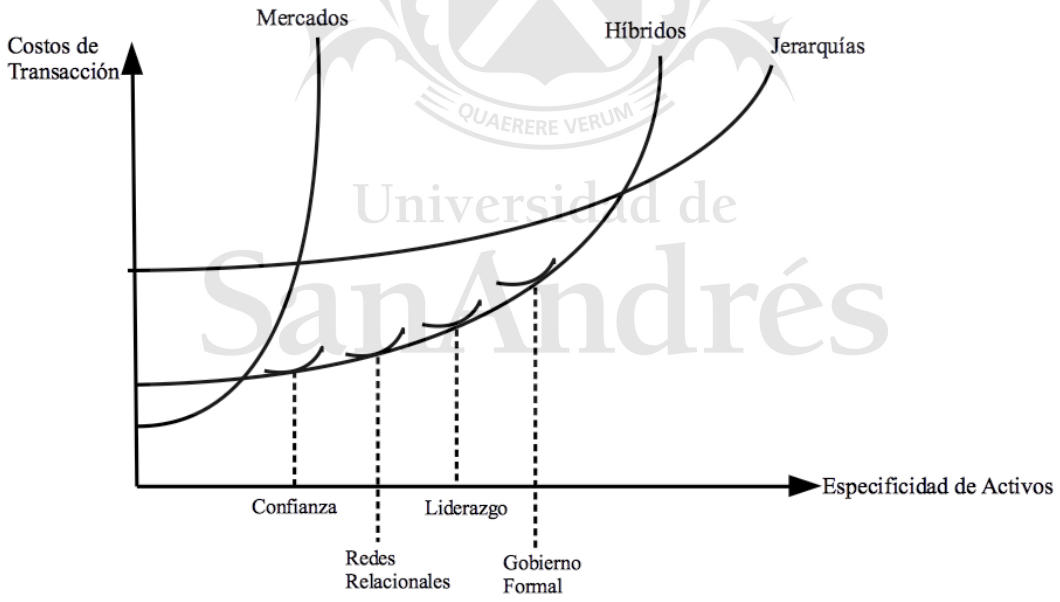

Figura 5.2-1

Acorde al análisis propuesto por Senesi et al (2013), que identifica las estructuras híbridas en la agroindustria argentina, en el presente trabajo se propone ubicar las estructuras de híbridos informales dentro de las dependientes de confianza, y las estructuras de redes dentro de las estructuras híbridas con coordinación vía liderazgo, dada su estructura descentralizada en regiones pero coordinada vía organismos centrales. Esta tipología será útil

para entender como una red que utilice una tecnología de Blockchain puede impactar las estructuras organizacionales existentes.

5.3 Blockchain aplicado a la agroindustria en Argentina

Como primer acercamiento a la utilización de Blockchain en la agroindustria en Argentina, se puede utilizar la metodología propuesta por Wüst y Gervais (2017) donde proponen un diagrama ilustrativo para entender en qué casos un Blockchain puede ser útil, y en qué casos no es necesario.

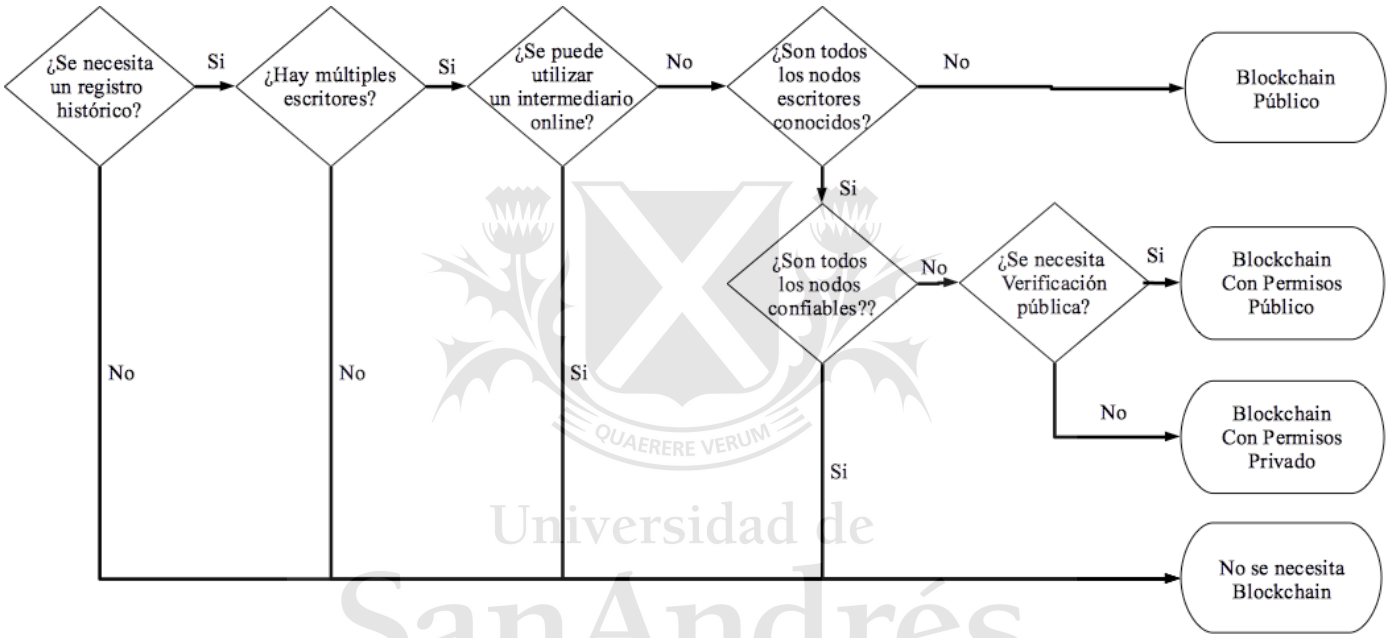

Figura 5.3-1

Según los autores, los requisitos indispensables son la necesidad de un registro histórico, la existencia de distintos participantes que puedan generar transacciones en el registro, la imposibilidad de consensuar un intermediario que esté siempre disponible (a costo razonable), y que haya algún grado de desconocimiento o desconfianza entre los participantes.

Aplicando esta metodología al campo, la primera pregunta es si es necesario un registro histórico de transacciones. Dado que se intercambian bienes y servicios, a crédito, que existen situaciones donde se reparten rentas acorde a beneficios futuros, y que hay múltiples impuestos a pagar a futuro, se puede concluir que es necesario tener registros históricos de las

transacciones entre actores económicos. Dado lo analizado por los autores en las secciones anteriores, se identifican múltiples actores participando en la red, todos con mecanismos complejos e idiosincráticos. Ante la pregunta si hay un sistema de terceros, que este siempre online en la red, que pueda actuar como escritor de registros (como si fuera un escribano), no parece haberlo. ¿Se conocen todos los participantes? Sí, no hay una necesidad o existencia de anonimato en la red. ¿Se confía en todos los participantes? Aquí uno puede interpretar que no, que justamente la generación de reputación es una de las partes más importantes para poder generar transacciones. Es aquí donde la utilización de Blockchain puede servir para dotar a los participantes de confianza y reputación que no podrían generar por sí solos antes de ingresar a la red. También se decir que la verificación de los registros es necesaria y debería poder ser validada por todos los participantes (esto no quiere decir que puedan ver el contenido, sino que puedan verificar la inmutabilidad de los registros).

Acorde a la metodología de Wüst y Gervais (2017), se puede empezar a analizar la industria del agro en Argentina utilizando un registro distribuido, en formato de un Blockchain de consorcio, o más específicamente, un Blockchain con permisos.

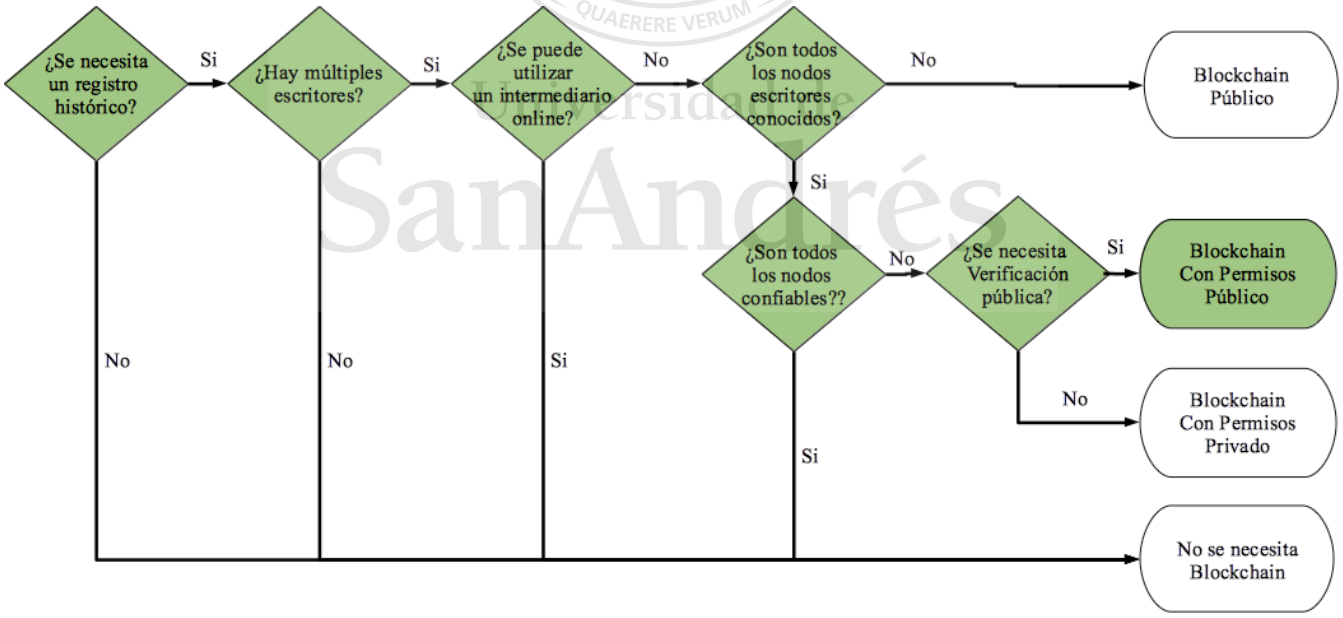

Figura 5.3-2

Esto no quiere decir que necesariamente una red de Blockchain sea posible o rentable de implementar, pero sí que, dado el estado de la tecnología hoy en día, es un buen primer paso para analizarlo de manera teórica.

Continuando con el análisis, hay varias opciones a considerar. Dado que se está analizando un Blockchain de consorcio, esto implica que hay un agente u organismo que permite el alta de nuevos participantes en la red.

En caso de que el organismo que busque actuar como facilitador del Blockchain, sea el coordinador central de la red, puede armar reglas de manera tal que siga siendo beneficiario de la cadena, al mismo tiempo que reduce los costos de coordinación dado el mejor flujo de información y la posibilidad de ejecutar contratos de manera automatizada (contratos inteligentes). En estos casos, los participantes se benefician de una mayor transparencia de registros y la posibilidad de participar de una red donde la reputación es crítica para su participación, aún sin haber participado de transacciones con sus otros pares. Al tener mayores resguardos para protegerse del oportunismo, los costos de transacción también bajan en la estructura híbrida de liderazgo (tal como es definida por Ménard (2004)). Esto hace la estructura de liderazgo todavía más atractiva desde un punto de vista de costos de transacción óptima con respecto a las estructuras jerárquicas o de mercado, asumiendo que el coordinador elige empujar esta iniciativa en búsqueda de mayor coordinación y control de un mercado.

Sin embargo, si uno introduce la posibilidad de que el resto de los participantes empujen un sistema de consorcio que también compita con el creado por el coordinador, entonces el coordinador tiene menos incentivos a armar reglas que alejen a los otros participantes de su cadena. Esto puede generar mayor participación y ganancia social en caso de que todos los participantes puedan salir ganando de una mayor confianza y transparencia en los registros, ya sea por una reducción de trámites y costos administrativos, o mediante un mejor acceso a la financiación de créditos sin la necesidad de tener garantes que sustituyan la reputación. En este caso se crean mayores incentivos a organizarse en redes, bajando los costos de transacción totales, pero no necesariamente prevalece alguna estructura híbrida sobre otra.

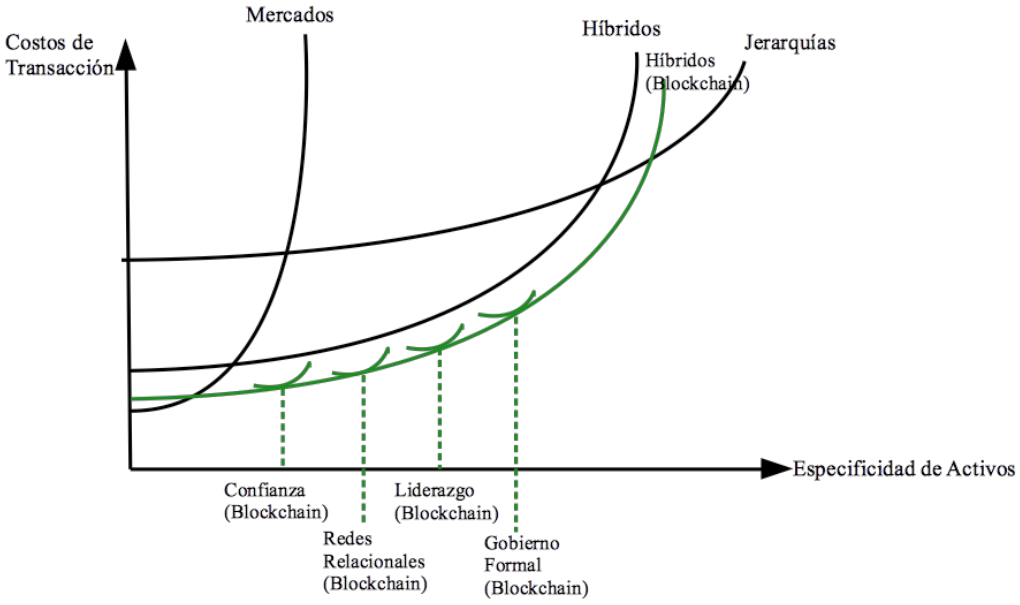

Figura 5.3-3

En conclusión, la mayoría de los beneficios provienen de una mejor articulación de efectos reputacionales, que se traducen en un menor riesgo de derechos de expropiación tal como se indicaba en la sección 4.3. Volviendo a lo definido por Ménard con respecto a estructuras híbridas donde sugiere que la reputación puede crecer viniendo de (1) transacciones recurrentes entre socios, (2) familiaridad entre participantes por compartir antecedentes en común, (3) la existencia de información acerca de transacciones con terceros y (4) el compartir redes en común que tengan normas de comportamiento específicas, Blockchain permite una mejora en éstas áreas que resultan de particular importancia para la agroindustria. Esto reduce los costos de transacción y el esfuerzo de entablar relaciones a mediano y largo plazo entre participantes de la industria, facilitando la cooperación y generando potenciales beneficios entre distintos productores y contratistas.

6. Conclusión

Blockchain sigue siendo una tecnología naciente, y no podemos predecir cuán exitosa será en su objetivo de generar un ecosistema de transacciones sin intermediarios. Existen múltiples barreras para su adopción, que todavía se están analizando y tratando de resolver. Sin embargo, su propuesta es interesante y permite una manera alternativa de imaginar un mercado.

Este trabajo tuvo como objetivo acercar el entendimiento de los mecanismos de interacción que permite Blockchain, a la teoría económica de costos de transacción. En pos de este objetivo, se hizo un análisis detallado del funcionamiento de Blockchain, de manera que se pueda entender qué posibles transacciones pueden ser ejecutadas dentro de esta plataforma tecnológica.

Se describió como Blockchain, al utilizar mecanismos de hashing y de criptografía asimétrica, provee un sistema de interacción que permite mantener un registro inalterable de transacciones, sin la necesidad de un intermediario que garantice la veracidad de la información. El mecanismo de incentivos que facilita este registro permite la integridad del sistema, y asegura que a mayor utilización del sistema, el registro tendrá mayor transparencia, posibilitando una definición menos costosa de los derechos de propiedad.

Sin embargo, Blockchain tiene múltiples limitaciones que impiden su adopción masiva. Por un lado, la velocidad de verificación de transacciones es menor a la posibilitada por intermediarios centralizados. Por otro, los mismos mecanismos de verificación que actúan como incentivos para atraer participantes a las plataformas son muchas veces costosos en términos energéticos, lo cual los hace inviables ecológicamente a largo plazo. La existencia de múltiples plataformas que se utilizan para distintos tipos de transacciones todavía no converge en un sistema de interoperabilidad que permita mover activos de una plataforma a otra, lo cual genera un ecosistema confuso donde cada plataforma compite por atraer participantes a su red.

La falta de regulación clara con respecto a la financiación de nuevos proyectos de Blockchain genera riesgo de engaños y de proyectos que nunca terminan ejecutándose, quitándole credibilidad a futuros proyectos en el área.

Sin embargo, uno de los problemas más claros en la adopción de Blockchain es la falta de un problema claro a resolverse por la tecnología. El caso de uso más claro es la posibilidad de intercambiar activos monetarios sin la necesidad de un intermediario que garantice la seguridad de la transacción. Sin embargo, la velocidad de verificación de plataformas tales

como Bitcoin hacen que estas plataformas no sean preferibles hoy a las proveídas por empresas tales como tarjetas de crédito y bancos.

Esto genera una situación particular, que es que las mismas empresas que corren el riesgo de ser reemplazadas por esta tecnología, aparecen como actores que impulsan nuevos casos de uso para la tecnología.

Este trabajó presenta los tipos de Blockchain de consorcio, y Blockchain privados, que se diferencian de los Blockchain públicos, al estar impulsados por un organismo que actúa como garante de confianza. Esto es, un sistema que se rige con la mismas propiedades de Blockchain, pero que requiere confianza en el nodo que define las reglas de juego. En este tipo de arquitectura, existen nodos que aprueban la participación de los distintos agentes en la economía, pero la integridad de las transacciones sigue siendo garantizada mediante la validación y verificación de todos los nodos.

Estos sistemas proveen algunas ventajas, tales como mayor velocidad de transacciones, y casos de uso más concretos, sin embargo hoy en día no existen mayores ejemplos de casos de éxito rotundo.

Sin embargo, muchas de las limitaciones técnicas están siendo investigadas, con distintas posibilidades de resolverse, por lo que esta tecnología sigue siendo un tópico de conversación frecuente.

Dada esta situación, este proyecto elige analizar el potencial impacto de Blockchain en la economía mediante la lupa de la economía de costos de transacción. Esta rama de investigación pone foco en las transacciones como unidad de actividad y busca entender cuáles son los factores que generan fricción en el intercambio de bienes y servicios entre agentes económicos. En particular, la existencia de información asimétrica y el riesgo de oportunismo lleva a la dificultad de entablar relaciones a mediano y largo plazo entre agentes.

La economía de costos de transacción sugiere que la elección de estructuras de organización lleva a la reducción de estos costos de transacción de manera tal de asegurar que el intercambio siga existiendo, y la posibilidad de oportunismo sea menor. Las estructuras propuestas son la estructura jerárquica, donde es la empresa que elige integrar verticalmente la producción, el mercado, donde las transacciones se rigen mediante los mecanismos clásicos de precios, y las estructuras híbridas, caracterizadas por escenarios donde distintos participantes, que normalmente compiten, eligen compartir recursos en pos de lograr mayores beneficios en conjunto.

Este trabajo propone un paralelismo entre los Blockchain públicos, de consorcio, y los privados, con las estructuras de organización propuestas por la economía de costos de transacción. En particular, este paralelismo está dado que por el grado de coordinación centralizada necesaria en cada uno de los escenarios, así como también cuánta libertad existe para participar en ese ecosistema.

Concretamente, para analizar el impacto teórico de Blockchain con el enfoque de costos de transacción, se utilizó un análisis comparativo tal como propuso Williamson (1991). En este escenario, el autor proponía teorizar acerca de cambios en los parámetros institucionales que impactan los costos de transacción y entender cómo esos cambios afectan la elección de cada estructura de organización.

Williamson (1991) propone poner foco en cambios en la definición de derechos de propiedad, efectos reputacionales, ejecución de contratos e incertidumbre. En este trabajo, utilizamos el mismo enfoque, analizando cómo Blockchain afecta cada una de estas áreas.

El análisis concluye que la integridad e inalterabilidad de Blockchain promueve un ecosistema que permite una mejor definición de derechos de propiedad, tal que reduce los riesgos de expropiación gubernamental, y de proveedores y competidores. Esta mejora de los derechos de propiedad asegura un menor costo adicional de definir previsiones para reducir oportunismo, empujando a una reducción generalizada de costos de transacción, por lo que las estructuras híbridas y de mercado salen favorecidas con respecto a las estructuras jerárquicas (que suelen ser las elegidas cuando los riesgos de expropiación de rentas son altos).

Con respecto a los efectos reputacionales, se concluye que la mayor integridad de transacciones, y la existencia de un ecosistema y registros en común entre participantes reduce la necesidad de generar reputación para poder participar en transacciones con nuevos actores. Dado que los agentes todos interactúan en plataformas transparentes y confiables, pueden asegurarse de verificar el historial de cada participante antes de intercambiar cualquier servicio, lo cual permite menores barreras de entrada y también reduce los costos asociados a la definición de contratos que definan términos y condiciones más estrictos para reducir oportunismo. Dado que la generación de reputación es de particular importancia para las estructuras híbridas, sugerimos que la mejora de efectos reputacionales converge en la elección de estructuras híbridas por sobre las estructuras descentralizadas o jerárquicas.

En cuanto a mejoras en la ejecución y supervisión de contratos, se sugiere que la utilización de contratos inteligentes permite sistematizar y automatizar un conjunto de reglas y

condiciones, siempre y cuando las contingencias sean conocidas y puedan ser planificadas de antemano. Este escenario, acorde a la teoría de costos de transacción, es más común en estructuras de mercado, por ende la utilización de Blockchain permite reducir los costos asociados a la ejecución de contratos en estructuras de mercado, favoreciendo estas estructuras con respecto a las otras. Sin embargo, esta conclusión sólo es válida para la ejecución de contratos completos, y no es válida para contratos incompletos, que son necesarios para formar vínculos a mediano y largo plazo en estructuras híbridas.

En cuanto a la incertidumbre, dado que es un parámetro externo, no se encuentra un beneficio claro en utilizar Blockchain, aunque la distribución de información de manera transparente y automática puede permitir mayor coordinación entre agentes en una economía, de manera tal de poder corregir acciones ante la existencia de shocks externos. Sin embargo, esto también puede ser sugerido mediante la utilización de cualquier sistema de información centralizado, por ende no es un resultado concluyente.

En esencia, Blockchain permite la reducción de costos de transacción mediante la mejora de reputación, la ejecución de contratos inteligentes, y una definición transparente de derechos de propiedad. Esto está dado por la integridad propia que se logra con el mecanismo de incentivos que es característico de Blockchain.

Una crítica que puede hacerse a este modelo es que analiza un cambio a la vez, en lugar de analizar todos los cambios al mismo tiempo. Williamson (1991) toma en cuenta esta crítica y sugiere que si los cambios de parámetros son independientes, la teoría puede ser aplicada al considerar los cambios aplicados de manera secuencial. Sin embargo, este no es el caso, y los cambios están todos relacionados dado que se dan por la misma tecnología. En este caso, sugerimos que dado que el trabajo concluye que bajo todos los escenarios, la tendencia se da hacia la descentralización, no esperamos cambios significativos en las conclusiones.

Otra crítica es que se está considerando un escenario donde la misma implementación de la tecnología no tiene costo. Sin embargo, uno de los mayores problemas que afronta la tecnología en la práctica es que es costosa de implementar, en particular cuando su éxito depende de que más participantes se sumen a la red. Sugerimos que el análisis de costo / beneficio es uno distinto al planteado por los costos de transacción, por ende las conclusiones no se verán afectadas. Sin embargo, la aplicación práctica de este análisis en el mundo real depende de que Blockchain sea visto como una alternativa económica para reducir los costos de transacción. En caso contrario, no tendrá adopción en el futuro.

Definidas estas conclusiones, se analizó la industria agrícola en Argentina para entender cómo podría utilizarse esta tecnología y cómo impacta las estructuras de gobernanza existentes.

Dado que el escenario actual en la industria es de redes, coordinadas por un organismo central, y dado que la reputación es uno de los componentes más importantes para generar transacciones a futuro, sugerimos que la utilización de Blockchain de consorcio, coordinados por el organismo coordinador, o creados por los productores, es una manera de mejorar la confianza entre participantes, reduciendo las barreras de entrada y facilitando la cooperación entre agentes en la economía. En este escenario, las estructuras híbridas se tornan todavía más atractivas para la organización de esta industria, profundizando el modelo actual, aunque permitiendo la coordinación de la red de una manera más descentralizada, reduciendo el foco de poder en el coordinador.

En conclusión, Blockchain permite repensar cómo se ejecutan intercambios en la economía, pero hoy está lejos de ser adoptada de manera general. La teoría de costos de transacción avala la promesa de reducción de costos de transacción, potencialmente generando una tendencia hacia la descentralización en mercados donde la reputación y los derechos de propiedad son importantes. Será interesante analizar a futuro si Blockchain cumple esta promesa.

7. Bibliografía

[Chainworks] 2018, 18 de mayo, *Fundamentals of Hyperledger Architecture* [Video] URL: https://www.youtube.com/watch?v=8rDabrzopUg

Abadi, J., & Brunnermeier, M. (2018). Blockchain economics. mimeo Princeton University.

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of Initial Coin Offerings. *Journal of Economics and Business*.

Allen, Darcy. "Discovering and developing the blockchain cryptoeconomy." (2017).

Back, A. (2002). Hashcash-a denial of service counter-measure.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.

Berg, C., Davidson, S., & Potts, J. (2018). Some Public Economics of Blockchain Technology.

Bisang, R., Anlló, G., & Campi, M. (2008). Una revolución (no tan) silenciosa. Claves para repensar el agro en Argentina. Desarrollo Económico, 165-207.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-38.

Catalini, C., & Gans, J. S. (2016). Some simple economics of the blockchain (No. w22952). National Bureau of Economic Research.

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international conference on World Wide Web (pp. 213-224). ACM.

Coase, R. (1998). The new institutional economics. *The American Economic Review*, *88*(2), 72-74.

Coase, R. H. (1937). The nature of the firm. Economica, 4(16), 386-405.

Coulouris, G. F., Dollimore, J., & Kindberg, T. (2005). Distributed systems: concepts and design. pearson education.

Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain.

de Vries, A. (2018). Bitcoin's Growing Energy Problem. Joule, 2(5), 801-805.

Drescher, D. (2017). Blockchain basics. Apress

Jakobsson, M., & Juels, A. (1999). Proofs of work and bread pudding protocols. In Secure Information Networks (pp. 258-272). Springer, Boston, MA.

Juels, A., & Brainard, J. G. (1999, March). Client puzzles: A Cryptographic countermeasure against connection depletion attacks. In NDSS (Vol. 99, pp. 151-165)

MacDonald, T. (2015). Theory of non-territorial internal exit.

Ménard, C. (2004). The economics of hybrid organizations. Journal of Institutional and Theoretical Economics JITE, 160(3), 345-376.

Ménard, C. (2012). Hybrid modes of organization. Alliances, Joint Ventures, Networks, and other strange animals.

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

Powell, W. (2003). Neither market nor hierarchy. The sociology of organizations: classic, contemporary, and critical readings, 315, 104-117.

Senesi, S., Chaddad, F. R., & Palau, H. (2013)a. Networks in Argentine agriculture: a multiple-case study approach. Revista de Administração (São Paulo), 48(2), 281-294.

Senesi, S. I., Palau, H., Chaddad, F. R., & Daziano, M. (2013). The evolution of farming networks in a fragile institutional environment: the case of Argentina. Journal on chain and network science, 13(1), 71-82.

Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). Encyclopedia of cryptography and security. Springer Science & Business Media pp 98, 487- 491

Williamson, O. (2000). Contract and economic organization. *Revue d'economie industrielle*, *92*(1), 55-66.

Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. The journal of Law and Economics, 22(2), 233-261.

Williamson, O. E. (1981). The economics of organization: The transaction cost approach. American journal of sociology, 87(3), 548-577.

Williamson, O. E. (1998). Transaction cost economics: how it works; where it is headed. De economist, 146(1), 23-58.

Williamson, O. E. (1999). Strategy research: governance and competence perspectives. *Strategic management journal*, *20*(12), 1087-1108.

Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. *Administrative science quarterly*, 269-296.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia.

Wüst, K., & Gervais, A. (2017). Do you need a Blockchain?. IACR Cryptology ePrint Archive, 2017, 375.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In Software Architecture (ICSA), 2017 IEEE International Conference on (pp. 243-252). IEEE.

8. Anexo

8.1 Programa para resolver ejercicio Hash

Ejecutable en Python

```
import hashlib
import time
h = hashlib.sha256()
#Dificultad de algoritmo (cantidad de ceros)
dificultad = int(input("Ingrese dificultad: "))
#Definir Texto Original
text = input("Ingrese Texto: ")
#Nonce Original
nonce = 0
#Busco el valor nonce tal que se cumple la restricción
start_time = time.time()
while True:
    raw = (text +str(nonce))
    h = hashlib.sha256()
    h.update(raw.encode())
    result = h.hexdigest()
    if not result.startswith(dificultad*str(0)):
        nonce += 1
    else:
        print("el nonce que resuelve el ejercicio con dificultad ",dificultad, " es: "+str(nonce))
        print("el valor hash para ",raw," es ",result)
        print("El tiempo de Procesamiento fue de --- %s segundos ---" % (time.time() - start_time))
        break
```

8.2 Programa para verificar solución Hash

Ejecutable en Python

```
import hashlib
import time
h = hashlib.sha256()
M = input("Solucion a verificar")
start_time = time.time()
h.update(M.encode())
result = h.hexdigest()
print("El valor hash para ",M," es ",result)
print("El tiempo de Procesamiento fue de --- %s segundos ---" % (time.time() - start_time))
```

8.3 Criptografía Asimétrica: Un ejemplo

Para describir un ejemplo de criptografía asimétrica, se verá un ejemplo comúnmente utilizado en criptografía, que es la transmisión de mensajes entre dos participantes, llamados Alice y Bob[34].

En la figura 8.3-1, Alice quiere enviar el texto "¡Hola Mundo!" a Bob, y firmarlo digitalmente, para constatar que al momento de firmarlo, eso era lo que el texto contenía y por ende certifica el contenido. Para firmarlo digitalmente, primero procesa el texto a través de una función hash, y luego utiliza su llave privada para encriptar la información. Luego, Alice envía el documento conteniendo el texto original "¡Hola Mundo!" y también el texto cifrado a Bob. Bob recibe el documento, y necesita constatar que efectivamente el documento no ha sido adulterado desde que Alice lo envió. Para eso, utiliza la llave pública de Alice, para descifrar la información, y derivar el valor hash. Además de esto, procesa el texto "¡Hola Mundo!" a través de la función hash para llegar a su propio resultado de la función. Si los valores descifrados y hash son iguales, entonces es evidencia de que no hubo modificaciones. Si los valores son distintos, entonces el valor texto recibido por Bob es distinto del que se procesó

[34] Alice y Bob figuran en la mayoría de los ejemplos ilustrativos en criptografía y computación

por Alice al momento de generar su primer valor hash, por ende hubo alguna manipulación en la información.

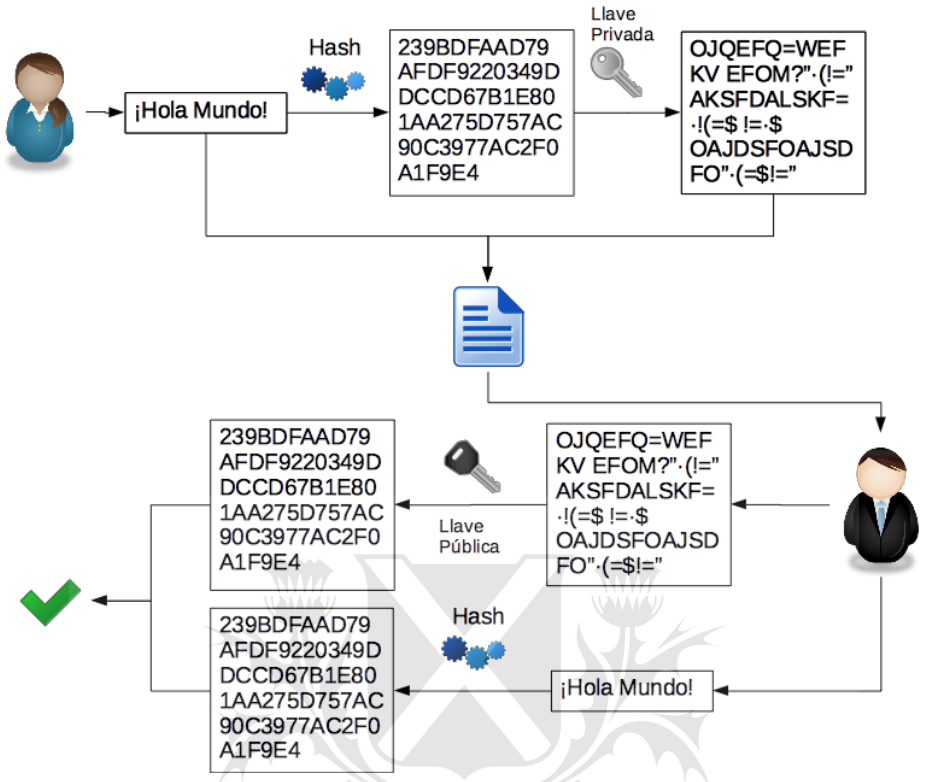

Figura 8.3-1: Diagrama de verificación de firmas digitales utilizando criptografía asimétrica

8.4 Resolución de Ejercicio Hash y creación de nuevos bloques

El ejercicio hash por resolver en el proceso de generación de nuevos bloques es encontrar un valor nonce tal que tomando los valores de: (1) las transacciones del bloque, (2) el valor hash del bloque previo, (3) la dificultad, (4) la marca temporal de creación del bloque, y (5) el nonce encuentren un valor que cumpla la restricción de dificultad establecida.

Agrupar las transacciones también plantea un problema a resolver, dado que pueden ser miles de transacciones. La solución propuesta es utilizar funciones hash y una estructura de *árbol de Merkle*. Un árbol de Merkle es una estructura de árbol binario donde cada hoja contiene el valor hash de un bloque de información, y donde cada nodo superior contiene el valor hash de la concatenación de los nodos anteriores. Representado gráficamente:

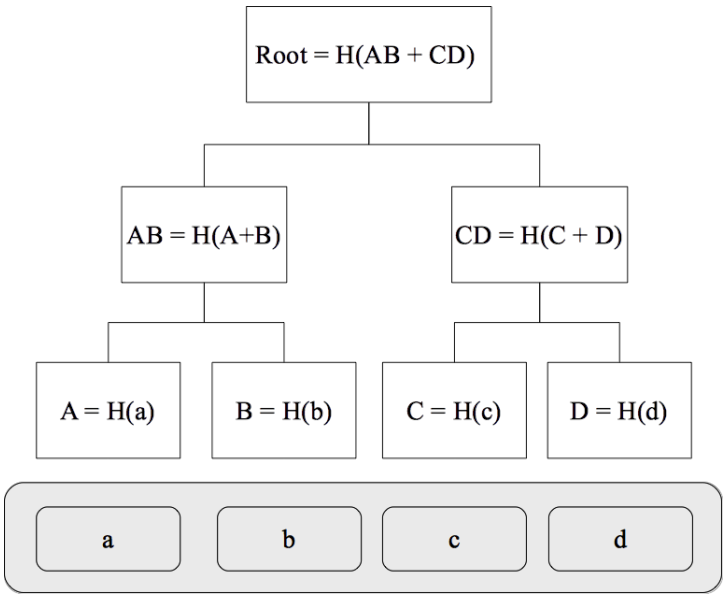

Figura 8.4-1: Árbol Merkle, donde a, b, c y d son los datos para procesar. Cada nodo superior contiene el hash de los datos de sus hojas inferiores

En la figura 8.4-1 se ve como los datos a, b, c y d son convertidos a valores hash utilizando la función H(M). A medida que se sube en la estructura, los nodos superiores están formados por valores hash a partir de los valores hash calculados anteriormente. El nodo superior, es denominado valor raíz, y permite sintetizar todas la estructura en un solo valor. Como se explicó al hablar de funciones hash, los valores hash son utilizados para identificar manipulación de información. En el diagrama superior, *si alguno de los valores, a, b, c, o d fuese cambiado luego de calcular el valor raíz, todos los cálculos superiores dejarían de ser válidos*. Por ende, si en el tiempo el valor raíz cambia, quiere decir que alguna transacción fue modificada.

Volviendo al problema computacional a resolver, se mencionó que el objetivo era encontrar un valor nonce tal que tomando los valores de: (1) las transacciones del bloque, (2) el valor hash del bloque previo, (3) la dificultad, (4) la marca temporal de creación del bloque, y (5) el nonce encuentren un valor que cumpla la restricción de dificultad establecida. Dado que se describió el concepto de árbol de Merkle, se puede aclarar que el valor que identifica a las transacciones del bloque es la raíz del árbol de Merkle. El diagrama 8.4-2 ilustra el problema a resolver:

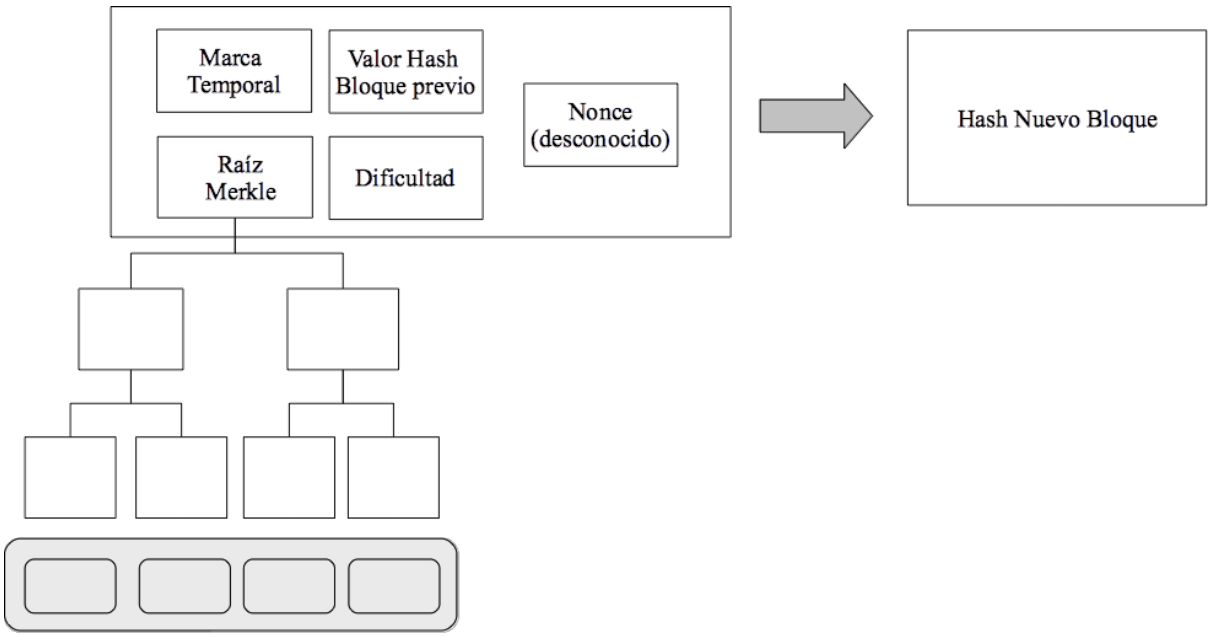

Figura 8.4-2

La figura muestra un escenario donde el objetivo es encontrar el nonce tal que el hash del nuevo bloque cumpla la restricción de dificultad actual al momento de generar el nuevo bloque. *Una vez el ejercicio está resuelto, el valor hash resultante es el nuevo valor hash con el que se identifica al bloque creado*, tal como se muestra en las figuras siguientes:

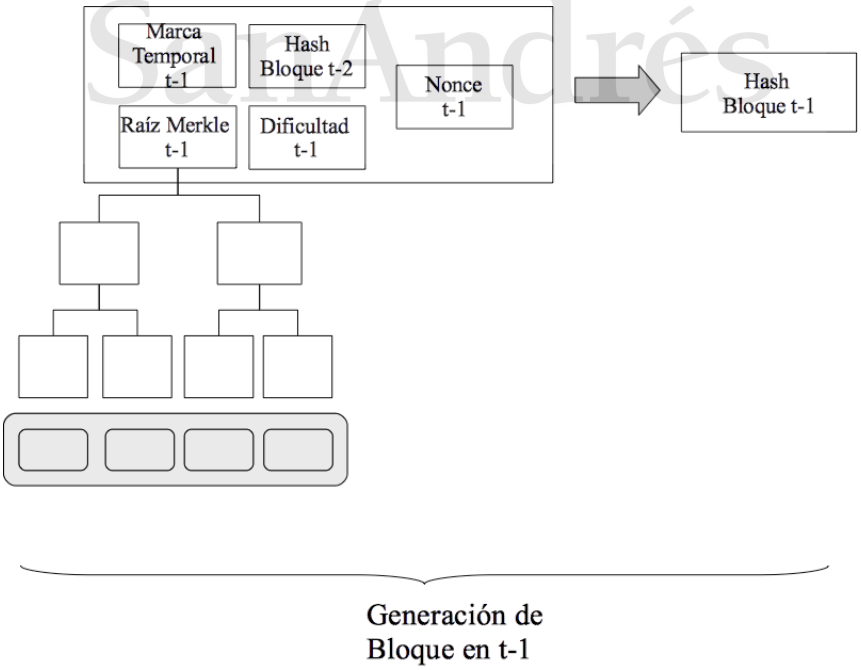

Figura 8.4 -3

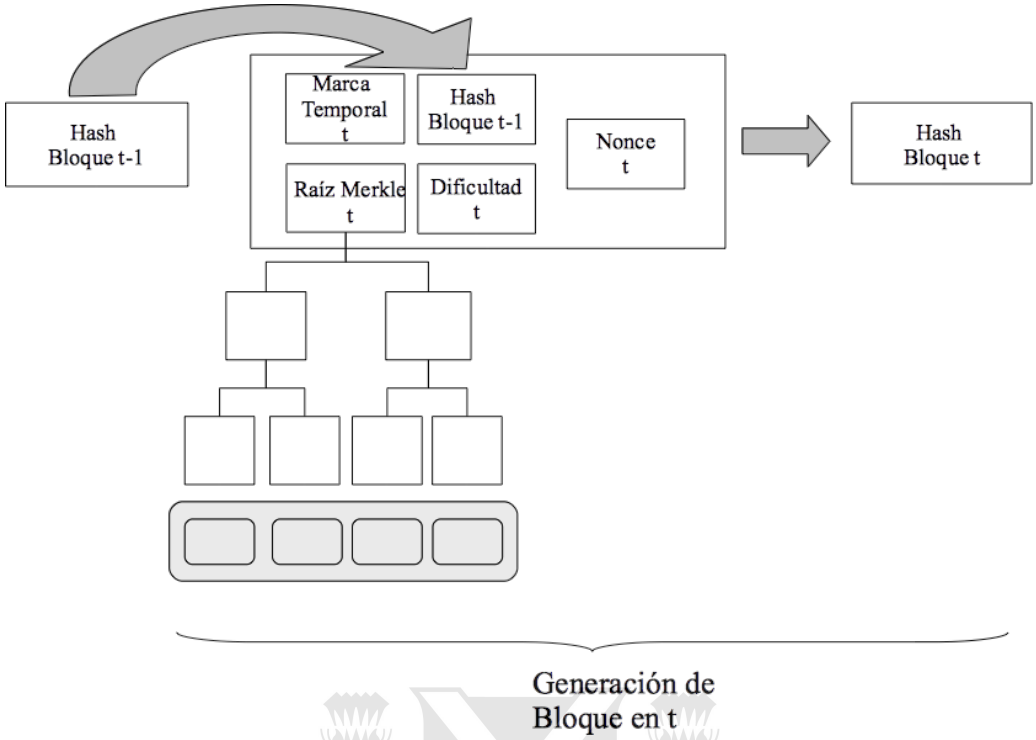

Figura 8.4-4