



Facultad de Ciencias Económicas y Empresariales ICADE

BLOCKCHAIN: BASTIÓN DE LA LIBERTAD

Investigación a la luz de la teoría austriaca de la tecnología blockchain como condición posibilitadora.

Nombre: Patricia Falagan de la Sierra

Clave: 201600630

Director: Jose Luis Fernández Fernández

RESUMEN

Este trabajo de Fin de Grado aborda la afinidad entre los postulados económicos y filosóficos de la Escuela Austriaca de Economía con la tecnología blockchain. El devenir de esta tecnología viene dado por el impulso humanista que lo ha precedido, desde David Chaum hasta Nakamoto, todas las innovaciones en el campo han estado orientadas a la protección de la soberanía individual. Así, este trabajo examina el caso de Bitcoin como una institución social acontecida en el mercado, en consonancia con el Origen Evolutivo de Menger y el Teorema Regresivo de Mises. Además, estudia también el caso de Ethereum como condición posibilitadora del orden espontáneo propuesto por Hayek. En definitiva, este Trabajo pretende demostrar el potencial de blockchain como una tecnología garante de la libertad individual.

PALABRAS CLAVE: blockchain, libertad, dinero, inflación, Escuela Austriaca de Economía, Bitcoin, Ethereum, Mises, Hayek, Menger.

ABSTRACT

This thesis deals with the affinity between the economic and philosophical postulates of the Austrian School of Economics and blockchain technology. The evolution of this technology is given by the humanist impulse that has preceded it, from David Chaum to Nakamoto, all innovations in the field have been oriented to the protection of individual sovereignty. Thus, this paper examines the case of Bitcoin as a social institution that occurred in the market, in line with Menger's Evolutionary Origin and Mises' Regressive Theorem. In addition, it also studies the case of Ethereum as an enabling condition for the spontaneous order proposed by Hayek. In short, this paper aims to demonstrate the potential of blockchain as a technology that guarantees individual freedom.

KEY WORDS: blockchain, liberty, money, Austrian School of Economics, Bitcoin, Ethereum, Menger, Mises, Hayek, inflation.

1	Introducción.....	5
2	Estado de la Cuestión.....	7
2.1	La Democratización de la Criptografía: nuevos estudios e innovaciones	7
2.1.1	David Chaum, la defensa de la privacidad y la descentralización.....	8
2.2	Primera Referencia a la Cadena de Bloques: Stornetta y Haber	9
2.3	La Proof of Work y el correo basura.....	10
2.3.1.1	Una actualización: Reusable Proof of Work	11
2.4	Nick Szabo: el desconocido precursor	11
2.4.1	Los Smart Contracts	11
2.4.2	El antecedente inmediato de Bitcoin: Bitgold	12
2.5	B-Money: el vislumbramiento paralelo de Wei Dai	13
2.6	Movimiento Cypherpunk como motor del progreso técnico: las motivaciones humanísticas	13
2.6.1	Eric Hughes y el Manifiesto Cypherpunk	14
2.6.2	El Crypto-Anarchist Manifiesto de Timothy May	15
2.6.3	Pretty Good Privacy y Phillip Zimmerman	16
3	Marco Teórico	17
3.1	Conceptualización de Blockchain	17
3.2	Conceptualización de Bitcoin.....	18
3.2.1	Sistema Peer 2 Peer y la Descentralización.....	19
3.2.2	Reglas de funcionamiento de Bitcoin.....	19
3.2.2.1	Header y el Hash	20
3.2.2.2	Proof of Work o Nonce	21
3.2.3	Proceso de creación de los Bitcoins o Minería.....	21
3.3	Conceptualización de Ethereum.....	23
3.3.1	Las aplicaciones descentralizadas o DApps	24
3.3.2	La alternativa de Ethereum para el PoW: Proof of Stake.....	25
3.4	Conceptualización de la Escuela Austriaca de Economía	26
3.4.1	Aportaciones Económicas. Teoría Monetaria	28
3.4.1.1	El Origen Evolutivo de Menger	28
3.4.1.2	El Teorema de Regresión de Mises	29
3.4.1.3	Otras aportaciones económicas: la Teoría del Ciclo Económico y la Imposibilidad del Socialismo	29
3.4.2	Fundamentación filosófica y política	30
3.4.2.1	La acción humana y el orden espontáneo.....	30
3.4.2.2	La Libertad como Condición de Posibilidad	31
4	Análisis	32
4.1	Bitcoin: la materialización de la libertad económica	32

4.1.1	El Origen Natural de Bitcoin en relación con el Teorema de Regresión	32
4.1.1.1	¿Puede Bitcoin ser considerado Dinero?.....	33
4.1.1.1.1	Intercambio.....	33
4.1.1.1.2	Unidad de cuenta.....	35
4.1.1.1.3	Reserva de Valor	36
4.1.2	La Falacia de Money or Nothing.....	37
4.1.3	De las Posibilidades de Bitcoin respecto a la Libertad Económica.....	38
4.2	Ethereum como posibilitador de la libertad individual	39
4.2.1	El Orden Espontáneo y la Cooperación entre Individuos	40
4.2.2	La Libertad y No Coacción	40
4.2.3	La Descentralización, el Orden Caórdico y la Anarquía.....	42
5	Conclusión.....	43
6	Bibliografía	46

De la piel para adentro empieza mi exclusiva jurisdicción. Elijo yo aquello que puede o no cruzar esa frontera. Soy un estado soberano, y las lindes de mi piel me resultan mucho más sagradas que los confines políticos de cualquier país.

Antonio Escotado Espinosa

1 INTRODUCCIÓN

En 2009, un perfil anónimo, bajo el seudónimo de Satoshi Nakamoto, publicaba un artículo que llevaba por nombre “*Bitcoin: A Peer-to-Peer Electronic Cash System*”. En él, se proponía un sistema de pagos alternativo basado en el tú a tú, que consiguiera acabar con el problema del *double-spending*, la confianza y la autoridad única (Nakamoto, 2008). Una innovación revolucionaria que, aunque parecía una solución a un único problema, ha resultado ser una tecnología extrapolable a más ámbitos y con un potencial enorme para la transformación de todos los sectores de la economía. “Estamos ante el nacimiento de una tecnología que propone nuevas formas de optimizar nuestras relaciones ahorrar costes administrativos favorecer cooperaciones sectoriales y todas las posibilidades imaginables” (Várez, 2017). Posteriormente, en 2015, Vitalik Buterin fundaba Ethereum, la primera plataforma programable de blockchain. Ethereum es una plataforma que sirve de base para que desarrolladores de forma autónoma desarrollen aplicaciones distribuidas o DApps, sentando las bases de una nueva era de internet (Ethereum, 2021). Desde estos dos acontecimientos han sido millones las aplicaciones que se han desarrollado, las posibilidades que se han descubierto, que ha conllevado una constante revalorización de los activos digitales.

Estos dos acontecimientos aparecieron gracias al impulso humanista de diversos intelectuales del campo de la criptografía. Desde la expansión de la criptografía al ámbito civil, hasta el movimiento cripto-anarquista, la motivación ulterior que ha movido todas las innovaciones en este campo ha sido eminentemente ética. Si ha habido una preocupación a todos ellos, esa ha sido la privacidad y la soberanía individual. Así, todos los esfuerzos se han centrado en conseguir un cambio de paradigma en la sociedad que gire en torno a estas dos ideas. Los pocos años que llevan Bitcoin y Ethereum en funcionamiento han puesto de manifiesto las infinitas posibilidades que ambas ofrecen. Junto a la Inteligencia Artificial, la robótica avanzada o el 5G, esta será uno de los elementos fundamentales de la Cuarta Revolución Industrial, una revolución que redefinirá la realidad y los sistemas socio económicos que existen actualmente. Pero esta revolución no ha de tener una vocación únicamente técnica, debe tener una vocación humana y ética.

En este sentido y en conexión a las preocupaciones mencionadas, la blockchain no sólo es relevante por su capacidad de simplificar procesos sino porque alberga la posibilidad de crear estructuras más libres en pro del individuo. Así, blockchain encuentra una estrecha relación con el pensamiento de la Escuela Austriaca de economía, tanto su teoría económica como su fundamentación filosófica. Ya en el Siglo de Oro español, los escolásticos como Diego de Covarrubias, Martín de Azpilicueta, Suárez o Francisco de Vitoria, imbuyeron la especial importancia de la libertad y de sus implicaciones en el campo de la teoría política y económica. Estos fueron conscientes en su tiempo del acontecimiento de leyes que acontecían fruto de la acción humana y que no respondían a instancias políticas. Heredero de estas nociones, el Padre

Jesuita Juan de Mariana elaboró una teoría económica y política muy influyente y en consonancia con el valor de la libertad. Siglos después, la Escuela Austriaca de Economía fundada por Carl Menger en el Siglo XX retomaba toda esta fundamentación, dando lugar a una de las aportaciones más valiosas en el campo de la economía. Si bien valiosa, poco conocida y desplazada del mainstream académico por sus postulados.

La lectura de las obras de Carl Menger, Friedrich Hayek, Ludwig von Mises o Murray Rothbard, sugiere una estrecha relación con blockchain, ya que esta, por sus características intrínsecas, parece ser la materialización de muchas de sus ideas. De hecho, muchos de los autores pioneros en el campo de la criptografía y patentes contribuyentes a la creación de Bitcoin se han considerado a sí mismos austriacos, o al menos, afines a esas ideas. La blockchain es ya una institución social que ha nacido de la acción humana, es decir, de la cooperación espontánea de los individuos que permite el florecimiento de la creatividad. Además, no sólo es un agente de libertad por su origen sino también por sus consecuencias. La descentralización, la privacidad o la no modificabilidad hacen a blockchain un instrumento idóneo para la liberalización de las sociedades.

La sociedad actual, sometida a los postulados de los Estados modernos, urge a una redefinición de las relaciones entre individuos y de estos con el Estado. La libertad es el principio indivisible que cimienta la dignidad humana, su privación ha acarreado las consecuencias más temibles experimentadas en la historia de la humanidad. Los sucesos del Siglo XX pusieron de manifiesto la importancia de esta y cómo su privación ha conducido inevitablemente a la miseria, tanto material como espiritual de los pueblos. Hoy en día, son muchos los problemas que acucian a la libertad individual, así es imprescindible encontrar métodos para preservarla y protegerla. Blockchain cumple con todos los requisitos para dar esta batalla, Bitcoin actúa ya como moneda paralela en regímenes totalitarios como Venezuela, y Ehtereum ya ha servido como vía de escape a la censura de China.

De esta manera, el objetivo de este trabajo es investigar las posibilidades que ofrece la tecnología blockchain en la preservación y expansión de la libertad y soberanía individual. Por este motivo, se hará un doble análisis. En primer lugar, la compatibilidad de los principios económicos austriacos, principalmente la teoría de Carl Menger, con BTC y las criptomonedas. En segundo lugar, un análisis de los *smartcontracts*, Ethereum y otras aplicaciones como materialización de la fundamentación filosófica de la Escuela Austriaca y posteriores formulaciones.

2 ESTADO DE LA CUESTIÓN

Aunque es el surgimiento de blockchain es novedoso y supone un cambio de paradigma en el entender de internet y de nuestra realidad socio económica. La tecnología que cimienta este sistema no es una innovación radical, sino que la mayoría de sus características y elementos ya existían para otros usos. Lo que hace **Bitcoin** como precursor de todos los usos posteriores de la blockchain, es unificar todos elementos dando lugar a un nuevo uso del conjunto. Su creación fue la primera gran innovación, un experimento que, a día de hoy, tiene un **valor de 44.430,19 €** (Coinbase, 2021) y una **capitalización de un trillón de dólares** (CoinMarketCap, 2021) alzando su máximo histórico. La segunda innovación es lo que se denominó blockchain, que fue, el descubrimiento de las posibilidades que ofrecía la tecnología que sustentaba BTC para todo tipo de cooperaciones. Así, hoy todas las instituciones financieras están investigando e invirtiendo en esta tecnología. La tercera innovación dio paso al concepto de “*smart contract*” materializado en Ethereum (Gupta, 2017).

Sin embargo, todas estas innovaciones, y, las que quedan por llegar, no se pueden entender si antes hacer un análisis de la tecnología precursora, es decir, de las aportaciones y estudios que fueron ampliando los usos de las tecnologías existentes. Además, es preciso hacer un análisis de las implicaciones y filosofía que se esconde detrás de cada paso para poder entender la dimensión humanística que ofrece el blockchain. Si bien es difícil rastrear el génesis de las ideas que llevan a la final creación de blockchain, es posible situar cronológicamente ciertas aportaciones que fueron sentando las bases para un nuevo entender de internet.

2.1 La Democratización de la Criptografía: nuevos estudios e innovaciones

Uno de los elementos fundamentales de blockchain es la **criptografía**, de hecho, Nakamoto proponía el despliegue de infraestructuras clave PKI, una forma avanzada de criptografía asimétrica, para dotar de seguridad a la red (Tapscott & Tapscott, 2017). En la actualidad, la criptografía es conocida por el público en general, pero en los años 70 no era algo demasiado común. Se entendía que el ejército y los servicios de inteligencia utilizaban ciertos códigos y protocolos de comunicación especiales, pero no se contemplaba la criptografía como una ciencia en sí misma. En ese momento empresas como IBM y Universidades como Stanford y el MIT tenían cierto interés en la aplicación y los usos de esta ciencia (Smid & Branstad, 1988). Esta situación cambia con **dos hechos relevantes**.

En primer lugar, la publicación del Gobierno de los Estados Unidos del ***Data Encryption Standard (DES)***. El DES es un algoritmo de cifrado en bloque; la longitud de bloques es de 64 bits y la longitud de clave de 56 bits, un estándar excelente para el momento de su creación, pero que hoy resulta obsoleto en la arquitectura informática que vivimos (de la Guía, Hernández, Montoya, Muñoz, & Fúster, 2004).

En segundo lugar, la publicación del primer trabajo disponible públicamente sobre criptografía de clave pública “*New Directions in Cryptography*” (Lopp, 2016). En ese artículo “describieron un protocolo por medio del cual dos personas pueden **intercambiarse pequeñas informaciones secretas por un canal inseguro**. Este protocolo se llama **cambio de clave de Diffie-Helman**” (de la Guía, Hernández, Montoya, Muñoz, & Fúster, 2004, pág. 138). La relevancia de la aportación de Diffie y Helman reside en la expansión de la criptografía como una herramienta capaz de solucionar problemas abiertos fuera del campo militar. El desarrollo de hardware digital barato había roto las limitaciones y había reducido costes hasta el punto de poder utilizarse en aplicaciones comerciales y en comunicaciones de todo tipo. Esta situación llamaba a la necesidad de sistemas criptográficos equivalentes a una firma escrita (Diffie & Hellman, 1976). Supieron ver en los años 70, la necesidad de dotar de seguridad al mundo digital que posteriormente albergaría transacciones y comunicaciones cotidianas de todo tipo. Además, ya en su momento Diffie mostraba una **visión descentralizada de la autoridad** (Carrascosa, Kuchkovsky, & Preukschat, 2017).

2.1.1 David Chaum, la defensa de la privacidad y la descentralización

En los años 80, el profesor e investigador de criptografía **David Chaum** fue pionero en tratar las implicaciones éticas de la automatización y digitalización de los negocios. Doctorado en Criptografía por la Universidad de Berkeley, es considerado el padre del dinero digital y es fundador de diversas entidades dedicadas al estudio de dicho campo: la International Association for Cryptologic Research (IACR) y el National Research Institute for Mathematics and Computer Science (CWI) (Bit2Me, 2021).

Chaum dedicó sus conocimientos de criptografía y su investigación, principalmente, a la cuestión ética de la **privacidad**. En **1981** publicaba su artículo “*Hidden Trace Email, Return Addresses, and Digital Pseudonyms*” en el cual trataba la posibilidad de crear sistemas de comunicación que ocultara tanto, los participantes, como el contenido de la comunicación sobre un sistema que **no necesitara una autoridad de confianza universal**, y, además con direcciones no rastreables. Otra propuesta para este sistema era el uso de seudónimos digitales no rastreables de los cuales el poseedor tenía plena soberanía. En este *paper* ya se intuyen elementos que hacen clave a la tecnología blockchain actual, como la descentralización o la identidad soberana digital.

Posteriormente, en **1985** publicaba el artículo por el que es conocido como el padre del dinero digital: “*Security without Identification: Card Computers to make Big Brother Obsolete*”, que no sólo trataba la idea del dinero digital como algo práctico y eficaz sino también como una alternativa más ética al sistema de pagos existente en el momento, y, en la actualidad. La idea consistía en la creación de un sistema de pagos a través de *card computers* en el cual el individuo tendría la capacidad de **proteger su propia seguridad y privacidad**. Para Chaum la

computarización estaba robando a los individuos la capacidad de monitorizar su información y conocer con que fines se estaba utilizando y la automatización de los pagos no escapaba a estos peligros (Chaum, 1985). El objetivo de este artículo era doble encontrar una solución de ventaja mutua que consiguiera aunar: (a) la necesidad y beneficios que revierte en una organización la automatización de sus procesos comerciales; y (b) la protección del individuo frente a los peligros que dicho proceso conlleva. Esto se conseguía a través de un complejo entramado de elementos entre los cuales traía a colación su desarrollo en el artículo anterior: los seudónimos. De esta forma, Chaum creó **Digicash** en **1989**, una **compañía de dinero digital**, para llevar a cabo transacciones con aceptadores de *e-cash*, en la cual todas las transacciones eran anónimas (Lunt, 1996).

Como se ha mostrado, las aportaciones a nivel técnico de David Chaum han sido vitales para la formulación de Bitcoin y posteriormente de blockchain. No obstante, estas contribuciones responden a una **ulterior motivación ética**, de proteger al individuo frente a abusos de otros individuos u organizaciones. Ciertamente la filosofía subyacente a las soluciones ideadas por Chaum sirvieron posteriormente de fundamentación filosófica para el movimiento que se explicará más adelante de los *Cypherpunks*, y se podrían resumir en privacidad, anonimato, descentralización.

2.2 Primera Referencia a la Cadena de Bloques: Stornetta y Haber

Otra gran aportación a la Cadena de Bloques es el estudio de **Stuart Haber**, PhD e investigador, junto a **W. Scott Stornetta**, PhD por Stanford y licenciado en Harvard, ambos pioneros en el campo. En **1991** publicaban “*How to time-stamp a digital document*” que trataba de buscar una solución al problema de la modificación de documentos digitales, es decir, **cómo certificar cuando un documento era creado o se modificaba por última vez**. De hecho, en el *paper* de Nakamoto también se cita este documento como fundamental para la idea de BTC. Formularon a través de la práctica computacional, un esquema capaz de garantizar la firma de los bits del documento y un *time-stamp* inmodificable. Para ello, propusieron dos soluciones basadas en el concepto de Hash criptográfico y la firma. En primer lugar, una solución que *linkeaba* los Hashes de los documentos subidos un TSS, ya que el Hash de un documento debía llevar dentro el anterior *time-stamp*, y distribuía esa cadena. En segundo lugar, una solución basada en la selección aleatoria de los agentes que harían el *time-stamp*, prescindiendo así de un TSS centralizado (Haber & Stornetta, 1991). Así, Stornetta se convertía en la **primera persona en hablar de un sistema de jerarquía a la que denominó cadena de bloques** (Bit2Me, 2021).

Este trabajo, ponía de manifiesto la relevancia y la utilidad de un sistema concatenado para la gestión de datos, el uso de la criptografía y la eficacia de la descentralización. De una manera

similar a la aportación de Chaum, la contribución de Stornetta ha sido de primordial importancia para la posterior formación del movimiento Cypherpunk¹.

2.3 La Proof of Work y el correo basura

La primera mención a la función de *proof-of-work* o (POW) es la de **Cynthia Dwork** una de las personas más influyentes en la investigación criptográfica e informática. Doctorada por la Universidad de Cornell ha hecho aportaciones de gran importancia destacando la privacidad y descentralización (Bit2Me, 2021). En **1992** junto a **Moni Naor**, PhD por Berkeley, publicaban una solución para acabar con el correo basura, y en general con el abuso de los recursos compartidos: “*Pricing via Processing or Combatting Junk Mail*”. Se trataba de una **exigencia de cálculo** de una función moderadamente difícil, que no intratable, **para poder acceder al recurso** (Dwork & Naor, 1993). En definitiva, un intento de incrementar el coste de enviar masivamente correos que ha tenido unas implicaciones mucho mayores, no sólo por los distintos casos de uso, sino también porque sentó la base para uno de los elementos fundamentales de Bitcoin.

Una elaboración similar se hizo por **Juels** y **Brainard** en su artículo “*Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks*” de **1999**, en el cual, se presentaba un protocolo con pequeños puzzles criptográficos para **evitar ataques de agotamiento de la conexión** (Juels & Brainard, 1999). Por ejemplo, el **ataque TCP SYN flooding** que consiste en el envío masivo de paquetes SYN² sin respuesta a los paquetes ACK³ que el servidor envía de vuelta, saturando así el servidor consiguiendo frenar el flujo de paquetes legítimos del mismo (Cloudflare, 2021), y, dejando los puertos abiertos (a la espera del tercer paquete ACK). La aportación de Juels y Brainard no es más que otra aplicación de la idea del proof of work referida a servidores de conexión.

En ese mismo año, Juels después de proponer los *client puzzles*, elaboraba junto a **Jakobsson** el concepto de POW. Retoman esa idea que había propuesto Dwork para reducir el spam del correo, y hacen una elaboración más detallada y exhaustiva del concepto que se había vislumbrado, pero no caracterizado. Un sistema en el que **un prover** demuestra a un **verificador** que ha realizado una **cierta cantidad de trabajo computacional en un intervalo de tiempo determinado** (Jakobsson & Juels, 1999).

En **1997 Adam Back**, doctor en Ciencias de la Computación y uno de los integrantes más tempranos del movimiento Cypherpunk (Bit2Me, 2021), hacia una propuesta computacional para

¹ Movimiento que se analizará más adelante en el Estado de la Cuestión.

² El primer paquete que una IP manda a un servidor para pedir conectarse se llama: *Synchronization*.

³ El segundo paquete que envía el servidor al solicitante se llama: *Acknowledgement*. Después de este envío el solicitante deberá mandar otro paquete ACK para cerrar el loop.

evitar el envío masivo de correos: POW⁴. En su artículo “*Hashcash – A Denial of Service Counter-Measure*”, unos años después, actualizaba los casos de uso de esta idea. No sólo era una **técnica computacional** para controlar el spam, sino que también era **aplicable a cualquier recurso compartido general** (Back, 2002). Fue él, el primero en ponerlo en funcionamiento, creando Hashcash. Ante las amenazas a las que está expuesto BTC, Nakamoto al escribir la propuesta añadió el mecanismo Hashcash (Nakamoto, 2008) para conferirle una mayor seguridad al sistema. Este mecanismo supone **una parte del algoritmo de minado** de BTC ya que se requiere que los mineros encuentren un número llamado *nonce* (Erfani & Ahmad, 2019) proceso que se explicará más adelante.

2.3.1.1 *Una actualización: Reusable Proof of Work*

En **2004**, el desarrollador de software americano **Hal Finney (1956-2014)** juntaba la prueba de trabajo con la técnica de encriptación de clave pública RSA. El criptosistema RSA es una evolución del modelo Diffie-Helman (de la Guía, Hernández, Montoya, Muñoz, & Fúster, 2004) y sus aplicaciones son principalmente cifrado y firma. Así la propuesta de Finney era utilizar **Hashcash como token de prueba de trabajo** y a partir de ahí, dar **como resultado tokens firmados por RSA** que serían tokens de **prueba de trabajo reutilizables** (Finney, 2004). La importancia de su mejora radica en la posibilidad de reutilización secuencial evitando el problema del *double-spending*.

2.4 Nick Szabo: el desconocido precursor

2.4.1 Los Smart Contracts

En **1994** el americano **Nick Szabo**⁵ acuñaba en su artículo para Hacker News el concepto de **Smart Contracts**:

*“I define a smart contract as a **computerized transaction protocol that executes terms of a contract**. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries”* (Szabo, 1995).

Recogiendo las innovaciones en criptografía, anonimato o descentralización que habían desarrollado los autores anteriores, Nick Szabo actualizaba el concepto tan longevo y cotidiano del contrato para crear los contratos inteligentes. En esencia, esta creación responde a la necesidad

⁴ El autor matizó posteriormente que desconocía las aportaciones anteriores.

⁵ De este autor sólo se conoce que se licenció en Ciencias de la Computación y Derecho por la University of Washington, se desconoce su fecha de nacimiento, su estado civil, incluso hay teorías que defienden a Szabo como Satoshi Nakamoto, alegaciones que siempre ha negado (Bit2Me, 2021). Su anonimato convierte a Szabo en la personificación de los valores que ha defendido y aportado con sus aportaciones teóricas.

del hombre de vincularse unos con otros para diversos fines, una acción que se venía dando de manera generalizada desde Grecia y que hoy constituye uno de los elementos fundacionales de nuestras sociedades.

Para Szabo el contrato inteligente no es más que un **contrato normal**, sino que en vez de estar definido o escrito en papel está **escrito en una máquina** (Szabo, 2017). Para explicarlo, el informático toma el ejemplo de las máquinas dispensadoras, máquinas que tienen programados los términos de una relación comercial, la máquina comprueba que el dinero introducido por el cliente es el suficiente para dispensar cierto producto, **si se dan las condiciones establecidas se ejecuta inmediatamente** (Tapscott & Tapscott, 2017). Es decir, como se expone en la definición, un protocolo que ejecuta los términos del contrato si se dan las condiciones, es lo que lo diferencia de los contratos tradicionales, mientras los simples contratos se limitan a incorporar promesas del futuro cumplimiento de las prestaciones, los inteligentes las ejecutan (Anguiano, 2018). Además, aplicado a la tecnología blockchain y observando la teoría de la contratación, el Smart Contract al estar edificado sobre un consenso descentralizado tiene el potencial de reducir en gran medida el alcance de contingencias no contratables (He & Cong, 2019).

La aportación de Szabo ha sido vital para la innovación sobre la idea de Bitcoin, Ethereum nace como una plataforma basada en la tecnología subyacente, con algunas modificaciones, para algo más que sólo pagos, es un Marketplace de servicios financieros juegos y apps que carecen de la capacidad de robar datos o censurar (Ethereum, 2021). De esta manera, con el desarrollo de blockchain han ido descubriéndose distintos usos para la idea de Szabo que tienen el potencial de reconfigurar todas las industrias, a saber: la industria financiera, por ejemplo, la concesión de préstamos entre individuos o las aseguradoras (Díez García & Gómez Lardies, 2017).

2.4.2 El antecedente inmediato de Bitcoin: Bitgold

Además de la creación de los Smart Contracts, Szabo también supo predecir el Bitcoin. En 2005 publicaba un artículo que llevaba por nombre “*Bitgold*” en el exponía **el problema que plantea el dinero tradicional y daba una posible solución**. El dinero tradicional está sujeto a una tercera parte que asegure su valor, pero esta dependencia implica cierta **arbitrariedad** que implica por ejemplo episodios de inflación e hiperinflación como ocurrió en el Siglo XX (Szabo, 2005). De hecho, ya de forma anterior Szabo había expuesto el problema de un *third party* como garante en su artículo “*Trusted Third Parties are Security Holes*” (Szabo, 2001) ya que introduce un riesgo inherente porque introduce posibilidad de robo o fallo técnico (Ammous, 2018). Así, Szabo proponía una alternativa basada en un protocolo por el cual se pudieran crear **bits infalsificables con cierta independencia y confianza mínima, es decir, una suerte de patrón oro, pero en bits** (Szabo, 2005).

Este modelo que proponía Szabo se acercaba de forma muy fidedigna al posteriormente creado BTC y recogía las aportaciones analizadas con anterioridad, a saber: el POW, la descentralización de Chaum o el *time-stamp* de Stornetta. De hecho, Finney en su explicación de RPOW exponía la utilidad de aplicar su aportación a este sistema: “*RPOW facilitaría el uso de los tokens POW como una forma de oro de bits al permitir que los tokens se pasen e intercambien de persona a persona*” (Finney, 2004). Sin embargo, es preciso salvar las distancias con BTC, entre ellas destaca que era un sistema basado en un sistema de *strings* en vez de bloques. Además, este sistema todavía presentaba una seguridad floja debido a que era susceptible al *Sybil Attack* y tampoco resolvía el *Byzantine Problem* (Tomov, 2019).

Aun exhibiendo diferencias sustanciales, las dos aportaciones de Szabo han sido de suma importancia para la revolución digital de blockchain a través de BTC. Se puede considerar estas dos grandes aportaciones como el recogimiento de los conceptos introducidos anteriormente y que alcanzan su máximo esplendor en Bitcoin y en las innovaciones que han acontecido con posterioridad.

2.5 B-Money: el vislumbamiento paralelo de Wei Dai

De forma análoga a la formulación de Szabo, en 1998 el ingeniero y criptógrafo chino **Wei Dai** fascinado por la obra de Tim May publicaba el artículo “**B-Money**” (1998). Partiendo de la teoría cripto-anarquista que exponía May, Dai clamaba **la necesidad de un medio de intercambio y una forma de hacer cumplir los contratos en una comunidad definida por la cooperación de sus participantes** (Dai, 1998). Su propuesta era la de un sistema distribuido en el cual todos los participantes podrían crear dinero y llevar a cabo transacciones con otros miembros de esa comunidad. En él, reminiscencia a los seudónimos de Chaum, todos los participantes serían anónimos, condición conseguida por la utilización de claves públicas (Tomov, 2019). Además, al ser distribuida cada integrante tendría una copia de la base de datos, a lo que denominó *wallet* (Dai, 1998). En definitiva, tanto el Bit Gold como el B Money han sido los prototipos de BTC y han conseguido recoger las aportaciones de todos los autores anteriores.

2.6 Movimiento Cypherpunk como motor del progreso técnico: las motivaciones humanísticas

Las aportaciones y mejoras expuestas en el apartado anterior no responden únicamente a una pretensión de mejora puramente técnica, respondían a un motivo ulterior impulsado por ciertos valores. Desde Diffie y Helman proponiendo su modelo criptográfico para procesos cotidianos, pasando por Chaum y su preocupación por la privacidad o Szabo y su voluntad de preservar la soberanía individual, se puede observar que más que la técnica, todos estos intelectuales perseguían mejorar la situación del individuo en una sociedad cada vez más digitalizada. Instaban a una **revisión de la libertad, la privacidad y la información** (Carrascosa, Kuchkovsky, &

Preukschat, 2017). El hilo conductor de todo el proceso que llevó a Bitcoin y a la posterior Blockchain ha sido mayormente ético.

Ese hilo conductor y preocupación ética fue la que impulso a varias personalidades del entorno informático y criptográfico comienzan a juntarse con unos valores comunes. Si bien, la mayoría de los autores explicados anteriormente son considerados **Cypherpunks**, es a principios de los años 90 cuando surgía la lista de correos Cypherpunk. En ella, destacados informáticos e intelectuales del mundo de la criptografía debatían sobre cuestiones, tanto técnicas como humanísticas. Entre ellos destacan: Adam Back, Jude Milhon, David Chaum, Eric Hughes, Timothy C. May, John Gilmore, Fen Labalme, Lance Cottrell, Nick Szabo, Richard Stallman, Romana Machado, Ron Rivest, Tatu Ylönen, Tim Berners-Lee y Ulf Moller (Bit2Me, 2021).

A finales de **1992 Eric Hughes, Timothy May y John Gilmore** comenzaron a reunirse mensualmente en Gilmore-Cygnus Solutions en San Francisco y se denominaron Cypherpunks (Lopp, 2016). Inspirados por el **Hacktivismo**, un Cypherpunk se define como:

Persona que utiliza la encriptación al acceder a una red informática para garantizar la privacidad, especialmente frente a las autoridades gubernamentales (Oxford Dictionary, 2021)

Para estos, la **censura y la vigilancia eran los dos males de la era informática**, pero veían la **encriptación como un medio para eludir ambos** (Anderson, 2020). Es decir, un movimiento con motivaciones profundamente humanísticas, que hicieron uso de sofisticadas técnicas de encriptación para evitar, por la vida de los hechos, que los Gobiernos pudiesen adueñarse de la información almacenada en las redes (Bastos, 2020). En ese mismo año, Hughes recogía en un texto con forma de manifiesto, las ideas y valores que motivaban e impulsaban a todos estos profesionales.

2.6.1 Eric Hughes y el Manifiesto Cypherpunk

En **1993**, el matemático, criptógrafo y programador americano **Eric Hughes** redactaba el “*Cypherpunk Manifesto*”, en el cual recogía por escrito y formalmente los principios que guiaban a este movimiento que había surgido de manera espontánea durante los años 80 y 90.

La preocupación principal, que se observaba por primera vez en el cambio de Diffie y Helman y la obra de Chaum es la **privacidad**, así, comienza el Manifiesto haciendo referencia a la cuestión:

*Privacy is necessary for an open society in the electronic age. **Privacy is not secrecy.** A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. **Privacy is the Power to selectively reveal oneself to the world** (Hughes, 1993).*

La privacidad es, como afirma otro de los grandes pensadores Cypherpunk Jonathan Logan, una **condición necesaria para entablar relaciones interpersonales significativas y veraces**, y también, para que una **persona pueda desarrollar su propio “yo” y asumir la responsabilidad individual** de las decisiones y acciones que se derivan de ellas (Logan, 2012). Hughes aplicó esta idea a las transacciones y defendiendo que, de la misma manera que cuando una persona compra una revista en una tienda el dependiente no necesita conocer su identidad, se debería garantizar y **solo tener conocimiento de lo que es esencial a la y transacción** (Hughes, 1993). Para poder cumplir esta pretensión se hace necesario el uso de la criptografía, haciendo visible el contenido de un mensaje únicamente al destinatario. Para este encriptar es *expresar el deseo de privacidad*, y hacer una encriptación débil, es *expresar el deseo de no tanta privacidad* (Hughes, 1993). En este sentido, es preciso matizar la cuestión que planteaba Schneier: si no estoy haciendo nada malo, **¿por qué debería esconderme?** (Lopp, 2016). Sería falaz caer en la premisa errónea de entender la privacidad como el ocultamiento de algo malo, la **privacidad es inherente a la dignidad del hombre**. Hay ciertas acciones cotidianas que pertenecen a nuestra intimidad, y en eso mismo reside el valor de la privacidad, en ocultar por ejemplo relaciones íntimas que no son per sé algo malo (Schneier, 2006).

Además, el enfoque que le da a este concepto consiste en un hacer, preservar la privacidad depende del interesado en ella, llama a la acción. Sin embargo, una acción cooperativa y no individual, ya que un sistema que es generalmente utilizado no puede ser cerrado.

2.6.2 El Crypto-Anarchist Manifiesto de Timothy May

Además de ser un reconocido ingeniero electrónico y científico de Intel, **Tim May (1951-2018)** fue un teórico político. Esa faceta suya es conocida por la fundación del **movimiento crypto-anarchist**, que bebía de la fuente filosófica del movimiento Cypherpunk. En **1988** publicaba “*The crypto Anarchist Manifiesto*” el documento que sentaba las bases del movimiento cripto anarquista.

En consonancia con sus predecesores y compañeros Cypherpunks, su escrito parte de la idea del anonimato y la privacidad:

“Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other” (May, The Crypto Anarchist Manifiesto, 1988)

La importancia de la aportación de May reside en que por primera vez se formaliza un documento que vas más allá del Manifiesto Cypherpunk, no sólo explica los principios que inspiraron todo este proceso de progreso, sino que sienta un corpus de teoría política (May, 1994).

Además de esta aportación, May publicó dos artículos más en los que especificaba cuestiones filosófico-políticas respecto a su teoría cripto-anarquista. En 1994 publicaba “*The Cyphernomicon*” documento en el cual se hace una exposición del pensamiento de May enmarcado en el pensamiento anarquista genérico, pero a través de la lente de las criptodivisas (Chohan, 2017). En definitiva, el desarrollo de May no es más que una actualización del pensamiento anarquista, más cercano al pensamiento anarcocapitalista y libertario que a un anarquismo colectivista, y con unos matices característicos de la tecnología que lo apoya.

2.6.3 Pretty Good Privacy y Phillip Zimmerman

En 1991 Phil Zimmerman publicaba el código de *Pretty Good Privacy (PGP)*, un paquete software para la encriptación de correo electrónico creado inicialmente como una herramienta para la **protección de los Derechos Humanos** (Zimmermann, 2021). Zimmermann produjo este software con la idea de proteger los DDHH de personas que necesitaban **comunicarse de forma segura debido a la opresión ejercida por sus gobiernos** (McLaughlin, 2006). A pesar de esa intención, el gobierno de los Estados Unidos trató de impedir su difusión en la red, y de otros softwares similares, por cuestiones de seguridad nacional. Hoy sigue siendo objeto de debate la condición de PGP como la Máquina Enigma utilizada por los Aliados en la segunda Guerra Mundial, o, por el contrario, como un simple algoritmo (Koepsell, 2000).

Si bien su aportación no fue decisoria para la creación de BTC, como si lo fueron la de otros compañeros Cypherpunks, su aportación tiene una **dimensión humanística de primordial importancia**. Zimmermann instó a una revisión de nuestra realidad, cuando los Padres Fundadores escribieron la Constitución, el derecho a una conversación privada era un derecho natural no sólo por el significado filosófico de natural, sino porque dada la tecnología de ese momento no existía amenaza a este posible (Zimmermann, 1999). Así, el propósito de su obra no es más que, al igual que sus compañeros, devolver la soberanía individual a las personas: *PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it* (Zimmermann, 1999).

En síntesis, desde la democratización de la criptografía a partir del DES y el cambio de clave Diffie-Hellman, lo que ha movido el progreso técnico en este campo de estudio ha sido un motor humanístico. Así, ha quedado demostrado que Bitcoin no fue algo tan innovador como se puede considerar a priori, ya que desde los años 70 se llevaban haciendo aportaciones a la cuestión. Y,

además, que las aportaciones que van apareciendo no emanan de un ansia de progreso técnico sino por una pretensión de mejorar la calidad de vida de los individuos, y preservar la esfera personal. El elemento transversal a todos los autores es la preocupación por la libertad y la privacidad del individuo. Por ello, Bitcoin evidencia un gran potencial en estos términos. De esta manera, se procederá en el siguiente apartado a conceptualizar las plataformas que serán objeto de análisis en este trabajo. En primer lugar, se definirá y explicará qué son Bitcoin y Ethereum, exponiendo sus partes, principios y funcionamiento. En segundo lugar, se procederá a conceptualizar las aportaciones y postulados de la Escuela Austriaca de Economía, visión metodológica que será utilizado para el análisis de las dos plataformas como garantes de la libertad individual.

3 MARCO TEÓRICO

3.1 Conceptualización de Blockchain

“Una blockchain no es otra cosa que una **base de datos** que se halla **distribuida** entre diferentes participantes, **protegida criptográficamente** y organizada en **bloques de transacciones** reales relacionados entre sí **matemáticamente.**” (Preukschat, 2017). Es decir, consiste en un gran libro contable digitalizado que utiliza criptografía fuerte para sus transacciones, y que, por ello, no puede ser modificada. Es una plataforma que permite a todo el mundo discernir lo que es verdad de lo que no, y que, **al ser un código abierto permite a todo el mundo que lo desee ejecutarlo** (Tapscott & Tapscott, 2017). Lo que distingue a blockchain de cualquier otra base de datos son sus reglas específicas para la inscripción de los datos. Este protocolo le confiere sus características distintivas: consistencia, dado que no puede entrar en conflicto con otros datos; inmutable, dada su encadenación y encriptación no es posible su modificación; poseíble, la albergan todos los nodos de la red, es descentralizada (Song, 2018).

La red en la que opera una blockchain está compuesta por unos elementos básicos:

- a) **Nodos:** ordenadores con la capacidad computacional para ejecutar, ya sean personales o una supercomputadora (Preukschat, 2017). Para que estos sean capaces de comunicarse entre sí cuentan con un protocolo.
- b) **Protocolo:** un protocolo se define genéricamente como un conjunto de convenciones (Cerf & Kahn, 1974) para que los ordenadores puedan “entenderse”. El más conocido y cotidiano es el protocolo de comunicación TCP/IP el cual consiste en un mecanismo de transporte para entregar datos entre ordenadores o entre ordenadores y terminales utilizando un protocolo para poder dotar de sentido al mecanismo (Cerf & Kahn, 1974). Este protocolo establece, por ejemplo, un número de bits determinado para los paquetes que se pueden enviar al servidor, la comunicación ACK-SYN... DE esta manera

blockchain cuenta con un protocolo fiable que es el soporte de muchas cadenas de bloques distintas (Tapscott & Tapscott, 2017).

- c) **Criptografía:** la criptografía se ocupa del diseño de procedimientos para cifrar es decir para enmascarar una determinada información de carácter confidencial (de la Guía, Hernández, Montoya, Muñoz, & Fúster, 2004). En la blockchain juega un papel esencial para evitar el fraude o la manipulación de la información, así como actúa de garante de la privacidad
- d) **Consenso:** es el fundamento que permite que todos los participantes en el blockchain puedan confiar en la información que se encuentra grabada en ella (Preukschat, 2017). La implementación de algoritmos de consenso es lo que dota de seguridad a la red (Zheng, Xie, Dai, Chen, & Wang, 2017).

En definitiva, la blockchain es una tecnología que nace como la agrupación de todas las aportaciones teóricas, explicadas en el estado de la cuestión, que dieron lugar a BTC. Sin embargo, lejos de haberse quedado en la condición posibilitadora de las criptomonedas, ha llegado para generar un **cambio de paradigma en nuestro entender del internet**. De hecho, blockchain responde a una nueva revolución de internet, el *Internet of Value* o Internet del Valor (Ripple, 2017). Se trata de una **forma instantánea de transmitir valor**, de la misma manera que se transmiten fotos o videos, no sólo valor financiero sino todo tipo de activos como por ejemplo propiedad intelectual (Truong, Um, Zhou, & Myoung Lee, 2018).

3.2 Conceptualización de Bitcoin

Bitcoin es la moneda **con mayor capitalización bursátil** del mercado de las criptomonedas actual (CoinMarketCap, 2021), fue la primera criptomoneda en aparecer en 2009 y desde la creación del bloque génesis el 3 de diciembre de ese año, y, la primera transacción el 12 de diciembre entre Nakamoto y Hal Finney no ha hecho más que crecer (Bit2Me, 2021). Hoy en día se encuentra sujeta a un fuerte debate en la opinión pública y en el mundo de las finanzas. Son multitud los gurús del mundo financiero quienes han criticado en el pasado a esta divisa digital. Desde las numerosas declaraciones de Warren Buffet sobre este activo, calificándolo como un engaño y afirmando que nunca dispondría de ellas (Buffett, 2020) o las de Jamie Dimon, consejero delegado de JP Morgan, en 2017 y la posterior prohibición sobre ellas por parte de JP Morgan en 2018 (Partz, 2019). Sin embargo, parece acontecer una tendencia de confianza hacia esta nueva tecnología entre los que criticaban sus inicios, la adquisición de Poloniex en 2018 por parte de Circle y respaldado por Goldman Sachs, o la integración de la tecnología de Zcash en JP Morgan (Tapscott & Tapscott, 2017). Siendo BTC la criptodivisa pionera y el sujeto de este análisis es preciso dar una definición para su posterior estudio.

Bitcoin es un **sistema digital de pagos de tipo p2p** que con su nacimiento pretendía solucionar el problema del doble gasto. Un sistema en el cual la **red marca el tiempo de las transacciones mediante un Hash en una cadena continua de pruebas de trabajo** basadas en el Hash, formando un **registro que no puede cambiarse sin rehacer la prueba de trabajo** (Nakamoto, 2008). La motivación de Nakamoto era la de trasladar los beneficios del dinero tradicional (falta de intermediarios e irrevocabilidad de las transacciones) al reino digital, combinado con una política monetaria que evitara la manipulación (Ammous, 2018).

3.2.1 Sistema Peer 2 Peer y la Descentralización

Una de las grandes innovaciones de BTC es su condición de p2p. Esta condición de par a par es la que **elimina el problema del intermediario**, es decir, los pagos son realizados de un usuario a otro sin necesidad de que la divisa atraviese ninguna institución. El funcionamiento es similar al del protocolo de descarga de archivos **BitTorrent**. En BitTorrent, los archivos divididos en trozos, y los descargadores de un archivo intercambian trozos subiendo y bajando de forma similar a la de un *tit for-tat* para evitar el comportamiento parasitario (Pouwelse, Garbacki, Epema, & Sips, 2005). De la misma manera, en BTC todos los mineros son poseedores de partes de la *distributed ledger* y se convierten en origen cuando intervienen en una transacción dentro de la red (Nakamoto, 2008). En definitiva, se puede resumir esta idea en la desintermediación como regla, la continuidad y funcionalidad no dependen de una sola parte (Vivas, 2017).

3.2.2 Reglas de funcionamiento de Bitcoin

Los bloques que conforman la cadena blockchain están formados por texto. Estos bloques son el equivalente a las páginas de un libro de contabilidad gigante que está distribuido, y, por ello, el texto consiste en los datos de las transacciones (Chamapgne, 2014). Estos bloques **no han de superar el megabyte** de tamaño, tal y como añadía Nakamoto en una nueva línea de código, y en él se meten todas las **transacciones** en cola que quepan, **aproximadamente 2000 o 2200** (Bit2Me, 2021).

Figura 1. Historial de transacciones Bitcoin a día 3 de marzo de 2021


Altura	Fecha	Transacciones	Minado por	Tamaño del bloque (bytes)
 673021	3/3/21 19:46	2567	AntMiner	897613
 673020	3/3/21 19:28	2190	SlushPool	909790
 673019	3/3/21 19:27	2947	Unknown	875034
 673018	3/3/21 19:01	1638	Unknown	932016
 673017	3/3/21 18:53	3428	Unknown	939932

Fuente: (Bit2Me, 2021)

Como se puede observar en la fotografía, los bloques contienen aproximadamente el mismo número de transacciones, varía en función de la complejidad de la transacción, y nunca

sobrepasan el 1MB. Además de las transacciones, los bloques incluyen más **elementos** que merecen un análisis más detenido: un *header Hasheado*, la fecha y hora de creación, la transacción de recompensa al minero y un POW.

Figura 2: Anatomía de un Bloque

Resumen			
Height	673,032	Versión	0x3fff0000
confirmaciones	7	Dificultad	22.44 T / 21.72 T
Tamaño	1,327,498 Bytes	Bits	0x170cf4e3
Stripped Size	888,651 Bytes	Nonce	0xa492c029
Weight	3,993,451	Transmitido por	AntPool
Conteo de transacciones	1,860	Hora	2021-03-03 21:03:34
		Hash de bloque	000000000000000000000000c8b90c2c2c42b25e26109074e3c43052cc9e392e6490a
		Bloque anterior	0000000000000000000000002639bb903d0750820bab3f22947d45523aa95f79d4ff1
		Bloque siguiente	000000000000000000000000a3b9f337ab6763e1bc8398fae8680e415355e281a8554
		Raiz Merkle	a65fba4f2d317aa1ab0966f11f7c5c5dd4b9203decfb74bf5353217a541df64f
		Other Explorers	 BLOCKCHAIR

Fuente: (BTC.com, 2021)

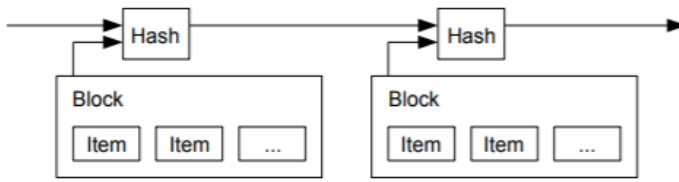
En la fotografía del libro contable se puede observar cómo el bloque tiene el número de transacción, en este caso 673.032, las confirmaciones que ha tenido dentro de la red para ser confirmado, el peso y número de transacciones, y, a la derecha, el *header* o Hash de bloque, el Hash anterior y el Hash siguiente.

3.2.2.1 Header y el Hash

El primer elemento conformante de un bloque es el *header*, es decir, un **encabezamiento**. El título es una cabecera de 80 bytes perteneciente a un único bloque que se *Hashifica* repetidamente para crear una prueba de trabajo (Bitcoin Developer, 2021). El término **Hash** refiere a un **mecanismo criptográfico** que se denomina función Hash. Las funciones Hash se denominan frecuentemente funciones de compendio de mensajes. Su objetivo es **extraer una cadena de bits de longitud fija de un mensaje** (archivo informático o imagen) **de cualquier longitud**. Se utilizan normalmente para firmas digitales, es decir, para autenticar mensajes y además, son hipersensibles ya que cualquier modificación del mensaje “m”, $H(m') \neq H(m)$, daría un *bit-string* radicalmente distinto (Fridrich & Goljan, 2000). De esta manera, Nakamoto aplicó el concepto de Hash, y el sistema de *Hashcash* creado por Adam Back y explicado anteriormente, para poder marcar los bloques, como también apuntaban Stornetta y Haber (Nakamoto, 2008). Además, dota de mayor seguridad ya que sólo el que conoce el código criptográfico para crear el Hash es el único capaz de descifrarlo, quién lo lea sin acceso al código no puede descifrarlo.

De esta manera, cada bloque tiene un Hash que le identifica y que le sitúa en un tiempo determinado, pero también incluye el Hash del bloque anterior, mecanismo que posibilita que exista la cadena, y así no se pueda modificar:

Figura 3. Timestamp Server

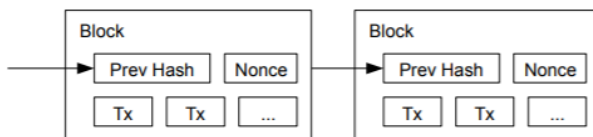


Fuente: (Nakamoto, 2008)

3.2.2.2 Proof of Work o Nonce

El concepto creado por Dwork y Moni y actualizado por numerosos académicos es una parte fundamental de BTC. El POW que, por definición, consiste en un problema matemático para evitar el uso masivo de recursos compartidos, en este caso se utiliza como prueba de dificultad. La **prueba de trabajo** consiste en **buscar un valor** que, cuando se convierte en Hash que **comienza con un número de bits cero**. El trabajo medio requerido es exponencial en el número de bits cero necesarios y puede verificarse ejecutando un único Hash (Nakamoto, 2008). Es decir, funciona de forma conjunta con el Hash para evitar la manipulación de la información de los bloques (Bit2Me, 2021). Es precisamente en esto en lo que consiste el **proceso de minería**, en **resolver la prueba de trabajo** encontrando un valor de nonce criptográfico dentro de un rango determinado. La red escala el rango para mantener un promedio de un nuevo bloque cada diez minutos (Kumar, Duwe, & Vilim, 2016).

Figura 4: Funcionamiento del Proof of Work y Nonce



Fuente: (Nakamoto, 2008)

3.2.3 Proceso de creación de los Bitcoins o Minería

Para llegar a esa anatomía del bloque hay un proceso previo, y se denomina **minería**. El proceso comienza cuando se hace una **petición de transacción**, es decir, la transacción que va a tener lugar se difunde a todos los nodos (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008). La solicitud de transacción incluye: la dirección BTC del pagador, que contiene la fuente de fondos para el pago; la dirección de BTC del receptor (receptor del pago); la cantidad de BTCs que han sido transferidos (Chamapgne, 2014). Esta **información es el texto** que se mencionaba anteriormente que **va dentro de cada bloque**. Una vez es **transmitida esta información** cada nodo recopila las nuevas transacciones, junto al Hash del bloque anterior y el **factor de dificultad actual**, que es la medida de la dificultad del *nonce* correcto requerido para la generación de bloques (Dev, 2014).










El minero que consigue resolver la prueba de trabajo **transmite el bloque a todos los nodos de la red**, es decir, a los demás mineros. Los integrantes de la red **examinan si las transacciones que contiene son válidas** y no se han gastado anteriormente, si es así los nodos aceptan el bloque de **forma democrática** y se une a la cadena (Nakamoto, 2008).

Todo este proceso está determinado por la **condición de dificultad**. En 2010 Satoshi Nakamoto hacía una nueva aportación en la lista de correos en la que ajustaba y profundizaba en la condición de dificultad. Esta idea consiste en un **incremento situacional del nivel de dificultad de la prueba de trabajo, dependiendo del nivel de competencia de los mineros** (Chamapgne, 2014). Es importante que estas pruebas de trabajo sean lo suficientemente duras para que los mineros tengan la oportunidad de unificar sus puntos de vista en presencia de un adversario que interfiera pero que tenga un poder computacional limitado, pero lo suficientemente fáciles como para que se puedan resolver regularmente y permitan a los mineros progresar. Como tal, a medida que la población de mineros evoluciona con el tiempo, también debería hacerlo la dificultad de estas pruebas (Kiayias, Garay, & Leonardos, 2017).

La dificultad mínima es de 32 bits cero, por lo que incluso si una sola persona dirigiera un nodo, la dificultad no es más fácil que eso. Durante la mayor parte del año pasado, estuvimos rondando por debajo del mínimo. El 30 de diciembre lo superamos y el algoritmo se ajustó a una mayor dificultad. Desde entonces, la dificultad ha aumentado con cada ajuste. El ajuste del 4 de febrero lo llevó de 1,34 veces la dificultad del año pasado a 1,82 veces más difícil que el año pasado. Eso significa que sólo se genera un 55% de monedas por la misma cantidad de trabajo. La dificultad se ajusta proporcionalmente al esfuerzo total de la red. Si el número de nodos se duplica, la dificultad también se duplicará, devolviendo el total generado a la tasa objetivo (Nakamoto, 2010).

Esta condición de dificultad consiste en que los Hashes generados para cada bloque deberán empezar por un **número determinado de ceros**, que como se ha explicado, va variando en función de la competencia de cada momento en la red. De esta forma, el Hash puede resolver la prueba de trabajo sin cumplir la condición de los ceros. A continuación, se muestra una parte del libro de transacciones en las que se puede observar cómo todos los Hashes tienen un número de ceros determinado en cada momento.

Figura 5. Últimas transacciones realizadas con Bitcoin a 3 de marzo de 2021

Height	Transmitido por	Tamaño(B)	Recompensa	Hora	Hash de bloque
673,038	 BTC.com	1,357,337	7.46224458 BTC	5 minutes ago	000000000000000000000004b153b54c34e9ae5ab1802ca4ebd6dd9e285c592e47aa
673,037	 Binance Pool	1,416,492	7.54803212 BTC	24 minutes ago	000000000000000000000005b6266fc291a889caff9be7f0852a15d7c451cc3bb433
673,036	 AntPool	1,299,947	6.91578556 BTC	45 minutes ago	0000000000000000000000030448df3ef64948f74691a9e2ba404e0fe69c3d5abf1
673,035	 BTC.com	1,221,810	6.81965960 BTC	49 minutes ago	0000000000000000000000037a28df33b851b5f41d39973ca09d588b22bb57da4719
673,034	 AntPool	1,150,732	7.08269261 BTC	50 minutes ago	000000000000000000000007fc82da82e1eee5d310938bf09936e42f2739126f3f31
673,033	 AntPool	1,090,787	7.29307318 BTC	52 minutes ago	00000000000000000000000a3b9f337ab6763e1bc8398fae8680e41535e281a8554
673,032	 AntPool	1,327,498	7.64505334 BTC	55 minutes ago	00000000000000000000000c8b90c2c2c42b25e26109074e3c43052cc9e392e6490a
673,031	 Huobi.pool	1,257,532	6.98452913 BTC	1 hora 11 minutes ago	000000000000000000000002639bb903d0750820bab3f22947d45523aa95f79d4ff1
673,030	 F2Pool	1,304,941	7.37417051 BTC	1 hora 16 minutes ago	00000000000000000000000cbc4598cfe52190846932df0b680e8fa70ee3529f35e8

Fuente: (BTC.com, 2021)

El propósito de esta condición no sólo reside en evitar que múltiples mineros piratas se agrupen para poder aprobar transacciones falsas, sino que también limita el tiempo de creación. La condición está fijada para que estadísticamente se tarden 10 minutos y cada 2016 bloques se revisa para hacer un ajuste, tal y como se explica en el correo citado.

Después de todo el proceso, el minero que consigue crear el bloque obtiene una recompensa, y así surgen los nuevos bitcoins. Si bien en el dinero tradicional, la moneda la puede emitir el Estado, aquí la única forma de generar Bitcoins es minando bloques. Esta recompensa se encuentra programada dentro del protocolo que hace funcionar a la criptomoneda. Su función, es la de ser un incentivo para que los mineros realicen su trabajo (Maldonado, 2020)

3.3 Conceptualización de Ethereum

En 2013, el joven programador ruso **Vitálík Buterin** publicaba un *whitepaper* proponiendo un uso diferente de la blockchain: **Ethereum**. Si bien Bitcoin es un **protocolo de código abierto**⁶ para servir como sistema de pago, Ethereum es **una plataforma para aplicaciones descentralizadas** o DApps (Buterin, 2014). Las redes blockchain de código abierto como Ethereum y Bitcoin son kits que permiten poner en marcha un sistema económico en software, con gestión de cuentas y una unidad de intercambio nativa para pasar entre cuentas. Algo así como el juego Monopoly. La gente llama a estas unidades nativas de intercambio monedas, tokens o criptomonedas, pero no son diferentes de los tokens de cualquier otro sistema: son una forma de

⁶ Un software de código abierto es aquel que permite a los usuarios utilizar, estudiar, mejorar y/o redistribuir el mismo, bien en su forma original o con las modificaciones que se realicen con posterioridad. Para estudiar un software, para mejorarlo o adaptarlo a las necesidades de cada uno, es imprescindible disponer de un código fuente. Sin embargo, no debemos confundir software libre con el software de código abierto. El software libre requiere obviamente disponer de código abierto si bien lo contrario no es siempre cierto. Existen numerosas licencias de código que aunque aseguran la disponibilidad del código fuente impiden su modificación o su uso en determinados fines por ejemplo comerciales o militares (Escudero, 2017).

dinero que sólo se puede utilizar dentro de ese sistema. Pero Ethereum va un paso más allá ya que posibilita la **escritura de contratos financieros con otros usuarios del sistema** (Dannen, 2017).

El impulso para la creación de Buterin, viene por tratar de facilitar las transacciones entre individuos que consienten y que, de otro modo, no tendrían medios para confiar los unos en los otros. Esto puede deberse a la separación geográfica, la dificultad de interconexión, o quizás la incompatibilidad, incompetencia, falta de voluntad, incertidumbre, inconveniencia o corrupción de los sistemas legales existentes (Wood, 2014). De hecho, lo más característico de Ethereum son, lo que anticipó Nick Szabo en 1994 (Szabo, 1995), los **contratos inteligentes** o *Smart Contracts*. Gracias a su lenguaje de tipo Turing complete⁷, la plataforma Ethereum es capaz de expresar todos los cálculos computacionales en contratos inteligentes (Tikhomirov, 2018).

Además, la creación de Ethereum tiene unas importantes **implicaciones éticas** ya que tiene como objetivo reconfigurar el entender que tenemos sobre internet. Crear un nuevo concepto de internet que ostente ciertos rasgos en favor del individuo, a saber:

- *Un internet donde dinero y pagos están integrados.*
- *Un internet donde los usuarios pueden ser dueños de sus datos, y tus aplicaciones no te espían ni te roban.*
- *Un internet donde todos tienen acceso a un sistema financiero abierto.*
- *Un internet construido sobre una infraestructura neutral y de acceso libre que ninguna empresa ni persona controla* (Ethereum, 2021)

Queda patente la importancia y el potencial humanístico que tiene esta plataforma. A fin de hacer una consideración más profunda de ella es preciso analizar varios de los elementos fundamentales que lo posibilitan. Por ello, se procederá a definir los conceptos de Dapps y Proof of Stake.

3.3.1 Las aplicaciones descentralizadas o DApps

De la misma manera que internet es una plataforma para aplicaciones como el correo electrónico, telnet o www, Ethereum sirve de plataforma para el desarrollo de aplicaciones (Kumar, Shrivastava, & Tanwar, 2020). Una DApp se describe como **trustless**, es decir, sin confianza⁸; y p2p. Es decir, una aplicación normal, pero con la característica distintiva de que no hay un único servidor o entidad que lo controle como en un modelo cliente-servidor (Kishimoto, Masuda, Yano, & Dai, 2020). De la misma forma que los Smart Contracts, se ejecuta en un protocolo de consenso seguro a través de una red de ordenadores, y estas suelen controlar activos en la cadena,

⁷ Un lenguaje proveniente del modelo matemático de la Turing Machine que incorpora entre otros elementos la combinatoria o la máquina de estados finitos.



















⁸ Se dice que son de confianza mínima porque no precisan confiar en una persona o ente centralizado sino que es suficiente con confiar en la función, es decir, en que el código se ejecutará automáticamente (Szabo, 2017).

como criptomonedas o tokens (Szabo, 2017). De esta manera, se pueden reducir las características de las DApps a (Awad, 2021):

- **Descentralizadas**, es decir, independientes.
- **Deterministas**: se ejecuta el código independientemente del entorno.
- **Basadas en un Turing Complete**: dados los recursos requeridos, la DApp puede llevar a cabo cualquier acción.
- **Aisladas**: se ejecutan en un entorno virtual denominado Ethereum Virtual Machine⁹ (EVM) que conlleva que si el contrato tuviera un bug no amenazaría el correcto funcionamiento de la red de blockchain (Awad, 2021).

El ejemplo pionero de utilización de las DApps en Ethereum fueron las *Initial Coin Offers* o ICO, gracias a la cual un proyecto puede recaudar millones de dólares aportados por una comunidad global de inversores y sostenedores (Tapscott & Tapscott, 2017). A raíz de esa aplicación, han sido numerosas las DApps que han ido surgiendo y para usos de lo más diversos, desde *gaming*, a intercambio de activos digitales, hasta *marketplace*. A continuación, se muestran las DApps más populares por uso:

Figura 6. Ranking de DApps más utilizadas en Ethereum

	CATEGORY	PROTOCOL	BALANCE	USERS	VOLUME	ACTIVITY	
1	 Uniswap	Exchanges	ETH	\$7.03B	43.46k +7.14%	\$783.11M	
2	 SushiSwap	Exchanges	ETH	\$5.37B	4.55k +29.51%	\$446.61M	
3	 Rarible	Marketplaces	ETH	\$480.12	4.16k +4.23%	\$839.59k	
4	 1inch.exchange	Exchanges	ETH	\$3.50k	2.91k -6.25%	\$72.74M	
5	 OpenSea	Marketplaces	ETH	\$17.27k	2.17k +2.84%	\$2.63M	
6	 Synthetix	DeFi	ETH	\$218.56k	1.76k -24.39%	\$0.00	
7	 Axie Infinity	Games	ETH	\$2.39M	1.49k +49.75%	\$197.58k	
8	 NEW Alchemix	DeFi	ETH	\$18.01M	948 +65.73%	\$3.11M	
9	 WBTC	DeFi	ETH	\$480.18k	766 -4.84%	\$0.00	

Fuente: (DappRadar, 2021)

3.3.2 La alternativa de Ethereum para el PoW: Proof of Stake

La **Proof of Stake (PoS)** o Prueba de Participación es uno de los dos protocolos de consenso más utilizados, es un algoritmo que de la misma manera que PoW trata de crear consenso entre las

⁹ La Ethereum Virtual Machine o EVM, es una máquina virtual que forma parte del ecosistema blockchain de Ethereum. Esta es capaz de ejecutar una amplia gama de instrucciones que le permiten una gran flexibilidad a la hora de realizar distintas operaciones. Utiliza un lenguaje de programación creado específicamente para los Smart Contracts que se denomina Solidity (Bit2Me, 2021).

partes que integran la red (Bit2Me, 2021). Además del problema del **acaparamiento que los pools de minería** pueden hacer sobre el hasheado de los bloques, PoW plantea otro problema es el completo **anonimato de** los fragmentos que validan transacciones con un pequeño porcentaje del hash power porque se expone a posibles ataques de hackers. Por ello, Buterin ofrece PoS como alternativa ya que debido a los esquemas avanzados de prueba de trabajo, como las torres de rompecabezas, y la algoritmos de consenso bizantinos tolerantes a fallos utilizados en las cadenas de bloques privadas: los participantes en el proceso de consenso tienen algún tipo de identidad, aunque sólo sea la **identidad criptográfica seudónima de una dirección**, por lo que podemos resolver el problema del "ataque dirigido" con **esquemas de muestreo aleatorio**, seleccionando aleatoriamente un conjunto de nodos para **procesar cualquier conjunto de transacciones de todo el grupo de validadores**, lo que hace imposible que los atacantes se dirijan específicamente a una transacción concreta o a un fragmento concreto (Buterin, 2016).

En definitiva, se trata de una actualización de protocolo que hizo Ethereum y seguidamente Cardano, dado que resuelve la dependencia sobre el consumo energético y reduciendo el coste, materializado en unas *fees* más bajas (King & Nadal, 2019).

3.4 Conceptualización de la Escuela Austriaca de Economía

La **Escuela Austriaca de Economía** es una escuela de pensamiento económico fundada por **Carl Menger (1840-1921)** en el último tercio del siglo XIX, y que posteriormente ha albergado a autores como: Ludwing Von Mises, Eugen von Böhm-Bawerk, Murray Rothbard, Friedrich Hayek, o el contemporáneo español Jesús Huerta de Soto (Instituto Xoán de Lugo, 2021). A pesar de ser haber sido creada a finales del **siglo XIX**, se puede afirmar que encuentra sus orígenes en el **XV** cuando los **Escolásticos**, seguidores de Santo Tomás de Aquino, que estudiaban en la **Escuela de Salamanca** observaron la existencia de leyes económicas y de causa y efecto que funcionaban de forma similar a las naturales (Mises Institute, 2021). Y, yendo antes en la historia, se encuentran ideas en el pensamiento jurídico romano (Leoni, 1974, pág. 116). Si bien, los coetáneos de Menger no se interesaron, e incluso dificultaron su obra, hasta bien entrados los años 70 no había Escuela, sólo estaba Menger (von Mises, 2003).

La principal aportación de esta escuela es:

“el desarrollo de una Ciencia Económica siempre basada en el ser humano hoy protagonista de todos los procesos y eventos sociales (subjetivismo), así como, la creación sobre la base del subjetivismo y, por primera vez en la historia del pensamiento humano, de toda una teoría formal sobre el surgimiento espontáneo y evolución de todas las instituciones sociales (económicas, jurídicas y lingüísticas) entendidas como esquemas pautados de comportamiento” (Huerta de Soto, 1994, pág. 18)

A pesar de haber estado siempre sometida a un interesante debate interno, la Escuela Austriaca se caracteriza por una serie de principios que el economista **Fritz Machlup (1902-1983)** exponía por ser comunes a la mayoría de los autores (Leeson & Boettke, 2002):

1. **Individualismo metodológico**: en última instancia, podemos justificar los fenómenos económicos como resultado de las acciones de los individuos; por lo tanto, las acciones individuales deben servir como base de la teoría económica.
2. **Subjetivismo metodológico**: las cuestiones de valor, expectativas, intención y conocimiento son creadas en la mente de los individuos y deben ser consideradas en esta perspectiva.
3. **Marginalismo**: todas las decisiones económicas se toman al margen, son elecciones relativas a la última unidad añadida o sustraída de un stock determinado. La ley de la utilidad marginal es “una ley estrictamente praxeológica, es decir, inserta en la propia lógica de la acción humana” (Huerta de Soto, 1994, pág. 22)
4. **Gustos y preferencias**: la demanda de bienes y servicios por parte de los individuos depende de sus valoraciones subjetivas de la capacidad de dichos bienes y servicios para satisfacer sus deseos
5. **Coste de oportunidad**: Todas las actividades tienen un coste, y este coste es la alternativa más valorada a la que se renuncia porque los medios para satisfacerla se han dedicado a algún otro uso (más valorado).
6. **Estructura temporal del consumo y la producción**: Todas las decisiones tienen lugar en el tiempo. Las decisiones sobre cómo asignar los recursos para el consumo y la producción de consumo y producción a lo largo del tiempo están determinadas por las preferencias temporales de los individuos (Machlup, 1982).

Y añade otros dos más que han sido más controvertidos:

7. **Soberanía del consumidor**
8. **Individualismo político**: para poder existir ha de cumplirse la condición de la libertad económica (Machlup, 1982)

Estos principios ponen de manifiesto la peculiaridad de la Escuela Austriaca de Economía en comparación con su antagonista, la Escuela Keynesiana. Si bien es un corpus de análisis económico, la Escuela Austriaca también es eminentemente humanista y multidisciplinar, ya que parte del ser humano tal y como es en la realidad y deja a un lado los estereotipos robotizados del *homo economicus* que centran los modelos matemáticos Keynesianos (Huerta de Soto, 2012).

Dentro de todas las aportaciones de los autores de la Escuela Austriaca, se procederá a analizar los elementos y teorías que conciernen al objeto de este trabajo. Así, en primer lugar, se analizará la **teoría monetaria austriaca**, y **el origen del dinero**. Conceptos que serán utilizados en la

primera parte del análisis referido a Bitcoin. En segundo lugar, se analizará la **fundamentación filosófica** de la Escuela, principalmente el concepto de coacción, orden espontáneo y procesos de mercado. Estos conceptos serán tratados más adelante, en el análisis, en referencia a Ethereum y las blockchain.

3.4.1 Aportaciones Económicas. Teoría Monetaria

En cuanto a esta cuestión respecta, la obra más importante es *The Origins of Money (1892)* de Carl Menger, en la cual explica que **no es el gobierno quien crea el dinero sino el mercado**. Los individuos deciden que bienes son más susceptibles de ser medios de intercambio (Mises Institute, 2021), y por ello, estas instituciones forzosamente van surgiendo de manera espontánea y evolutiva del proceso social de interacciones humanas que, para Menger, constituyen el objeto de la ciencia económica (Huerta de Soto, 2016, pág. 51).

3.4.1.1 El Origen Evolutivo de Menger

En una sociedad que funciona a través de la división del trabajo, resulta necesario distribuir entre sus miembros el excedente de producción, y esta distribución puede darse de forma centralizada o descentralizada (Rallo, El Origen Evolutivo del Dinero, 2014). Esa pretensión de distribución e intercambio de bienes se topa con el problema de los diferentes *degrees of salebleness* o **grados de vendibilidad** (Menger, 2009, pág. 21). Atendiendo a los inicios de la historia del dinero, los intercambios se formalizaban en **trueques** que podían ser o bien spot, **intercambio directo** y al contado de dos mercancías; o bien, diferido, intercambio directo y aplazado de dos mercancías (Rallo, 2014). El trueque directo exigía que la otra parte tuviera lo que una parte desea, y viceversa, es decir, el trueque presenta el **problema de la doble coincidencia de necesidades** (Huerta de Soto, 2010), raras veces ocurre que lleguen a encontrarse esas dos (Menger, 1874, pág. 119). Es un error de la economía asumir que todas las mercancías en un momento y un mercado determinado pueden suponerse en una relación de intercambio definida, es decir, que pueden ser intercambiadas en cantidades definidas a voluntad (Menger, 2009, pág. 23).

En este contexto, debido a las restricciones que acarrea el cambio directo y a la necesidad de realizar intercambios, se inicia un **proceso descentralizado de prueba y error en el que tienden a preponderar los comportamientos que mejor coordinan los ajustes sociales** (Huerta de Soto, 1994, pág. 23), que en este caso es: en vez de exigir aquello que necesitan, exigir un bien no por esperar usarlo como bien de consumo o producción, sino como un bien sujeto a una mayor frecuencia de intercambios, es decir, más líquido (Huerta de Soto, 2010). En palabras de Menger, se considera **más líquido a un activo** “según la mayor o menor facilidad con la que se puede disponer de ellos en un mercado en cualquier momento conveniente a los precios corrientes de compra” (Menger, 2009, pág. 25).

3.4.1.2 *El Teorema de Regresión de Mises*

Mises toma como punto de partida un orden económico basado en la división del trabajo, propiedad privada y el libre intercambio de bienes y servicios (von Mises, 1997, pág. 3). Y tomando como base la aportación de Menger, **Ludwig von Mises** elaboró el **Teorema de la Regresión**, siendo su principal tesis la idea de que para que el dinero ha de ser un bien con ciertas cualidades antes de ser utilizado como tal (Šurda, 2014).

Este teorema viene a resolver el problema del razonamiento circular que se pensaba que existía en relación con la aplicación de la ley de la utilidad marginal al dinero (Huerta de Soto, 1994, pág. 27). Por ello, Mises alega que la **demanda de una moneda hoy viene por el valor que tuvo ayer**, “una moneda se demanda hoy básicamente porque se piensa que mañana va a conservar su valor, va a mantener su poder adquisitivo. De manera similar, en el pasado se demandó esa moneda porque se pensó que hoy en día mantendría su valor” (OroyFinanzas, 2015). Es decir, la **utilidad marginal del dinero en un momento no depende de los mismos precios que ella genera, sino que depende de los precios registrados con anterioridad** (Almará, 2021).

Además, Mises distinguía entre valor de uso y valor de cambio, constituyendo así un carácter distintivo al dinero. Si bien Mises parte de la idea del bien con mayor negociabilidad para ser utilizado como medio de intercambio (von Mises, 1997, pág. 6), añade el valor de cambio basado en una cosa distinta a su función monetaria para poder considerar a un bien dinero (Grau Navarro, 2020). Es importante mencionar, que Mises consideraba al dinero también como un depósito de valor, por ello, el oro, **gracias a su durabilidad y maleabilidad**, conserva y es fácil de utilizar como medio de intercambio. De ahí su enorme ventaja respecto a otros metales (Matarán, 2020).

3.4.1.3 *Otras aportaciones económicas: la Teoría del Ciclo Económico y la Imposibilidad del Socialismo*

Además de la teoría monetaria que concierne al objeto de este Trabajo de Fin de Grado, la Escuela Austriaca ha hecho otras aportaciones de suma importancia a la Ciencia Económica. Tomando las teorías subjetivas del capital e interés de Böhm-Bawerk, Mises llegó a la conclusión de que la **concesión expansiva de créditos sin respaldo** de ahorro efectivo al que daba lugar el sistema bancario basado en coeficiente de reserva fraccionaria guiado por un Banco Central **generaba un crecimiento cíclico y descontrolado de la oferta monetaria** (Huerta de Soto, 1994, pág. 28). Es decir, al expandir los bancos la oferta de dinero **empuja al tipo de interés por debajo del tipo natural**, o sea, el del mercado libre que refleja la voluntad de sus participantes (Rothbard, 2009). Estos sufren una reducción artificial que provoca un desajuste en el sistema de producción que acaba por reajustarse con una recesión (Rallo, 2013). Hayek contribuyó de igual manera a la formulación de **la Teoría del Ciclo Económico** en un intenso debate con John Maynard Keynes (Huerta de Soto, 1994, pág. 36).

Por último, una de las aportaciones más interesantes es la refutación austriaca del socialismo, demostrando ser un sistema teóricamente imposible por el **problema del cálculo económico**. Hayek alegaba en **La Arrogancia Fatal (1988)** la imposibilidad de fijar precios por la falta de información de los planificadores centrales (Rallo, 2010), ya que como se ha expuesto, la Escuela Austriaca se sirve del subjetivismo.

3.4.2 Fundamentación filosófica y política

La Escuela Austriaca ha hecho aportaciones muy valiosas para el campo de la ciencia política. Su atención se ha dirigido principalmente, y como se mencionaba con los principios de Machlup anteriormente, a los **procesos dinámicos que acontecen en el mercado**, donde afloran **características como la espontaneidad, creatividad y el orden espontáneo** (Huerta de Soto, 2009). Es preciso traer a colación estos elementos por la influencia que han tenido sobre autores como Nick Szabo, Eric Hughes, Timothy May o especialmente Satoshi Nakamoto (Allen, Berg, Davidson, & Potts, 2021).

3.4.2.1 La acción humana y el orden espontáneo

Uno de los postulados básicos de los Austriacos, que se comienza a intuir en los escritos de Menger y luego desarrolla Mises, es la **acción humana** “*entendida como una característica esencial y eminentemente creativa de todo ser humano y como el conjunto de facultades coordinadoras que son las que espontáneamente hacen posible el surgimiento, el mantenimiento y el desarrollo de la civilización*” (Huerta de Soto, 2005, pág. 41). En palabras de Mises, la acción humana “*es una conducta consciente, movilizadora de voluntad transformada en actuación, que pretende alcanzar precisos fines y objetivos; es una reacción consciente del ego ante los estímulos y las circunstancias del ambiente; es una reflexiva acomodación a aquella disposición del universo que está influyendo en la vida del sujeto*” (von Mises, 2011, pág. 15) y constituye un presupuesto irreductible (von Mises, 2011, pág. 23).

Como consecuencia directa de la acción humana como devenir natural del hombre, aparece la idea del orden espontáneo. Hayek entendía que **la sociedad libre se organiza de manera espontánea** a partir de las **decisiones particulares y empresariales que adoptan los individuos** (Domínguez, 2017). Un orden que no es deliberado ni fruto del diseño de los individuos, sino que simplemente acontece (Hayek, 1960, pág. 23). Este orden espontáneo da lugar a una sociedad, que Hayek denominó **nomocracia** que se encuentra estrechamente ligado a la libertad, otro de los valores fundamentales austriacos. Esta se traduce en “un marco jurídico basado en reglas generales dirigidas a respetar la libertad personal para que cada persona pueda desarrollar sus proyectos vitales” (Rallo, 2019, pág. 105).

3.4.2.2 *La Libertad como Condición de Posibilidad*

La acción humana y el orden espontáneos no pueden acontecer en la ausencia de libertad. La **libertad** constituye la **pedra angular**¹⁰ del pensamiento austriaco. Hayek la definía como: “*el estado en virtud del cual un hombre no se halla sujeto a coacción derivada de la voluntad arbitraria de otro o de otros*” (Hayek, 1960, pág. 30). En este sentido, entienden que el orden natural de la sociedad no es el estatismo sino el orden espontáneo. Así, se podría afirmar que el axioma central sería, en palabras de Rothbard: “ningún hombre ni grupo de hombres puede cometer una agresión contra la persona o la propiedad de alguna otra persona.” (Rothbard, 2013, pág. 35).

Así, la Escuela Austriaca ha encontrado en el Estado un carácter coactivo y, por ende, imposibilitador y bloqueador de la creatividad y espontaneidad empresarial. En consonancia a lo que definía Hayek, la libertad consiste en no estar sujeto a la arbitrariedad de otros, siendo el Estado en cierto sentido la imposición de la arbitrariedad de unos cuantos. Rothbard por su parte, consideraba que “a lo largo de la historia y en la actualidad, siempre hubo un agresor central, dominante y avasallador de todos estos derechos: el Estado” (Rothbard, 2013, pág. 37). Por ello, el libertario se niega a “darle al Estado aval moral para cometer acciones que, en opinión de casi todos, son inmorales, ilegales y criminales si las lleva a cabo una persona o un grupo en la sociedad” (Rothbard, 2013, pág. 37) y está llamado a “difundir la desmitificación y desacralización del Estado” (Rothbard, 2013, pág. 37).

Si bien la libertad constituye el fundamento, si existen diferencias dentro de la Escuela en este sentido. Si bien Rothbard se consideraba anarcocapitalista y abogaba por una desaparición total del Estado, otros como Hayek defendía la mínima intervención posible.

Una vez caracterizados los elementos que son objeto de este trabajo se procederá al análisis. En el siguiente apartado se investigará la compatibilidad entre Bitcoin y Ethereum con las formulaciones económicas y político-filosóficas de la Escuela Austriaca para aclarar el potencial de ambas como posibilitadoras de la libertad individual.

¹⁰ Esta importancia otorgada al valor de la libertad no nace sólo de un razonamiento apriorístico sino también de la experiencia de los autores de la Escuela que vivieron los sistemas totalitarios del S.XX en Europa. Y fueron perseguidos por sus ideas.

4 ANÁLISIS

En esta sección, se procederá al análisis de la compatibilidad y afinidad teórica existente entre la blockchain y los postulados de la Escuela Austriaca de Economía. Como ya se ha dejado entrever en el Estado de la Cuestión, muchos de los autores partícipes en la creación de Bitcoin y posteriormente blockchain se han considerado a sí mismos austriacos o libertarios, como el creador de BitGold Nick Szabo o el creador del Manifiesto Criptoanarquista, Eric Hughes. Además de postularse así, como se ha podido comprobar, el motor que ha impulsado el desarrollo tecnológico previo a Bitcoin encuentra un íntimo alineamiento con la fundamentación filosófica de los austriacos, a saber: la soberanía individual, la libertad o la privacidad.

Por ello, este capítulo de análisis se dividirá en dos partes. La primera, versará sobre Bitcoin como la materialización de los principios económicos y monetarios expuestos por primera vez por Carl Menger, y posteriormente por Hayek y Mises. En segundo lugar, se hará un análisis del alineamiento de la filosofía que respalda la teoría económica austriaca con los diversos usos de blockchain, principalmente sobre la plataforma Ethereum y otras plataformas de la misma tipología.

4.1 Bitcoin: la materialización de la libertad económica

Según la perspectiva Austriaca, y como se ha expuesto en el Marco Teórico, el origen del dinero es *“un proceso evolutivo competitivo en torno a ciertas dimensiones de selección, como las cualidades de divisibilidad, aceptación, escasez, estabilidad, resistencia a la manipulación y permanencia.”* (Allen, Berg, Davidson, & Potts, 2021). La Escuela Austriaca sitúa estas características como primordiales para el mantenimiento de la **libertad económica**, que, a su vez, **es posibilitadora de la individual**. A fin de entender, el encaje que encuentra el proyecto Bitcoin con la Teoría Monetaria Austriaca se analizará la afinidad de Bitcoin con el Teorema de Regresión de Mises, posteriormente se analizará la falacia *“money or nothing”*, para acabar con una disección de las posibilidades que ofrece Bitcoin para la preservación de la libertad.

4.1.1 El Origen Natural de Bitcoin en relación con el Teorema de Regresión

Adoptando los postulados de Menger y Mises expuestos en el Marco Teórico, se puede afirmar con rotundidad que BTC se corresponde con el origen natural que estos defendían. Bitcoin nace en 2009 a raíz del *whitepaper* publicado por un usuario anónimo llamado Satoshi Nakamoto, y gracias al desarrollo en el campo de la criptografía que se hizo desde los años 70. Ambos autores plantearon el origen del dinero como el intercambio de bienes que los individuos adoptan de forma alternativa al cambio directo o truque. Así, en contraposición a las teorías económicas mainstream, el **dinero constituye una institución social** y no un producto del Estado. En ese sentido, **BTC ha nacido de forma espontánea en un mercado**. Impulsado por una pretensión

de mejora técnica del dinero, y también, por una mejora ética, nace impulsado por el mercado con el fin de dotar al individuo de una mayor privacidad y libertad individual. Es por ello, una clara ejemplificación de lo que los austriacos contemplaban.

El debate sobre la relación Bitcoin-Mises radica en el previo uso de un **medio de intercambio indirecto como uno directo** (Almará, 2021), porque es eso mismo lo que le confiere una estructura de precios (Huerta de Soto, 2016). A este respecto, Graf alega que pudo ser utilizado como prueba de la red de *blockchain* o porque era un avance en el campo de la criptografía (Graf, On the Origins of Bitcoin, 2013). En la misma línea Tucker defiende el valor de Bitcoin como parte de la *blockchain* (Tucker, 2014). Y en diferente línea, Surda defiende que, dado el carácter praxeológico, y, por consiguiente, apriorístico, de la Escuela Austriaca, alegar que Bitcoin invalida el teorema de Regresión, sería pegarse un tiro en el pie rechazando el carácter apriorístico del mismo (Šurda, 2012).

Sin embargo, es necesario un entendimiento del contexto en el que surge Bitcoin, un entorno con unos avances tecnológicos que hubieran sido inimaginables en el Siglo XX cuando se formularon estos planteamientos. Por ello, se puede afirmar que Mises contemplaba el previo uso como intercambio directo por la necesidad de una estructura de precios que sirviera como referencia, por lo que el hecho de no haber sido un *commodity* objeto de intercambio directo **no refutaría la teoría regresiva** (Almará, 2021). Además, cuando BTC comienza a funcionar ya existía una estructura de precios: la de la moneda tradicional, de hecho, su valor se expresa en esos términos.

Quedando demostrada la compatibilidad del Teorema Regresivo de Mises y el Origen Evolutivo de Menger con Bitcoin, no es posible afirmar en términos absolutos la idoneidad de esta relación debido a que, por sus consecuencias, Bitcoin no acaba de casar. Menger pone como condiciones para que un bien se convierta en dinero: (a) su **liquidez** o negociabilidad y (b) su **universalidad** (Menger, 2009). De la misma manera Mises pone esas condiciones, pero reduce la universalidad a “generalmente” aceptado y usado (von Mises, 1997). Este conflicto abre paso a uno de los debates más importantes que rodean BTC desde su creación: ¿es BTC dinero?

4.1.1.1 ¿Puede Bitcoin ser considerado Dinero?

De acuerdo con lo expuesto en el apartado anterior, Bitcoin nace para ser y, es de hecho, un método de intercambio. El Banco de España define el dinero como aquel bien que cumple con las funciones de: (a) **medio de pago**, (b) **reserva de valor** y (c) **unidad de cuenta** (Banco de España, 2021). A fin de poder clarificar si es dinero o no, se analizarán estas tres funciones que históricamente se le han dado al dinero.

4.1.1.1.1 Intercambio

En primer lugar, es preciso analizar el criterio por el cual los individuos se decantan por un bien y no por otro para utilizarlo como método de intercambio. Como bien dice Menger, este criterio

es la **negociabilidad o liquidez** (Menger, *The Origins of Money*, 2009, pág. 21). Así, los individuos históricamente han utilizado metales, sal o ganado, y no edificios, por ejemplo. Bitcoin es un método digital, es decir, no hay un ente material que sea objeto del intercambio, sino unos **bits**. Un bit es la unidad mínima de información utilizada en informática, al ser un intangible, es un bien altamente líquido y negociable, **se transmite sin prácticamente ningún esfuerzo**.

A ello, es preciso añadir el problema del *double spending* y la **reducción de costes de transacción**. Como se expuso en el Estado de la Cuestión y Marco Teórico, Bitcoin nace, entre otros, con el fin de hacer más eficiente la necesidad de intercambio. Al ser p2p y ser 100% verificable consigue reducir el coste de transacción porque prescinde de intermediarios. Este es un factor determinante para la adopción en masa, debido al efecto de red, de un método de intercambio alternativo. Sólo se vence la resistencia al cambio si los costes de transacción del medio de intercambio en uso son más altos que el nuevo (Rallo, 2019). En ese sentido, Bitcoin presenta una **clara ventaja respecto al dinero fiat**.

Además, una de las características más importantes del dinero es la **fungibilidad**, es decir, que el bien sea homogéneo. Esta característica es fundamental para solventar el problema de la doble concurrencia de necesidades (Huerta de Soto, 2010) que se menciona con anterioridad. Bitcoin cumple con esta característica, **un BTC es perfectamente sustituible por otro BTC** (Kroeger & Sarkar, 2017, pág. 7) debido a que forman parte de una red que funciona a través de un protocolo común (Preukschat, 2017). Si bien, todavía dista de una fungibilidad perfecta como todos los medios de intercambio actuales (Lopp, 2020).

Teniendo en cuenta que a nivel teórico BTC cumple con las condiciones para ser método de intercambio, empíricamente se demuestra que vale para tal fin. Hoy, son **numerosos los bienes y servicios que pueden ser adquiridos con BTC**. El ejemplo más sonado es el de la empresa americana de coches Tesla. En febrero de 2021, su fundador Elon Musk anunciaba, a través de Twitter, la posibilidad de comprar un coche tesla con bitcoins:

Figura 7. Tweet del CEO y fundador de Tesla Elon Musk



Fuente: Twitter

Pero esta no es la única, la americana cadena de bocadillos Subway, fue la primera gran cadena en aceptar BTC en los pedidos online, seguidamente fue Burger King en países como Países Bajos o Venezuela (Buy Bitcoin Worldwide, 2021). También, desde 2014, el gigante Microsoft admite Bitcoin como forma de pago para sus apps y juegos de Xbox (Microsoft, 2014). Existe todo un mercado para BTC, solo es cuestión de encontrar otro usuario interesado en aceptar este método. A parte de empresas y particulares, el BTC se utiliza como medio pago para comprar juegos o demás productos dentro de plataformas como *Uniswap*.

En definitiva, no sólo BTC cumple con el requisito de ser método intercambio, sino que también es utilizado habitualmente por usuarios. Así lo demuestra el gran número de empresas y personas que aceptan BTC, y la **velocidad de crecimiento** de la blockchain que sustenta Bitcoin. A 2021 la tasa de crecimiento es de unos **144 bloques por día**, avalando así su uso.

4.1.1.1.2 Unidad de cuenta

Ser unidad de cuenta significa “*ser la unidad de medida en que se expresen los precios de todos los bienes y servicios que haya en la economía; esto se llama ser bien numerario*” (Banco de España, 2021). Sólo con un instrumento de cambio uniforme que actúe como unidad de cuenta, los cálculos económicos se vuelven posibles y con ello la posibilidad de especialización en tareas complejas (Ammous, 2018, pág. 20). Para ello, es fundamental que exista **cierta estabilidad de precios**, ya que si estos presentan grandes oscilaciones los individuos no podrían tomar sus decisiones de forma ordenada (Banco de España, 2021). Como apuntaba Hayek, el problema del cálculo económico estriba, en gran parte, en la falta de conocimiento por parte de los individuos, y no como se cree en el desconocimiento de como asignar recursos (Hayek F. A., 1945, pág. 524). Así, los **precios constituyen las síntesis individuales de condiciones y realidades que acontecen en el mercado** (Ammous, 2018, pág. 118). En definitiva, la condición de unidad de cuenta cobra una **especial importancia**, sobre todo, en un contexto en el que el mercado es el único ente capaz de sintetizar toda esta información y asignar valor (Hayek F. A., 1945).

A estos efectos, es preciso analizar con cautela si BTC puede actuar como unidad de cuenta. El mercado de criptodivisas es uno de los más volátiles existentes, como se puede apreciar en los siguientes gráficos, el precio varía considerablemente en 1 día en incluso en 1 hora.

Figura 8. Variaciones del precio de BTC en 1 día y 1 hora



Fuente: (Coinbase, 2021)

A pesar de esta volatilidad, son numerosos los bienes y servicios que se pueden adquirir con BTC y, empresas que han comenzado a adquirir este activo, como se ha expuesto. Sin embargo, los precios todavía se expresan en dólares o euros y luego se convierte a la hora de pagar, lo que demuestra que en la práctica Bitcoin todavía no lleva a cabo la función de unidad de cuenta por su excesiva **volatilidad**¹¹.

Sin embargo, el hecho de que actualmente no consiga completar esa función, y, en futuro próximo no es probable que se materialice (Ammous, 2018, pág. 221). Sin embargo, **no conlleva que en un futuro en el que se expanda su uso, no pueda llegar a serlo**. El potencial del sistema bitcoin pone de manifiesto que eventualmente si pudiera gozar de cierta estabilidad de precios sin necesidad de un ente controlador. Esto es posible gracias a la limitación que establecía Nakamoto sobre la creación de nueva moneda, algo similar a lo que ocurría con el patrón oro.

4.1.1.1.3 Reserva de Valor

El gran beneficio de BTC es que supera a los sistemas anteriores como reserva de valor (Ammous, 2018). Ser reserva de valor, significa “*tener unas características de durabilidad o permanencia en el tiempo que permitan el ahorro (traspasar consumo presente a consumo futuro)*” (Banco de España, 2021). La reserva tradicional ha sido el oro, siendo la **via de escape a expropiaciones estatales o simplemente ahorro** (Rallo, 2009). La superioridad del oro frente a otros commodities ha sido su escasez, evitando así el aumento de su oferta, y la portabilidad (Rothbard, 2016). Bitcoin ostenta las cualidades que le convierten en el candidato idóneo para ser reserva de valor, a saber: “la inexistencia de riesgo de custodia o contrapartida, no hay riesgo de redenominación, no es posible diluir su valor con un aumento de la oferta monetaria, no se deteriora con el tiempo y es barata de almacenar” (Polavieja, 2020).

En primer lugar, el **riesgo de custodia**, refiere al riesgo al que están sometidos los actores que desempeñan funciones de custodia de valor. Pueden surgir en el contexto de su prestación de servicios de custodia, asociados a actividades específicas y a consecuencias concretas, y es el mismo tipo de riesgo que un banco afronta, gestiona y mitiga normalmente para todos los servicios bancarios (Rosati, Fontan, Chan, & Russo, 2007, pág. 29). Al depender de una cadena

¹¹ Sin embargo, es preciso hacer un matiz en referencia a la cuestión de la volatilidad. Es considerado excesivamente volátil respecto al dólar. Argumento que tiene una lógica condición de bidireccionalidad, es decir, al igual que se puede considerar el BTC como volátil respecto al dólar, se podría considerar al dólar volátil respecto a BTC. En vista de la volatilidad que presentan otras criptomonedas como Litecoin o plataformas como Ethereum o Cardano, la volatilidad de BTC respecto a ellas ya no es tan alta o significativa. Históricamente si se ha demostrado una correlación entre las criptomonedas debido al reducido tamaño del ecosistema de criptomonedas (Shen, 2020). Por lo tanto, no es intrínsecamente volátil, en términos de los precios *fiat* sí que lo es, pero en términos criptomonedas no lo es tanto. No obstante, si hay una considerable variación de precios que imposibilita, de momento, el desarrollo de la función de unidad de cuenta, tal y cómo se ha expuesto en el apartado.

de bloques descentralizada, en manos de millones de ordenadores, **no existe el riesgo de quiebra** por ejemplo, como tendría un banco.

En segundo lugar, no existe **riesgo de redenominación** conlleva que no se pueda redefinir tu valor en otra unidad monetaria (Polavieja, 2020). porque esa misma cadena es inalterable ya que utiliza criptografía fuerte y los bloques se hayan encadenados (Nakamoto, 2008), esto también mitiga el riesgo de deterioro temporal. Además, **no existe riesgo de oferta monetaria** por el límite establecido por Nakamoto de **21 millones de BTCs**, y el límite temporal de 1 bloque por cada 10 minutos (Bit2Me, 2021). Este punto será analizado más adelante a la luz de las oportunidades que bitcoin proporciona a la libertad económica.

4.1.2 La Falacia de Money or Nothing

Ante este debate incierto, el investigador de Bitcoin y Escuela Austriaca Peter Šurda acuñó el la **falacia de Money or Nothing**, con la que etiquetaba la obseión por categorizar a Bitcoin como dinero o nada más (Šurda, 2013). El hecho de que **Bitcoin no sea considerado o no cumpla enteramente con los requisitos del concepto de dinero, no conlleva que no aporte valor**. Para Surda el concepto “dinero” depende del contexto, ya que si por ejemplo BTC comenzara a ser unidad de cuenta supondría el colapso del sistema fiat en un país y por tanto no sería un rotundo éxito o al menos, nos despistaría a la hora de dar una definición de dinero (Šurda, 2013).

Así, el hecho de que no compute *strictu sensu* con la definición de dinero no hace desaparecer el valor que aporta bitcoin. Por **no ser dinero, no dejaría de ser un método efectivo de intercambio** (Graf, 2013). En este sentido, si se puede utilizar como medio de intercambio de igual manera. Como expone Szabo, en la antigüedad se utilizaron todo tipo de bienes como medio y **aportaba valor al individuo, al menos a los dos integrantes de la transacción** (Szabo, 2002). Aunque el Teorema de Regresión habla de la necesidad de que el bien en cuestión haya sido susceptible de intercambio directo previo, teniendo así una estructura de precios, en el caso de Bitcoin se puede valorar respecto a los precios de una moneda normal. Es decir, de momento, puede seguir siendo utilizado como un método de intercambio si dos personas acuerdan un intercambio a una determinada tasa de intercambio expresada en la **unidad local común de fijación de precios** (Graf, 2013, pág. 4).

En definitiva, es preciso no estancarse en el debate, si abusado estéril, de conceptualizar Bitcoin como dinero o no, debido a que sea dinero o no, es sin duda un método que está aportando valor a los individuos.

4.1.3 De las Posibilidades de Bitcoin respecto a la Libertad Económica

Como se ha dejado entrever, Bitcoin encuentra un estrecho encaje con los postulados sostenidos por la Escuela Austriaca de Economía, y por ende con la libertad. Si algo está claro es el potencial disruptivo que, a nivel humano, tiene Bitcoin.

Como se ha vislumbrado en el apartado anterior, la gran aportación que hace bitcoin a la libertad económica, y por consiguiente a la individual, es **actuar como reserva de valor**. Hayek definía la **libertad como la ausencia de coacción**: “*el estado en virtud del cual un hombre no se halla sujeto a coacción derivada de la **voluntad arbitraria** de otro o de otros*” (Hayek F. A., 1960). En este caso, la definición *hayekiana* cobra especial importancia porque la moneda *fiat* está sujeta al control estatal, y, por consiguiente, a su arbitrariedad. Szabo considera que el dinero tradicional, al estar sujeto a una tercera parte que asegura y verifica, implica de forma insoslayable, estar sujeto a **cierta arbitrariedad** que se puso de manifiesto en el Siglo XX con la hiperinflación (Szabo, 2005). La **devaluación de la moneda nacional** ha sido una práctica frecuente a lo largo de la historia con el fin de, en términos comerciales, aventajarse respecto al resto de naciones (Huerta de Soto, 2012). Cuando los Estados aumentan la oferta monetaria, reducen el valor de la moneda, así, para un individuo **que ahorra el excedente de su renta en esa unidad monetaria, ve reducida la cantidad por un fenómeno totalmente ajeno a él** (von Mises, 1997). Es decir, el individuo ve su riqueza comprometida por la arbitrariedad “de otros” y a la constante expansión estatal (Hülsmann, 2008). Por sus características, BTC consigue sortear estos problemas, como Szabo vislumbró en su momento con Bitgold, un patrón oro de bits (Szabo, 2005).

Es pertinente entonces, traer a colación el ejemplo de países como **Argentina** o **Venezuela** en los cuales la arbitrariedad estatal ha reducido sus monedas a nada. El 5 de marzo de 2021 el Banco Central de Venezuela ampliaba el cono monetario con **billetes de hasta 1 millón de bolívares** (Banco Central de Venezuela, 2021). En la misma línea Argentina, registra un **48,1% de inflación** en 2021 (Reuters, 2021). En estos países el bitcoin ya funciona de hecho como **moneda alternativa y paralela a la oficial**. La ventaja del Bitcoin en el caso de Venezuela es que también se puede comprar fuera de Venezuela en cualquier moneda para que los residentes venezolanos lo vendan en Venezuela por bolívares, siguiendo el ritmo de la inflación (Johnson, 2019). Además, también permite **realizar transacciones en cualquier parte del mundo a precios normales** sin el control gubernamental (Haesly, 2016). El residente en Venezuela puede comprar con BTC y recibir directamente el bien, sorteando las limitaciones estatales.

En este sentido, Bitcoin presenta otra característica capaz de vencer el nacionalismo monetario: su **vocación universal**. Al ser un medio totalmente digital, tiene potencial de ser utilizado en cualquier lugar del mundo. De esta forma, su uso generalizado en distintas partes del mundo contribuiría a **solventar la obstrucción al intercambio internacional** y el **cálculo económico**

transfronterizo que suponen los tipos de cambio y diferencias de valor de divisas nacionales.

Por ello, la función de unidad de cuenta cobra especial importancia. Si el oro conseguía solucionar este problema siendo una única forma de dinero, independiente del control de cualquier gobierno o autoridad, era la referencia monetaria en todo el mundo, y los precios podían calibrarse con arreglo al oro (Ammous, 2018, pág. 222).

Por último, la característica de escasez y anarquía de Bitcoin le hace asemejarse al oro, pudiendo actuar como **control a la expansión estatal**. Aunque bitcoin en esencia es, su protocolo y red simulan la propiedad natural de la **escasez** (Graf, 2014, pág. 17). Además, el hecho de **no ser controlado por una autoridad** central lo hace más similar aún al oro (Weber, 2016). Una de las ventajas que traía consigo el patrón oro era:

“el límite a la capacidad de expansión crediticia que podía efectuarse dentro de cada país y que venía determinado por las salidas de oro que inexorablemente se producían en las economías relativamente más inflacionistas. Con el abandono del patrón oro, el advenimiento de los tipos de cambio flexibles y el triunfo del nacionalismo monetario, cada país pudo emprender libremente políticas de expansión crediticia, iniciándose una competencia inflacionaria de «todos contra todos». Solamente un área económica muy amplia e integrada de diversas naciones que hayan renunciado a la expansión crediticia y mantengan entre sí tipos de cambio fijos podrá librarse, relativamente (y no del todo), de los efectos negativos de una expansión crediticia general que se haya iniciado fuera de sus fronteras.” (Huerta de Soto, 2016, pág. 372)

Así, atendiendo a las similitudes entre el oro y Bitcoin, la capacidad de este último de servir de corsé a la ficticia expansión estatal abre una nueva posibilidad a la libertad económica. Lo mejor del oro es su suministro en el libre mercado y a través del trabajo de los individuos (Rothbard, 2016), así BTC ha de cumplir con la misma humana función de preservar la libertad.

4.2 Ethereum como posibilitador de la libertad individual

De la misma manera que Bitcoin introduce nuevas posibilidades para la libertad económica, Ethereum, y en general, la tecnología blockchain y plataformas programables derivadas de ella, como Cardano, son condición de posibilidad para **la cooperación y coordinación espontánea** de los individuos. De esta forma, al igual que Bitcoin con la Teoría Monetaria Austriaca, Ethereum encuentra un aliado en la filosofía cimiento de la Escuela Austriaca. Las condiciones inherentes de la tecnología blockchain, como los *smart contracts*, tienen el potencial de fortalecer la visión **anti-estatista** (Chawla, 2018). De hecho, como se expuso en el Estado de la Cuestión, muchos de los informáticos e intelectuales promotores del desarrollo de esta tecnología se han llegado a considera afines a la Escuela Austriaca o libertarios. A efectos de una mayor precisión y

concreción se hará el análisis sobre la creación de Vitalik Buterin, no obstante, es extrapolable a todas las nuevas plataformas que han aparecido con posteridad y cumplen la misma función.

4.2.1 El Orden Espontáneo y la Cooperación entre Individuos

Como se explicaba en el Marco Teórico, el cimiento filosófico de la Escuela Austriaca es la praxeología, así su postulado político fundamental es el orden espontáneo. De una forma similar a la Ilustración Escocesa de Adam Ferguson y Adam Smith, la Escuela Austriaca entiende al **hombre libre capaz de intercambiar y generar un orden sin pretenderlo**, simplemente como fruto de su actividad natural (Ferguson, 1782). De la misma forma que el dinero acontece como un proceso natural del mercado, el **orden** también constituye **una institución social**. Analizando blockchain a la luz de esta teoría se hace evidente que, la primera reúne todas las características para posibilitar la segunda.

Uno de los postulados de Ethereum es *“banking for everyone”* (Ethereum, 2021), ya que esta plataforma abre la posibilidad de **acceso a recursos financieros a personas que no cumplirían las condiciones exigidas por un banco**, o que **no tienen acceso directo a una entidad** (Buterin V. , 2014). De esta manera, Ethereum pone en contacto a particulares que emiten títulos de deuda personales en forma de tokens, con individuos dispuestos a adquirirlos como un activo (Jacynycz, Calvo, Hassan, & Sánchez-Ruiz, 2016). Ello se consigue a través de un *smart contract* programado en solidity, el lenguaje de programación de Ethereum, que dota de una mayor seguridad ya que el contrato se auto ejecuta dadas las circunstancias estipuladas (Szabo, 2017).

En esencia, lo que consigue la función de crowdfunding de Ethereum es generar una **cooperación descentralizada entre individuos**. Individuos que **no han de confiar** entre ellos dada las condiciones de blockchain, y que pone de manifiesto la practicidad de esa idea, que a priori podía parecer etérea, del orden espontáneo. A través de la **compatibilización de intereses personales** en el mercado, los individuos consiguen generar un orden, hecho que se ve reforzado por la característica *p2p*. Además, los individuos consiguen **expandir el horizonte de su libertad** teniendo nuevas oportunidades en el mercado fuera de los bancos tradicionales.

4.2.2 La Libertad y No Coacción

Desde la clave pública de Diffie y Helman, pasando por Chaum, hasta Szabo, Hughes o May, la fuerza motora ha sido siempre la búsqueda de privacidad y libertad individual. Así, Ethereum contempla estas ideas como principios de la red: *“a more private internet”* y *“censorship-resistant”*. Este hecho pone de manifiesto el compromiso de Ethereum con los valores fundamentales austriacos: la libertad individual y la no-coacción.

En primer lugar, *a more private internet* refiere a lo que ya se imbuía con las aportaciones de PGP o David Chaum, la **no necesidad de desvelar detalles personales para el uso de las aplicaciones**

desarrolladas sobre Ethereum. En palabras de Eric Hughes “*Privacy is the PoWer to selectively reveal oneself to the world*” (Hughes, 1993), es decir, ser soberanos de unos mismos, que conlleva ser libres. Como expone Logan, la privacidad es inherente al hombre y es una condición necesaria para entablar relaciones personales y desarrollar un “yo” del que se deriven responsabilidades personales (Logan, 2012). Esta red esta basada en el valor económico y no en el espionaje o *surveillance* (Ethereum, 2021). Todo esto concuerda con el concepto de soberanía digital, que refiere a ser los dueños de nuestros datos frente a gobiernos y grandes empresas que actualmente los expolían sin retribución hacia el individuo. Así, es pertinente traer a colación, la ya expuesta visión de Zimmermann, quién aplicó la encriptación del correo electrónico como protección de los DDHH y vía de escape a la opresión de los gobiernos (Zimmermann, 1999).

En el mismo sentido, la idea de *censorship-resistant* es una clara repulsa a la extralimitación de los Estados Modernos y las Big Techs sobre la libertad de expresión. Por ello, Buterin se propuso crear un espacio donde **no exista un ente centralizado con capacidad de ejercer ningún tipo de coacción sobre sus integrantes**: “la descentralización hace que sea casi imposible que alguien te impida recibir pagos o utilizar servicios en Ethereum” (Ethereum, 2021). De una manera parecida a la que se expone en el Marco Teórico y encarna Rothbard de el Estado como principal enemigo de la libertad (Rothbard M. , 2013, pág. 36). En este sentido, China ha sido un ejemplo de la vía de escape que supone blockchain a los gobiernos coactivos. De la misma forma que Bitcoin supone un refugio y una alternativa a los ciudadanos de países con una desorbitada inflación, Ethereum supone un refugio para los individuos de Estados en los que la libertad de expresión no tiene cabida.

El gobierno chino ha mantenido durante mucho tiempo las riendas de los medios de comunicación, tanto tradicionales como nuevos, para evitar la potencial subversión de su autoridad (Xu, 2014). Ciertas plataformas de internet han dotado de mayor autonomía a los individuos para la expresión y el debate sobre asuntos públicos, y han conseguido que los medios occidentales conozcan y se hagan eco de ellos. Siendo un claro ejemplo el incidente *My father is Li Gang* (Chan, Chau, & Fu, 2013). Sin embargo, internet sigue siendo objeto de la censura y el control estatal en China, pero las características de blockchain consiguen sortear ese problema. Ethereum pues, supone un aliado para aquellos que buscan expresarse libremente. El caso de la activista **Yue Xin** es un buen ejemplo de ello, su famosa carta fue escrita en chino e inglés en la metadata de diferentes transacciones de Ethereum. Al ser las transacciones permanentes y publicas cualquiera puede acceder a ella, y, además, no podría ser modificada. La descentralización de la red impide también que esta pudiera ser retirada. Este caso es otra materialización del objetivo de Zimmermann de aplicar la criptografía a la protección de los DDHH.

En definitiva, Ethereum siendo una blockchain pública reúne todas las características para garantizar la privacidad individual y la no coacción. Constituye un elemento fundamental para la preservación de la libertad en nuestra sociedad, y así fue concebida por todos sus precursores

4.2.3 La Descentralización, el Orden Caórdico y la Anarquía

En última instancia, lo comentado anteriormente, refiere a un nuevo modelo de realidad en la que la libertad cobra un papel protagonista: **la descentralización**. El fundador y ex CEO de Visa, acuñó el término chaordic para describir una forma de organización que integra el caos y el orden:

“The behavior of any self-organizing and self-governing organism, organization, or system that harmoniously blends characteristics of chaos and order. 2. Characteristic of the fundamental, organizing principle of nature” (Hock, 2005, pág. 13)

Un concepto inicialmente pensado para las organizaciones empresariales, en base a su experiencia una huída de la excesiva jerarquización, que encuentra una excelente aplicabilidad en el futuro de una sociedad en la que se de un uso generalizado y cotidiano de la tecnología blockchain. “Son una invitación a experimentar el **caos autorregulador** de una organización que **nadie controla completamente** y en la que **todos los que participan en ellas son responsables de la misma**” (Preukschat, 2017, pág. 198).

Esta idea guarda una estrecha relación con lo que los Cypherpunks, expuestos en el Estado de la Cuestión, y las corrientes han Crypto-anarquistas han defendido. Como afirma Runkle, la anarquía refiere a la libertad individual (Runkle, 1972, pág. 3). La anarquía también puede ser definida como descentralización (Clark, 1978, pág. 4). Entendiendo anarquía como “*ausencia de planificación*” y organización *down-up* anarquía refiere en su esencia a la idea de descentralización (Goodman, 1974). Diffie y Helman ya veían que la autoridad debía ser descentralizada (Carrascosa, Kuchkovsky, & Preukschat, 2017), y Chaum abogó fuertemente por la descentralización del poder (Chaum, 2019). Es decir, la anarquía a la que Hughes, May y todos los investigadores del campo de la criptografía y blockchain hacían referencia en esencia, es a la descentralización como postulado político-filosófico de organización. La descentralización, sin lugar a dudas, es una forma de organización que evita la centralización, y por ende, **reduce el riesgo de un excesivo poder o coacción**. Además, la descentralización encuentra una interesante coherencia con la formulación del orden espontáneo de los Austriacos. A efectos prácticos, la descentralización constituye un **orden no diseñado fruto de la cooperación de los individuos**. Además, esta forma de organización resuelve el **problema del conocimiento y el cálculo económico** puesto de manifiesto por Hayek y Mises, ya que, los individuos en sus relaciones van **sintetizando el conocimiento** que acontece en una economía o una sociedad. Así, Ethereum es un ejemplo de colaboración entre distintos individuos en condiciones de plena libertad y descentralización.

5 CONCLUSIÓN

La libertad como condición de la dignidad humana quedó demostrada con los totalitarismos del Siglo XX, que en palabras de Arendt reducían y aislaban al hombre hasta convertirlo en un átomo más. Los retos actuales que se ciernen sobre el valor de la libertad instan a una batalla por preservarla y mantenerla. El aliado perfecto para ello, como ha quedado demostrado a lo largo de este Trabajo de Fin de Grado es la tecnología blockchain. Motivada por la protección de la libertad, soberanía individual y privacidad, desde los años 70, los avances tecnológicos en el campo han sido revolucionarios. Y, estos ya han puesto de manifiesto su utilidad como garantes de la libertad individual.

En términos económicos Bitcoin supone una revolución de la teoría monetaria tal y como se conoce. Esta criptomoneda ha sido producto de las innovaciones del mercado, y su valor ha ido evolucionando en función de la confianza que los individuos han depositado en el proyecto. De esta manera, Bitcoin encuentra un interesante encaje con el origen natural de Menger y el Teorema de Regresión de Mises. Así, se confirma como una institución social que no necesita del estado para su existencia y eficiencia. Siendo un activo escaso, fungible, transferible y duradero, encuentra muchas similitudes con el oro. Si bien no puede ser categorizado como dinero *strictu sensu*, actúa de hecho como método de intercambio y como reserva de valor. Siendo de entre las dos la segunda la más importante, ya que consigue blindar al individuo frente a la arbitrariedad política y económica de los gobiernos. Lo que los autores de la Escuela de Salamanca ya veían como empobrecer a los individuos. Prueba de ello, es el flujo constante de Bitcoin entre los venezolanos que compran bienes en esta criptodivisa para escapar de la hiperinflación, o el caso de Argentina. En ambos países, esta moneda actúa ya en paralelo a las devaluadas monedas nacionales. Además, no sólo a nivel individual Bitcoin presenta la ventaja, frente al dinero fiat, de actuar como límite macroeconómico a la expansión descontrolada crediticia y de la oferta monetaria, actuando como una suerte de patrón oro.

No obstante, aunque Bitcoin no cumpla todas las características de la definición de dinero esto no conlleva que no sea nada o no aporte valor. Como se ha expuesto a lo largo del trabajo, sería erróneo partir de la falacia del “dinero o nada”. Las criptomonedas generan valor aunque sea sólo para dos personas que lo puedan utilizar como una transacción o a las personas que refugien sus ahorros en él. No sólo en términos monetarios o de ahorro sino también desde una perspectiva técnica ya que ha abierto la posibilidad a infinitos usos de la tecnología blockchain. Quizá este dando lugar a un concepto nuevo que no existe en la perspectiva actual, y por ello, sea estéril tratar de encajarlo en las categorías tradicionales, cuando su potencial traspasa todas las expectativas.

Por otro lado, el análisis de Ethereum como plataforma programable sobre la que corren Dapps y criptomonedas, ha dejado patente el potencial de la tecnología blockchain para el individuo. Las blockchains demuestran ser el espacio idóneo para el acontecer de la cooperación espontánea, ya que, consigue coordinar de forma inintencionada a los individuos y compatibilizar sus intereses. Así, frente a la organización centralizada en torno al estatismo, la descentralización de bloques expande la libertad de los individuos. Ethereum, y en general cualquier plataforma que comparta sus características, sirven de espacio para la materialización de esas ideas que Menger, pero especialmente Hayek y Mises, vislumbraron. La acción humana desarrollada en libertad como motor para la cooperación de los individuos que desemboca en la generación de un orden espontáneo que admite toda la contingencia humana, por su base praxeológica.

Sin embargo, muchas son las voces detractoras que se han alzado en contra de este imparable avance de la libertad. Diferentes instituciones internacionales como el Banco Central Europeo o el FMI, o a nivel nacional el Banco de España, se han posicionado en contra de este tipo de activos y avances. Christine Lagarde en numerosas ocasiones ha manifestado su intención de regular el uso e intercambio de criptomonedas. En especial, Lagarde ha alegado la necesidad de regulación por actividades ilegítimas que se dieron en el nacimiento de Bitcoin. Esta oposición pone de manifiesto, que todavía hay cierta resistencia a su adopción. No obstante, esta resistencia viene principalmente por las instituciones de las que prescindir el sistema blockchain prescindir, por ello, es de esperar encontrar cierta rigidez y detracción ante innovaciones de este corte.

A pesar de las voces detractoras que pueden surgir, y las intenciones de frenar este proyecto a través de presión fiscal y control estatal, blockchain tiene un futuro prometedor. Un proyecto que ha conseguido superar obstáculos técnicos desde los años 80, donde la criptografía era algo muy incipiente, y movido por una pretensión tan trascendente es difícil que pueda desistir en su empresa. Como elemento habilitador de una mayor libertad en la libertad, las criptomonedas y sistemas blockchains han de ser incentivados por los gobiernos e incluidos en los procesos sociales.

En definitiva, la tecnología blockchain constituye la materialización de la filosofía praxeológica de la Escuela Austriaca, y por ello, presenta un futuro prometedor para la libertad individual. Dadas las posibilidades que ofrece y a demostrado eficaces, las sociedades que acontezcan en unos años tienen el potencial de ser mucho más libres, donde la soberanía individual sea mayor gracias a la descentralización, a la par que seguras. La adopción y compra por parte de muchas grandes empresas tradicionales, y la capitalización en el mercado de BTC, hacen intuir que efectivamente el horizonte de esta tecnología ha llegado para quedarse. El futuro dirá, y la puerta queda abierta a algunas cuestiones como ¿permitirán los gobiernos el avance de estos proyectos

en detrimento de su soberanía? Y más importante ¿abrazarán los individuos un modelo con mayores proyecciones en términos de su libertad personal?

6 BIBLIOGRAFÍA

- Allen, D., Berg, C., Davidson, S., & Potts, J. (2021). Blockchain and investment: An Austrian approach. *The Review of Austrian Economics*, 34, 149–162.
doi:<https://doi.org/10.1007/s11138-020-00504-x>
- Almará, I. (2021). *La Escuela Austriaca y Bitcoin: segunda parte. Mises VS Bitcoin*. Obtenido de Instituto Xoan de Lugo: <https://xoandelugo.org/la-escuela-austriaca-y-bitcoin-segunda-parte-mises-vs-bitcoin-ignacio-almara/>
- Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money? *The Quarterly Review of Economics and Finance*, 70, 38-51. doi:<https://doi.org/10.1016/j.qref.2018.05.010>
- Ammous, S. (2018). *El Patrón Bitcoin* (6ª ed.). (M. Vaquero, Trad.) Barcelona: Deusto.
- Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. *Ethics and Information Technology*.
doi:<https://doi.org/10.1007/s10676-020-09571-x>
- Anguiano, J. M. (15 de Noviembre de 2018). *Garrigues Opina: 'Smart Contracts'. Introducción al 'contractware'*. Obtenido de Garrigues:
https://www.garrigues.com/es_ES/noticia/smart-contracts-introduccion-al-contractware
- Awad, D. (March de 2021). *Introduction to DApps*. Obtenido de Ethereum:
<https://ethereum.org/en/developers/docs/dapps/>
- Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure*. Obtenido de Hashcash:
<http://www.hashcash.org/papers/hashcash.pdf>
- Banco Central de Venezuela. (2021). *BCV amplía Cono Monetario vigente con incorporación de tres nuevos billetes*. Obtenido de Banco Central de Venezuela:
<http://www.bcv.org.ve/notas-de-prensa/bcv-amplia-cono-monetario-vigente-con-incorporacion-de-tres-nuevos-billetes>
- Banco de España. (2021). *El Dinero*. Obtenido de Aula Virtual del Banco de España Eurosistema:
https://aulavirtual.bde.es/wav/es/menu/pagos/Estabilidad_del_54d079146f44651.html
- Bastos, M. A. (29 de Diciembre de 2020). *Algunas cuestiones disputadas sobre el anarcocapitalismo (LII): Los "Cypherpunks"*. Obtenido de Instituto Juan de Mariana:
<https://juandemariana.org/ijm-actualidad/analisis-diario/algunas-cuestiones-disputadas-sobre-el-anarcocapitalismo-lii-los-cypherpunks/>
- Bit2Me. (2021). *¿Qué es la escalabilidad de Bitcoin?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/que-es-escalabilidad-de-bitcoin/#:~:text=Recordemos%20que%20Bitcoin%20tiene%20configurado,transacciones%20caben%20en%20un%20bloque.>
- Bit2Me. (2021). *¿Qué es la Ethereum Virtual Machine (EVM)?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/que-es-ethereum-virtual-machine-evm/>
- Bit2Me. (2021). *¿Qué es Prueba de participación / Proof of Stake (PoS)?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/que-es-proof-of-stake-pos/>
- Bit2Me. (2021). *¿Qué es un Nonce?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/que-es-nonce/>

- Bit2Me. (2021). *¿Quién es Adam Back?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/quien-es-adam-back/>
- Bit2Me. (25 de 01 de 2021). *¿Quien es David Chaum?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/quien-es-david-chaum/>
- Bit2Me. (17 de 02 de 2021). *¿Quién es Nick Szabo?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/quien-es-nick-szabo/>
- Bit2Me. (3 de 02 de 2021). *¿Quién es W. Scott Stornetta?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/quien-es-w-scott-stornetta/>
- Bit2Me. (2021). *What is a Cypherpunk?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/en/what-is-a-cypherpunk/>
- Bit2Me. (2021). *What is Bitcoin scalability?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/en/what-is-bitcoin-scalability/>
- Bitcoin Developer. (2021). *Glossary*. Obtenido de Bitcoin Developer: <https://developer.bitcoin.org/glossary.html>
- Block, W. E., & Davidson, L. (2015). Bitcoin, the Regression Theorem and the Emergence of a New Medium of Exchange. *The Quarterly Journal of Austrian Economics*, 18(3), 311-338.
- Blockchain.com. (03 de Marzo de 2021). *Bitcoin Explorer: Bloques*. Obtenido de Blockchain.com: <https://www.blockchain.com/btc/blocks?page=1>
- BTC.com. (03 de Marzo de 2021). *Latest Blocks*. Obtenido de BTC.com: <https://btc.com/>
- Buffett, W. (2020). Warren Buffett: Cryptocurrency ‘has no value’ – ‘I don’t own any and never will’. (B. Quick, Entrevistador) Obtenido de <https://www.cnbc.com/2020/02/24/warren-buffett-cryptocurrency-has-no-value.html>
- Buterin, V. (2014). *Ethereum Whitepaper*. Obtenido de Ethereum.org: <https://ethereum.org/en/whitepaper/>
- Buterin, V. (2016). *Ethereum: Platform Review. Opportunities and Challenges for Private and Consortium Blockchains*. Obtenido de Bitcoin Magazine.
- Buy Bitcoin Worldwide. (2021). *Bitcoin Restaurants*. Obtenido de Buy Bitcoin Worldwide: <https://www.buybitcoinworldwide.com/restaurants/>
- Carrascosa, C., Kuchkovsky, C., & Preukschat, Á. (2017). Hactivismo, cypherpunks y el nacimiento de la blockchain. En Á. Preukschat, C. Kuchovsky, G. Gómez Lardies, D. Díez García, Í. Molero, & Á. P. (coord.) (Ed.), *Blockchain: la Revolución Industrial de Internet* (8ª ed., págs. 175-189). Barcelona: Gestión 2000.
- Cerf, V. G., & Kahn, R. E. (May de 1974). A Protocol for Packet Network Intercommunication. *IEEE Trans on Comms*, 22(5).
- Chamagne, P. (2014). *El Libro de Satoshi*. BlockchainEspaña.com. Obtenido de <https://libroblockchain.com/satoshi/>
- Chan, C.-h., Chau, M., & Fu, K.-w. (2013). Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and the Real-Name Registration Policy. *IEEE Internet Computing*, 17(3), 42-50. doi:10.1109/MIC.2013.28

- Chamagne, P. (2014). *El Libro de Satoshi*. BlockchainEspaña.com. Obtenido de <https://libroblockchain.com/satoshi/>
- Chaum, D. (1985). SEcurity without Identification: Card Computers to make Big Brother Obsolete. *Communications of the ACM*, 28(10), 1030-1044. Obtenido de https://www.chaum.com/publications/Security_Without_Identification.html
- Chaum, D. (2019). *Interview: David Chaum*. Obtenido de National Research Institute for Mathematics and Computer Science (CWI): <https://www.cwi.nl/news/blogs/interview-david-chaum-2019blockchain-will-decentralize-power2019>
- Chawla, H. (2018). Blockchain: the key to anarchist self-governance? *Department of Politics and International Studies. University of Warwick*. doi:10.13140/RG.2.2.31779.14888
- Chohan, U. W. (2017). Cryptoanarchism and Cryptocurrencies. doi:<http://dx.doi.org/10.2139/ssrn.3079241>
- Clark, J. P. (1978). What is Anarchism? *Anarchism*, 19, 3-28. Obtenido de <https://www.jstor.org/stable/24219036>
- Cloudflare. (2021). *Ataque de inundación SYN*. Obtenido de Cloudflare: <https://www.cloudflare.com/es-la/learning/ddos/syn-flood-ddos-attack/>
- Coinbase. (19 de 02 de 2021). *Coinbase*. Obtenido de <https://www.coinbase.com/es/>
- CoinMarketCap. (19 de Febrero de 2021). *Bitcoin*. doi:<https://coinmarketcap.com/es/currencies/bitcoin/>
- Dai, W. (1998). *B-Money*. Obtenido de weidai.com: <http://www.weidai.com/bmoney.txt>
- Dannen, C. (2017). *Introducing Ethereum and Solidity*. New York: Apress.
- DappRadar. (2021). *Top Blockchain Dapps*. Obtenido de DappRadar.com: <https://dappradar.com/rankings/protocol/ethereum>
- de la Guía, D., Hernández, L., Montoya, F., Muñoz, J., & Fúster, A. (2004). *Técnicas Criptográficas de protección de datos* (3ª ed.). Madrid: Ra-Ma.
- Dev, J. A. (2014). Bitcoin mining acceleration and performance quantification. En IEEE (Ed.), *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, (págs. 1-6). Toronto. doi:10.1109/CCECE.2014.6900989
- Díez García, D., & Gómez Lardies, G. (2017). Banca y blockchain, ¿pioneros por necesidad? En Á. Preukschat, C. Kuchovsky, , G. Gómez Lardies, D. Díez García, Í. Molero, & Á. Preukschat (Ed.), *Blockchain: la Revolución Industrial de Internet* (págs. 32-43). Barcelona: Gestión 2000.
- Diffie, W., & Hellman, M. (November de 1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 645-654. Obtenido de <https://ee.stanford.edu/~hellman/publications/24.pdf>
- Domínguez, J. (2017). *F. A. Hayek, Gigante del Orden Espontáneo*. Obtenido de Instituto Juan de Mariana: <https://juandemariana.org/ijm-actualidad/pildoras-de-libertad/f-a-hayek-gigante-del-orden-espontaneo/>
- Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. *Lecture Notes in Computer Science*, 740. doi:https://doi.org/10.1007/3-540-48071-4_10

- Erfani, S., & Ahmad, M. (2019). Bitcoin Security Reference Model: An Implementation Platform. *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, (págs. 1-5). Iasi. doi:10.1109/ISSCS.2019.8801796
- Escudero, V. (2017). Software Libre y código abierto en el mundo de las Blockchains. En A. Preukschat, C. Kuchkovsky, G. Gómez Lardies, D. Díez García, & Í. Molero, *Blockchain: la Revolución Industrial de Internet* (págs. 221-227). Gestión 2000.
- Ethereum. (25 de 1 de 2021). *What is Ethereum?* Obtenido de Ethereum: <https://ethereum.org/es/what-is-ethereum/>
- Ferguson, A. (1782). *Essay on the History of Civil Society* (5th ed.). London: T. Cadell. Obtenido de https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/1428/Ferguson_1229_EBk_v6.0.pdf
- Finney, H. (2004). *RPOW - Reusable Proofs of Work*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/rpow/>
- Fridrich, J., & Goljan, M. (2000). Robust Hash Functions for Digital Watermarking. En IEEE (Ed.), *Proceedings International Conference on Information Technology: Coding and Computing*, (págs. 178-183). Las Vegas. doi:10.1109/ITCC.2000.844203
- Goodman, P. (1974). Notes on Decentralization. *Dissent Magazine*. Obtenido de <https://www.dissentmagazine.org/article/notes-on-decentralization>
- Garay, J., Kiayias, A., & Leonardos, N. (2017). *The Bitcoin Backbone Protocol with Chains of Variable Difficulty*. *Lecture Notes in Computer Science*, 291–323. doi:10.1007/978-3-319-63688-7_10
- Graf, K. S. (2013). *On the Origins of Bitcoin*. Obtenido de <https://static1.squarespace.com/static/5720adbdc6fc0891cbcce17c/t/580d685959cc689a7b411ba4/1477275058522/On+the+Origins+of+Bitcoin+Graf+03.11.13.pdf>
- Graf, K. S. (2014). *Revisiting Conceptions of Commodity and Scarcity in light of Bitcoin*. Obtenido de <https://nakamotoinstitute.org/static/docs/commodity-and-scarcity-in-light-of-bitcoin.pdf>
- Grau Navarro, J. (2020). *La Teoría del Dinero y del Crédito*. Obtenido de Nueva Revista: <https://www.nuevarevista.net/destacados/ludwig-von-mises-la-teoria-del-dinero-y-del-credito/#:~:text=Para%20que%20el%20dinero%20tenga,la%20historia%20de%20la%20humanidad.>
- Gupta, V. (2017). A Brief History of Blockchain. *Harvard Business Review Digital Articles*, 2–4.
- Haber, S., & Stornetta, W. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2), 99-111.
- Haesly, K. B. (2016). How to Solve a Problem Like Venecuela? An Argument for Virtual Currency. *Law and Business Review of the Americas*, 22(3). Obtenido de <https://scholar.smu.edu/lbra/vol22/iss3/12>
- Hayek, F. (1960). *The Constitution of Liberty*. Chengcheng Books.
- Hayek, F. A. (1945). The Use Of Knowledge In Society. *American Economic Review*, 35(4), 519-530.

- Hayek, F. A. (1960). *Los Fundamentos de la Libertad* (9ª ed.). (J. V. Secorún, Trad.) Unión Editorial.
- He, Z., & Cong, L. W. (May de 2019). Blockchain Disruption and Smart Contracts. (I. Goldstein, Ed.) *Review of Financial Studies*, 23(5), 1754-1797.
- Hock, D. (2005). *One From Many. Visa and the Rose of Chaordic Organization*. San Francisco: Berrett-Koehler Publishers, Inc.
- Huerta de Soto, J. (1994). *Estudios de Economía Política* (2ª ed., Vol. I). Madrid: Unión Editorial.
- Huerta de Soto, J. (2005). *Cálculo Económico y Función Empresarial* (3ª ed.). Madrid: Unión Editorial.
- Huerta de Soto, J. (June de 2009). The Essence of the Austrian School. *IEA Economic Affairs*. Obtenido de <https://doi.org/10.1111/j.1468-0270.2009.01892.x>
- Huerta de Soto, J. (2010). *Lecciones de Economía con Jesús Huerta de Soto*. Obtenido de Instituto Juan de Mariana: <https://www.youtube.com/playlist?list=PLXPi0C09DKYYoqMV1jeRQqu10swxQ-Hdj>
- Huerta de Soto, J. (2012). *El Sistema Monetario Perfecto*. Obtenido de En Defensa del Euro Amagifilms : <https://www.youtube.com/watch?v=Cfams8etqUI>
- Huerta de Soto, J. (2012). *La esencia de la Escuela Austriaca*. Guatemala: Universidad Francisco Marroquin.
- Huerta de Soto, J. (2016). *Dinero, Crédito Bancario y Ciclos Económicos*. Madrid: Unión Editorial. Obtenido de <https://www.jesushuertadesoto.com/libros/libros-en-espanol/dinero-credito-bancario-y-ciclos-economicos/>
- Hughes, E. (1993). *A Cypherpunk's Manifesto*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt>
- Hülsmann, J. G. (2008). *Deflation and Liberty*. Auburn: Ludwig von Mises Institute. Obtenido de <https://nakamotoinstitute.org/static/docs/deflation-and-liberty.pdf>
- Instituto Xoán de Lugo. (2021). *¿Qué es la Escuela Austriaca?* Obtenido de Instituto Xoán de Lugo: <https://xoandelugo.org/que-es-la-escuela-austriaca/>
- Jacynycz, V., Calvo, A., Hassan, S., & Sánchez-Ruiz, A. (2016). Betfunding: A Distributed Bounty-Based Crowdfunding Platform over Ethereum. *Advances in Intelligent Systems and Computing*, 474, 403-411.
- Jakobsson, M., & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols(Extended Abstract). *The International Federation for Information Processing*, 23. doi:10.1007/978-0-387-35568-9_18
- Johnson, J. (2019). Bitcoin and Venezuela's Unofficial Exchange Rate. *Ledger*, 4. doi:<https://doi.org/10.5195/ledger.2019.170>
- Juels, A., & Brainard, J. (1999). Client Puzzles: A Cryptographic Countermeasure Connection Depletion Attacks. *Proceedings of the Network and Distributed System Security Symposium NDSS*. California: RSA Laboratories. Obtenido de https://www.researchgate.net/publication/221655418_Client_Puzzles_A_Cryptographic_Countermeasure_Against_Connection_Depletion_Attacks

- Kiayias, A., Garay, J., & Leonardos, N. (2017). The Bitcoin Backbone Protocol with Chains of Variable Difficulty. *LECTure Notes in Computer Science*, 291-323. doi:10.1007/978-3-319-63688-7_10
- King, S., & Nadal, S. (2019). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *ACM SIGMETRICS Performance Evaluation Review*.
- Kishimoto, Y., Masuda, K., Yano, M., & Dai, C. (2020). Blockchain and Crypt Currency. *Economics, Law, and Institutions in Asia Pacific*.
- Koepsell, D. R. (2000). *The Ontology of Cyberspace: Philosophy, Law and the Future of Intellectual Property*. Illinois: Carus Publishing Company.
- Kroeger, A., & Sarkar, A. (2017). The Law of One Bitcoin Price? *Federal Reserve Bank of Philadelphia*. Obtenido de <https://www.philadelphiafed.org/-/media/frbp/assets/events/2017/consumer-finance/fintech-2017/day-1/law-of-one-bitcoin-price.pdf>
- Kumar, P., Shrivastava, G., & Tanwar, P. (2020). Demistifying Ethereum Technology: Application and Benefits of Decentralization. *Forensic Investigations and Risk Management in Mobile and Wireless Communications*. doi:10.4018/978-1-5225-9554-0.ch010
- Kumar, R., Duwe, H., & Vilim, M. (2016). Approximate Bitcoin Mining. En IEEE (Ed.), *2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC)*, (págs. 1-6). Austin. doi:10.1145/2897937.2897988
- Leoni, B. (1974). *La libertad y la ley*. Madrid: Unión Editorial.
- Logan, J. (2012). *The Treasure that is Privacy*. Obtenido de Opaque Link : <https://opaque.link/post/the-treasure-that-is-privacy/>
- Lopp, J. (9 de April de 2016). *Bitcoin and the Rise of the Cypherpunks*. Obtenido de Coindesk: <https://www.coindesk.com/the-rise-of-the-cypherpunks>
- Lopp, J. (2016). *Bitcoin and the Rise of the Cypherpunks*. Obtenido de Jameson Lopp: <https://blog.lopp.net/bitcoin-and-the-rise-of-the-cypherpunks/>
- Lopp, J. (2020). *What are the Key Properties of Bitcoin?* Obtenido de Nakamoto.com: <https://nakamoto.com/what-are-the-key-properties-of-bitcoin/>
- Lunt, P. (1996). E-cash becomes reality, via Mark Twain and Digicash. *American Bankers Association. ABA Banking Journal*, 88(1), 62. Obtenido de <https://search.proquest.com/openview/88d7b860c956ca549f8bcd21bb796e9e/1?pq-origsite=gscholar&cbl=47754>
- Maldonado, J. (22 de Marzo de 2020). *¿Qué es la recompensa de bloque?* Obtenido de Cointelegraph: <https://es.cointelegraph.com/explained/what-is-the-block-reward>
- Matarán, C. (2020). Reseña del libro La Teoría del Dinero y del Crédito. *Iberian Journal of the History of Economic Thought*, 7(2), 187-188. doi:<https://revistas.ucm.es/index.php/IJHE/article/view/70949>
- May, T. C. (1988). *The Crypto Anarchist Manifesto*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/crypto-anarchist-manifesto/>

- May, T. C. (1994). *Crypto Anarchy and Virtual Communities*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/virtual-communities/>
- McLaughlin, L. (2006). Philip Zimmermann on What's Next after PGP. *IEEE Security & Privacy*, 4(1), 10-13. doi:10.1109/MSP.2006.20
- Menger, C. (1874). *Principios de Economía Política*. Obra de Dominio Público. Obtenido de <http://www.esflspain.org.server.studentsforliberty.org/wp-content/uploads/2015/09/principios-de-economia-politica.pdf>
- Menger, C. (2009). *The Origins of Money*. (C. Foley, Trad.) Auburn, Alabama: Ludwig Von Mises Institute. Obtenido de https://cdn.mises.org/On%20the%20Origins%20of%20Money_5.pdf
- Metcalfe W. (2020) *Ethereum, Smart Contracts, DApps*. In: Yano M., Dai C., Masuda K., Kishimoto Y. (eds) *Blockchain and Crypto Currency. Economics, Law, and Institutions in Asia Pacific*. Springer, Singapore. https://doi.org/10.1007/978-981-15-3376-1_5
- Microsoft. (2014). *Now you can exchange bitcoins to buy apps, games and more for Windows, Windows Phone and Xbox*. Obtenido de Microsoft: <https://news.microsoft.com/?s=pay+bitcoin>
- Mises Institute. (2021). *¿Qué es la Economía Austriaca?* Obtenido de Mises Institute: <https://mises.org/es/%C2%BFQu%C3%A9-es-la-econom%C3%ADa-austriaca>
- Mises Institute. (2021). *On the Origins of Money*. Obtenido de Mises Institute: <https://mises.org/library/origins-money-0>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de Bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- Nakamoto, S. (05 de February de 2010). *Bitcoin Talk: Proof-of-work difficulty increasing*. Obtenido de The Satoshi Nakamoto Insitute: <https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/22/>
- N. B. Truong, T. Um, B. Zhou and G. M. Lee, "Strengthening the Blockchain-Based Internet of Value with Trust," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1-7, doi: 10.1109/ICC.2018.8423014
- OroyFinanzas. (2015). *¿Qué es el teorema regresivo de mises?* Obtenido de OroyFinanzas.com: <https://www.royfinanzas.com/2015/05/que-teorema-regresivo-mises-origen-dinero/#:~:text=%C2%BFQu%C3%A9%20es%20el%20teorema%20regresivo%20del%20dinero%20de%20Mises%3F&text=Seg%C3%BAn%20este%20teorema%2C%20una%20moneda,en%20d%C3%ADa%20mantendr%C3%ADa%20su%2>
- Partz, H. (24 de January de 2019). *A pesar de anteriores críticas, el CEO de JPMorgan, Jamie Dimon, no celebra el debilitamiento de Bitcoin*. Obtenido de Cointelegraph: <https://es.cointelegraph.com/news/despite-previous-criticism-jpmorgan-ceo-jamie-dimon-doesnt-celebrate-bitcoins-decline>
- Polavieja, M. (2020). *Bitcoin como reserva de valor*. Obtenido de Instituto Juan de Mariana: <https://juandemariana.org/ijm-actualidad/analisis-diario/bitcoin-como-reserva-de-valor/>
- Pouwelse, J., Garbacki, P., Epema, D., & Sips, H. (2005). The Bittorrent P2P File-Sharing System: Measurements and Analysis. *Peer-to-Peer Systems IV Lecture Notes in Computer Science, vol 3640*. doi:https://doi.org/10.1007/11558989_19

- Preukschat, Á. (2017). Capítulo 8. La Descentralización como Modelo de Vida. En G. Gómez Lardies, C. Kuchkovsky, A. Preukschat, D. Díez García, & I. Molero, *Blockchain: la Revolución Industrial de Internet* (págs. 195-199). Madrid: Gestión 2000.
- Preukschat, Á. (2017). Los fundamentos de la Tecnología Blockchain. En Á. Preukschat, C. Kuchovsky, G. Gómez Lardies, D. Díez García, & I. Molero, *Blockchain: la Revolución Industrial de Internet* (págs. 23-31). Barcelona: Gestión 2000.
- Rallo, J. (2009). *El Oro como Refugio Financiero y Reserva*. Obtenido de OroyFinanzas: <https://www.oroymas.com/2009/09/el-oro-como-refugio-financiero-y-reserva-de-valor/>
- Rallo, J. (2010). *Hayek y el Surgimiento del Orden Libre*. Obtenido de Juan Ramón Rallo: <https://juanramonrallo.com/hayek-y-el-surgimiento-del-orden-libre/>
- Rallo, J. (2013). *Una Ilustración Gráfica de la Teoría Austriaca del Ciclo Económico*. Obtenido de Juan Ramón Rallo: <https://juanramonrallo.com/una-ilustracion-grafica-de-la-teoria-austriaca-del-ciclo-economico/>
- Rallo, J. (2014). *El Origen Evolutivo del Dinero*. Obtenido de Juan Ramón Rallo: <https://juanramonrallo.com/el-origen-evolutivo-del-dinero/>
- Rallo, J. (2019). Bitcoin, ¿una alternativa al dólar? *Cotizalia*. Obtenido de https://blogs.elconfidencial.com/economia/laissez-faire/2019-08-26/bitcoin-alternativa-dolar_2191991/
- Rallo, J. (2019). *Liberalismo. Los 10 Principios Básicos del Orden Político Liberal* (8ª ed.). Madrid: Deusto.
- Reuters. (2021). *Analistas ven inflación Argentina 2021 en 48,1%, mejora respecto pronóstico anterior: banco central*. Obtenido de Thomson Reuters: <https://www.reuters.com/article/economia-argentina-idARL2N2L32Z5>
- Ripple. (21 de June de 2017). *The Internet of Value: What It Means and How It Benefits Everyone*. Obtenido de Ripple: <https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/>
- Rosati, S., Fontan, F., Chan, D., & Russo, D. (2007). The Securities Custody Industry. *Occasional Paper Series*(68). Obtenido de <https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp68.pdf>
- Rothbard, M. (2013). *Hacia una Nueva Libertad: Manifiesto Libertario* (1ª ed.). (L. Kofman, Trad.) Madrid: Unión Editorial.
- Rothbard, M. (2016). *Essentials of Money and Inflation*. Obtenido de Mises Institute: <https://mises.org/wire/rothbard-essentials-money-and-inflation>
- Rothbard, M. N. (2009). *The Essential von Mises*. Mises Institute. Obtenido de https://cdn.mises.org/The%20Essential%20von%20Mises_3.pdf
- Runkle, G. (1972). *Anarchism: Old and New*. Dell.
- Schneier, B. (March de 2006). *The Eternal Value of Privacy*. Obtenido de Schneier on Security: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

- Shen, M. (2020). *Why Ethereum and Bitcoin are very different investments*. Obtenido de Coindesk.com: <https://www.coindesk.com/why-ethereum-and-bitcoin-are-very-different-investments>
- Smid, M., & Branstad, D. (1988). The Data Encryption Standard: Past and. *Proceedings of the IEEE*, 76(5). Obtenido de <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4441>
- Song, J. (14 de May de 2018). *Why Blockchain is Hard*. Obtenido de Jimmy Song: <https://jimmysong.medium.com/why-blockchain-is-hard-60416ea4c5c>
- Šurda, P. (2012). *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Obtenido de Tesis. Vienna University of Economics: <https://nakamotoinstitute.org/static/docs/economics-of-bitcoin.pdf>
- Šurda, P. (2013). *Comentario respecto al artículo: Is Bitcoin Money?: What Economists Have To Say*. Obtenido de Economic Policy Journal: <https://www.economicpolicyjournal.com/2013/10/is-bitcoin-money-what-economists-have.html>
- Šurda, P. (2014). The Origin, Classification and Utility of Bitcoin. 1-28. doi:<http://dx.doi.org/10.2139/ssrn.2436823>
- Szabo, N. (1995). Smart Contracts. *Hacker News*. Obtenido de <https://www.tuicool.com/articles/%20U7veauY>
- Szabo, N. (1998). *Bit Gold*. Obtenido de Unenumerated: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
- Szabo, N. (2001). *Trusted Third Parties are Security Holes*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/trusted-third-parties/>
- Szabo, N. (2002). *Shelling Out: The Origins of Money*. Obtenido de The Nakamoto Institute: <https://nakamotoinstitute.org/shelling-out/>
- Szabo, N. (2005). *Bit Gold*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/bit-gold/>
- Szabo, N. (December de 2017). *Winning Strategy for Smart Contracts*. Obtenido de Blockchain Research Institute: https://grazielabrandao.files.wordpress.com/2019/06/g86cmijoemm8wp4g3tktg_1c16c8a028ce11e999f58be72bb04114_szabo-smart-contracts-v6d_1_.pdf
- Tapscott, D., & Tapscott, A. (2017). *La Revolución Blockchain*. (J. M. Salmerón, Trad.) Barcelona: Ediciones Deusto.
- Ammous, S. (2018). *El Patrón Bitcoin* (6ª ed.). (M. Vaquero, Trad.) Barcelona: Deusto.
- Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. *Ethics and Information Technology*. doi:<https://doi.org/10.1007/s10676-020-09571-x>
- Anguiano, J. M. (15 de Noviembre de 2018). *Garrigues Opina: 'Smart Contracts'. Introducción al 'contractware'*. Obtenido de Garrigues: https://www.garrigues.com/es_ES/noticia/smart-contracts-introduccion-al-contractware

- Awad, D. (March de 2021). *Introduction to DApps*. Obtenido de Ethereum:
<https://ethereum.org/en/developers/docs/dapps/>
- Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure*. Obtenido de Hashcash:
<http://www.hashcash.org/papers/hashcash.pdf>
- Bastos, M. A. (29 de Diciembre de 2020). *Algunas cuestiones disputadas sobre el anarcocapitalismo (LII): Los "Cypherpunks"*. Obtenido de Instituto Juan de Mariana:
<https://juandemariana.org/ijm-actualidad/analisis-diario/algunas-cuestiones-disputadas-sobre-el-anarcocapitalismo-lii-los-cypherpunks/>
- Bit2Me. (2021). *¿Qué es la escalabilidad de Bitcoin?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/que-es-escalabilidad-de-bitcoin/#:~:text=Recordemos%20que%20Bitcoin%20tiene%20configurado,transaccion%20caben%20en%20un%20bloque.>
- ¿Qué es la Ethereum Virtual Machine (EVM)?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/que-es-ethereum-virtual-machine-evm/>
- ¿Qué es Prueba de participación / Proof of Stake (PoS)?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/que-es-proof-of-stake-pos/>
- ¿Qué es un Nonce?* Obtenido de Bit2Me Academy: <https://academy.bit2me.com/que-es-nonce/>
- ¿Quién es Adam Back?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/quien-es-adam-back/>
- ¿Quien es David Chaum?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/quien-es-david-chaum/>
- ¿Quién es Nick Szabo?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/quien-es-nick-szabo/>
- ¿Quién es W. Scott Stornetta?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/quien-es-w-scott-stornetta/>
- What is a Cypherpunk?* Obtenido de Bit2Me Academy:
<https://academy.bit2me.com/en/what-is-a-cypherpunk/>
- Bitcoin Developer. (2021). *Glossary*. Obtenido de Bitcoin Developer:
<https://developer.bitcoin.org/glossary.html>
- Blockchain.com. (03 de Marzo de 2021). *Bitcoin Explorer: Bloques*. Obtenido de Blockchain.com: <https://www.blockchain.com/btc/blocks?page=1>
- BTC.com. (03 de Marzo de 2021). *Latest Blocks*. Obtenido de BTC.com: <https://btc.com/>
- Buffett, W. (2020). Warren Buffett: Cryptocurrency ‘has no value’ – ‘I don’t own any and never will’. (B. Quick, Entrevistador) Obtenido de <https://www.cnbc.com/2020/02/24/warren-buffett-cryptocurrency-has-no-value.html>
- Buterin, V. (2014). *Ethereum Whitepaper*. Obtenido de Ethereum.org:
<https://ethereum.org/en/whitepaper/>
- Buterin, V. (2016). *Ethereum: Platform Review. Opportunities and Challenges for Private and Consortium Blockchains*. Obtenido de Bitcoin Magazine.

- Carrascosa, C., Kuchkovsky, C., & Preukschat, Á. (2017). Hactivismo, cypherpunks y el nacimiento de la blockchain. En Á. Preukschat, C. Kuchovsky, G. Gómez Lardies, D. Díez García, Í. Molero, & Á. P. (coord.) (Ed.), *Blockchain: la Revolución Industrial de Internet* (8ª ed., págs. 175-189). Barcelona: Gestión 2000.
- Cerf, V. G., & Kahn, R. E. (May de 1974). A Protocol for Packet Network Intercommunication. *IEEE Trans on Comms*, 22(5).
- Chamapgne, P. (2014). *El Libro de Satoshi*. BlockchainEspaña.com. Obtenido de <https://libroblockchain.com/satoshi/>
- Chaum, D. (1985). SEcurity without Identification: Card Computers to make Big Brother Obsolete. *Communications of the ACM*, 28(10), 1030-1044. Obtenido de https://www.chaum.com/publications/Security_Wthout_Identification.html
- Chohan, U. W. (2017). Cryptoanarchism and Cryptocurrencies. doi:<http://dx.doi.org/10.2139/ssrn.3079241>
- Cloudflare. (2021). *Ataque de inundación SYN*. Obtenido de Cloudflare: <https://www.cloudflare.com/es-la/learning/ddos/syn-flood-ddos-attack/>
- Coinbase. (19 de 02 de 2021). *Coinbase*. Obtenido de <https://www.coinbase.com/es/>
- CoinMarketCap. (19 de Febrero de 2021). *Bitcoin*. doi:<https://coinmarketcap.com/es/currencies/bitcoin/>
- Dai, W. (1998). *B-Money*. Obtenido de weidai.com: <http://www.weidai.com/bmoney.txt>
- Dannen, C. (2017). *Introducing Ethereum and Solidity*. New York: Apress.
- DappRadar. (2021). *Top Blockchain Dapps*. Obtenido de DappRadar.com: <https://dappradar.com/rankings/protocol/ethereum>
- de la Guía, D., Hernández, L., Montoya, F., Muñoz, J., & Fúster, A. (2004). *Técnicas Criptográficas de protección de datos* (3ª ed.). Madrid: Ra-Ma.
- Dev, J. A. (2014). Bitcoin mining acceleration and performance quantification. En IEEE (Ed.), *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, (págs. 1-6). Toronto. doi:10.1109/CCECE.2014.6900989
- Díez García, D., & Gómez Lardies, G. (2017). Banca y blockchain, ¿pioneros por necesidad? En Á. Preukschat, C. Kuchovsky, . G. Gómez Lardies, D. Díez García, Í. Molero, & Á. Preukschat (Ed.), *Blockchain: la Revolución Industrial de Internet* (págs. 32-43). Barcelona: Gestión 2000.
- Díez García, D., & Gómez Lardies, G. (2017). Banca y Blockchain, ¿pioneros por necesidad? Y Las Aseguradoras se Reinventan. En Á. Preukschat, C. Kuchovsky, . G. Gómez Lardies, D. Díez García, Í. Molero, & Á. Preukschat (Ed.), *Blockchain: la Revolución Industrial de Internet* (págs. 32-43). Barcelona: Gestión 2000.
- Diffie, W., & Hellman, M. (November de 1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 645-654. Obtenido de <https://ee.stanford.edu/~hellman/publications/24.pdf>
- Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. *Lecture Notes in Computer Science*, 740. doi:https://doi.org/10.1007/3-540-48071-4_10

- Erfani, S., & Ahmad, M. (2019). Bitcoin Security Reference Model: An Implementation Platform. *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, (págs. 1-5). Iasi. doi:10.1109/ISSCS.2019.8801796
- Escudero, V. (2017). Software Libre y código abierto en el mundo de las Blockchains. En A. Preukschat, C. Kuchkovsky, G. Gómez Lardies, D. Díez García, & Í. Molero, *Blockchain: la Revolución Industrial de Internet* (págs. 221-227). Gestión 2000.
- Ethereum. (25 de 1 de 2021). *What is Ethereum?* Obtenido de Ethereum: <https://ethereum.org/es/what-is-ethereum/>
- Finney, H. (2004). *RPOW - Reusable Proofs of Work*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/rpow/>
- Fridrich, J., & Goljan, M. (2000). Robust Hash Functions for Digital Watermarking. En IEEE (Ed.), *Proceedings International Conference on Information Technology: Coding and Computing*, (págs. 178-183). Las Vegas. doi:10.1109/ITCC.2000.844203
- Garay, J., Kiayias, A., & Leonardos, N. (2017). *The Bitcoin Backbone Protocol with Chains of Variable Difficulty. Lecture Notes in Computer Science*, 291–323. doi:10.1007/978-3-319-63688-7_10
- Gupta, V. (2017). A Brief History of Blockchain. *Harvard Business Review Digital Articles*, 2–4.
- Haber, S., & Stornetta, W. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2), 99-111.
- He, Z., & Cong, L. W. (May de 2019). Blockchain Disruption and Smart Contracts. (I. Goldstein, Ed.) *Review of Financial Studies*, 23(5), 1754-1797.
- Hughes, E. (1993). *A Cypherpunk's Manifesto*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt>
- Jakobsson, M., & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols(Extended Abstract). *The International Federation for Information Processing*, 23. doi:10.1007/978-0-387-35568-9_18
- Juels, A., & Brainard, J. (1999). Client Puzzles: A Cryptographic Countermeasure Connection Depletion Attacks. *Proceedings of the Network and Distributed System Security Symposium NDSS*. California: RSA Laboratories. Obtenido de https://www.researchgate.net/publication/221655418_Client_Puzzles_A_Cryptographic_Countermeasure_Against_Connection_Depletion_Attacks
- Kiayias, A., Garay, J., & Leonardos, N. (2017). The Bitcoin Backbone Protocol with Chains of Variable Difficulty. *Lecture Notes in Computer Science*, 291-323. doi:10.1007/978-3-319-63688-7_10
- King, S., & Nadal, S. (2019). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *ACM SIGMETRICS Performance Evaluation Review*.
- Kishimoto, Y., Masuda, K., Yano, M., & Dai, C. (2020). Blockchain and Crypt Currency. *Economics, Law, and Institutions in Asia Pacific*.
- Koepsell, D. R. (2000). *The Ontology of Cyberspace: Philosophy, Law and the Future of Intellectual Property*. Illinois: Carus Publishing Company.

- Kumar, P., Shrivastava, G., & Tanwar, P. (2020). Demistifying Ethereum Technology: Application and Benefits of Decentralization. *Forensic Investigations and Risk Management in Mobile and Wireless Communications*. doi:10.4018/978-1-5225-9554-0.ch010
- Kumar, R., Duwe, H., & Vilim, M. (2016). Approximate Bitcoin Mining. En IEEE (Ed.), *2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC)*, (págs. 1-6). Austin. doi:10.1145/2897937.2897988
- Logan, J. (2012). *The Treasure that is Privacy*. Obtenido de Opaque Link : <https://opaque.link/post/the-treasure-that-is-privacy/>
- Lopp, J. (9 de April de 2016). *Bitcoin and the Rise of the Cypherpunks*. Obtenido de Coindesk: <https://www.coindesk.com/the-rise-of-the-cypherpunks>
- Lopp, J. (2016). *Bitcoin and the Rise of the Cypherpunks*. Obtenido de Jameson Lopp: <https://blog.lopp.net/bitcoin-and-the-rise-of-the-cypherpunks/>
- Lunt, P. (1996). E-cash becomes reality, via Mark Twain and Digicash. *American Bankers Association. ABA Banking Journal*, 88(1), 62. Obtenido de <https://search.proquest.com/openview/88d7b860c956ca549f8bcd21bb796e9e/1?pq-origsite=gscholar&cbl=47754>
- Maldonado, J. (22 de Marzo de 2020). *¿Qué es la recompensa de bloque?* Obtenido de Cointelegraph: <https://es.cointelegraph.com/explained/what-is-the-block-reward>
- McLaughlin, L. (2006). Philip Zimmermann on What's Next after PGP. *IEEE Security & Privacy*, 4(1), 10-13. doi:10.1109/MSP.2006.20
- Metcalfe W. (2020) Ethereum, Smart Contracts, DApps. In: Yano M., Dai C., Masuda K., Kishimoto Y. (eds) *Blockchain and Crypto Currency. Economics, Law, and Institutions in Asia Pacific*. Springer, Singapore. https://doi.org/10.1007/978-981-15-3376-1_5
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de Bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- Nakamoto, S. (05 de February de 2010). *Bitcoin Talk: Proof-of-work difficulty increasing*. Obtenido de The Satoshi Nakamoto Insitute: <https://satoshi.nakamoinstitute.org/posts/bitcointalk/threads/22/>
- N. B. Truong, T. Um, B. Zhou and G. M. Lee, "Strengthening the Blockchain-Based Internet of Value with Trust," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1-7, doi: 10.1109/ICC.2018.8423014
- Partz, H. (24 de January de 2019). *A pesar de anteriores críticas, el CEO de JPMorgan, Jamie Dimon, no celebra el debilitamiento de Bitcoin*. Obtenido de Cointelegraph: <https://es.cointelegraph.com/news/despite-previous-criticism-jpmorgan-ceo-jamie-dimon-doesnt-celebrate-bitcoins-decline>
- Pouwelse, J., Garbacki, P., Epema, D., & Sips, H. (2005). The Bittorrent P2P File-Sharing System: Measurements and Analysis. *Peer-to-Peer Systems IV Lecture Notes in Computer Science, vol 3640*. doi:https://doi.org/10.1007/11558989_19
- Preukschat, Á. (2017). Los fundamentos de la Tecnología Blockchain. En Á. Preukschat, C. Kuchovsky, G. Gómez Lardies, D. Díez García, & I. Molero, *Blockchain: la Revolución Industrial de Internet* (págs. 23-31). Barcelona: Gestión 2000.

- Ripple. (21 de June de 2017). *The Internet of Value: What It Means and How It Benefits Everyone*. Obtenido de Ripple: <https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/>
- Schneier, B. (March de 2006). *The Eternal Value of Privacy*. Obtenido de Schneier on Security: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html
- Smid, M., & Branstad, D. (1988). The Data Encryption Standard: Past and. *Proceedings of the IEEE*, 76(5). Obtenido de <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4441>
- Song, J. (14 de May de 2018). *Why Blockchain is Hard*. Obtenido de Jimmy Song: <https://jimmysong.medium.com/why-blockchain-is-hard-60416ea4c5c>
- Szabo, N. (1995). Smart Contracts. *Hacker News*. Obtenido de <https://www.tuicool.com/articles/%20U7veauY>
- Szabo, N. (1998). *Bit Gold*. Obtenido de Unenumerated: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
- Szabo, N. (2001). *Trusted Third Parties are Security Holes*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/trusted-third-parties/>
- Szabo, N. (2005). *Bit Gold*. Obtenido de Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/bit-gold/>
- Szabo, N. (December de 2017). *Winning Strategy for Smart Contracts*. Obtenido de Blockchain Research Institute: https://grazielabrandao.files.wordpress.com/2019/06/g86cmijoemm8wp4g3tktg_1c16c8a028ce11e999f58be72bb04114_szabo-smart-contracts-v6d_1_.pdf
- Tapscott, D., & Tapscott, A. (2017). *La Revolución Blockchain*. (J. M. Salmerón, Trad.) Barcelona: Ediciones Deusto.
- Tomov, Y. K. (2019). Bitcoin: Evolution of Blockchain Technology. En IEEE (Ed.), *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*, (págs. 1-4). Sozopol. doi:10.1109/ET.2019.8878322
- Tikhomirov S. (2018) Ethereum: State of Knowledge and Research Perspectives. In: Imine A., Fernandez J., Marion JY., Logrippo L., Garcia-Alfaro J. (eds) Foundations and Practice of Security. FPS 2017. Lecture Notes in Computer Science, vol 10723. Springer, Cham. https://doi.org/10.1007/978-3-319-75650-9_14
- Tomov, Y. K. (2019). Bitcoin: Evolution of Blockchain Technology. En IEEE (Ed.), *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*, (págs. 1-4). Sozopol. doi:10.1109/ET.2019.8878322
- Truong, N., Um, T.-W., Zhou, B., & Myoung Lee, G. (2018). Strengthening the Blockchain-based Internet of Value with Trust. *IEEE International Conference on Communications (ICC)*, (págs. 1-7). Kansas City. doi:10.1109/ICC.2018.8423014
- Tucker, J. A. (2014). *What gave Bitcoin its value?* Obtenido de FEE: <https://fee.org/articles/what-gave-bitcoin-its-value/>
- Várez, J. L. (2017). Prólogo. En A. Preukschat, C. Kuchkovsky, G. Gómez Lardies, D. Díez García, Í. Molero, & A. Preukschat (Ed.), *Blockchain: La Revolución Industrial de Internet* (8ª ed., págs. 11-15). Barcelona: Gestión 2000.

- von Mises, L. (1997). *La Teoría del Dinero y del Crédito*. (J. M. Fuente, Trad.) Madrid: Unión Editorial.
- von Mises, L. (2003). *The Historical Setting of the Austrian*. Ludwig von Mises Institute. Obtenido de https://cdn.mises.org/Historical%20Setting%20of%20the%20Austrian%20School%20of%20Economics_3.pdf
- von Mises, L. (2011). *La Acción Humana*. Madrid: Unión Editorial.
- Weber, W. E. (2016). A Bitcoin standard: Lessons from the gold standard. *Bank of Canada Staff Working Paper*(2016-14).
- Wood, G. (2014). Ethereum: a Secure Decentralised Generalised Transaction Ledger. *Ethereum project yellow paper*, 51(2014), 1-32.
- Xu, B. (2014). Media Censorship in China. *Council on Foreign Relations*.
- Y. K. Tomov, "Bitcoin: Evolution of Blockchain Technology," *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*, Sozopol, Bulgaria, 2019, pp. 1-4, doi: 10.1109/ET.2019.8878322.
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE 6th International Congress on Big Data*, (págs. 557-564). doi:10.1109/BigDataCongress.2017.85
- Zimmermann, P. (1999). *Why I Wrote PGP*. Obtenido de The Satoshi Nakamoto Institute: <https://nakamotoinstitute.org/why-i-wrote-pgp/>
- Zimmermann, P. (2021). *Creador de PGP*. Obtenido de Philip Zimmermann: <https://philzimmermann.com/EN/background/index.html>