

ÍNDICE

PRÓLOGO	XIII
CAPÍTULO 1. BITCOIN: ORIGEN DE LA CADENA DE BLOQUES.....	1
1.1 Introducción	1
1.2 Transacciones en Bitcoin.....	4
1.3 Cambio de paradigma	6
1.4 Prueba de trabajo en Bitcoin.....	8
1.5 Halving en Bitcoin	10
1.6 Proceso de minería	12
1.6.1 Los mineros en una red Blockchain.....	13
1.6.2 Incentivos.....	14
1.6.3 Pool de minado	17
1.6.4 Mempools	19
CAPÍTULO 2. INTRODUCCIÓN A BLOCKCHAIN	23
2.1 Introducción	23
2.2 Historia del concepto de Blockchain	24
2.3 Análisis de la tecnología Blockchain.....	25
2.3.1 Redes Peer to Peer (P2P)	27
2.4 Estructura de la cadena de bloques	29
2.4.1 Producción de bloques.....	30
2.4.2 Estructura básica de un bloque.....	31
2.4.3 Cabecera de bloque e inmutabilidad	32
2.4.4 Árboles de Merkle	33

2.4.5	Uso de árboles de Merkle en Blockchain	35
2.4.6	Bloques en Ethereum	36
2.5	Transacciones en Blockchain	37
2.6	Algoritmos de criptografía	41
2.6.1	Funciones hash	41
2.7	Criptografía asimétrica	43
2.7.1	Algoritmo ECDSA de curva elíptica	44
2.7.2	Taproot y uso de firmas Schnorr	45
CAPÍTULO 3. EL CONSENSO EN BLOCKCHAIN		47
3.1	Introducción	47
3.2	Algoritmos de consenso en la cadena de bloques	48
3.2.1	Algoritmo Prueba de Trabajo (Proof of Work)	49
3.2.2	Algoritmo Prueba de Participación (Proof of Stake)	52
3.2.3	Algoritmo Prueba de Participación Delegada (Delegated Proof of Stake)	57
3.2.4	Algoritmo Tolerancia a Fallos Bizantina Delegada	61
3.2.5	Algoritmo Prueba de Actividad (Proof of Activity)	62
3.2.6	Algoritmo Prueba de Autoridad (Proof of Authority)	63
3.2.7	Algoritmo Prueba de Quemado (Proof of Burn)	65
3.2.8	Algoritmo Prueba de Capacidad (Proof of Capacity)	66
3.2.9	Algoritmo Prueba por Tiempo Transcurrido (Proof of Elapsed Time)	67
3.2.10	Algoritmo Prueba de Punto de Control (Proof of Checkpoint)	68
3.2.11	Algoritmo de consenso de Ripple	68
3.3	Evolución de los algoritmos de consenso	69
3.3.1	Obelisk Consensus Algorithm (OCA)	70
3.3.2	Aplicaciones y ámbitos de uso	71
3.3.3	Nuevo paradigma Web of Trust	72
3.3.4	Algoritmo Prueba de Formulación	73
3.3.5	Algoritmo Overlord	75
3.3.6	Algoritmo Tolerante a Fallos Bizantino Mixto (MBFT)	75
3.3.7	Algoritmo SBAC (Shard Byzantinus Atomic Commit)	76
CAPÍTULO 4. BIFURCACIONES EN BLOCKCHAIN		79
4.1	Introducción	79
4.2	Tipos de bifurcaciones	80
4.2.1	Testigo Segregado (Segregated Witness)	81
4.2.2	Hard Forks en BitCoin	82
4.2.3	Hard Forks en Ethereum	83
4.3	Tipos de Blockchain	84
4.3.1	Blockchain pública	86

4.3.2 Blockchain privada	87
4.3.3 Blockchain híbrida o federada.....	89
4.3.4 Blockchain permitida vs pública.....	91
4.4 Protocolos Blockchain	91
4.4.1 HyperLedger	92
4.4.2 HyperLedger Fabric	95
4.4.3 HyperLedger SawTooth.....	97
4.4.4 Quorum.....	98
4.4.5 Corda.....	98
4.4.6 Enterprise Ethereum	98
4.5 Blockchain de segunda generación	99
4.6 Blockchain de tercera generación	100
CAPÍTULO 5. FUNDAMENTOS DE ETHEREUM	105
5.1 Introducción	105
5.2 Migración a Proof of Stake	107
5.2.1 Fusión o Merge en Ethereum	108
5.2.2 Fragmentación en Ethereum 2.0.....	109
5.3 Ethereum 2.0	109
5.3.1 Escalabilidad en Ethereum	110
5.3.2 Blockchain fragmentada.....	110
5.3.3 Fases de implementación de Ethereum 2.0	111
5.4 Características técnicas de Ethereum	111
5.4.1 Ventajas de utilizar Ethereum	112
5.4.2 Bitcoin vs Ethereum	113
5.5 Transacciones en Ethereum	114
5.5.1 Estructura de una transacción en Ethereum	115
5.5.2 El gas en Ethereum.....	117
5.5.3 Mensajes y transacciones	119
5.5.4 Función de transición de estado	120
5.5.5 Bloques en Ethereum.....	121
5.5.6 Tamaño y tiempo de generación de bloques	122
5.6 Máquina Virtual de Ethereum (EVM).....	123
5.6.1 Características de la EVM.....	124
5.6.2 Lenguajes de alto nivel de la EVM.....	124
5.6.3 Compilando código Solidity con Solc.....	125
5.6.4 Cuentas en Ethereum.....	127
5.6.5 Contratos inteligentes.....	129
5.7 Casos de uso de Ethereum	131
5.8 Explorando Ethereum con Etherscan	132

5.9 Añadiendo escalabilidad en Ethereum con Plasma.....	134
5.9.1 Mecanismo off-chain.....	136
5.9.2 Protección de la red con pruebas de fraude	138
5.9.3 Ventajas de Plasma	138
5.9.4 Seguridad en Plasma	139
5.9.5 Implementaciones de Plasma	140
5.9.6 Conclusiones de Plasma	141
5.10 Arbitrum.....	142
5.10.1 Uso de Optimistic RollUp en Arbitrum	144
5.10.2 AnyTrust Chains en Arbitrum	146
5.11 Probando smart contracts.....	146
5.12 Proyectos sobre Ethereum.....	147
5.13 Seguridad en Ethereum.....	147

CAPÍTULO 6. CONTRATOS INTELIGENTES, ORÁCULOS Y APLICACIONES

CENTRALIZADAS.....	149
6.1 Introducción.....	149
6.2 Lenguajes y frameworks de desarrollo.....	150
6.2.1 Framework Substrate.....	151
6.3 Oráculos	155
6.3.1 Características de los oráculos	156
6.3.2 Tipos de oráculos Blockchain	156
6.3.3 Riesgos de seguridad en los oráculos.....	158
6.3.4 Casos de usos de oráculos.....	159
6.3.5 ChainLink.....	160

CAPÍTULO 7. PROTOCOLOS DE SEGUNDA CAPA..... 163

7.1 Introducción.....	163
7.2 Lightning Network.....	163
7.3 Tipos de protocolos de segunda capa	165
7.3.1 State channels (Canales de estado).....	165
7.3.2 Sidechains (Cadenas laterales).....	165
7.4 Rollups.....	168
7.4.1 Zk-Rollups.....	169
7.4.2 Objetivos de las zk-Rollups.....	169
7.4.3 Casos de usos de las zk-Rollups.....	170
7.5 Prueba de conocimiento cero (zkp)	171
7.5.1 ZkLedger.....	172
7.5.2 Zk-SNARK.....	173
7.5.3 Zk-STARK	173

CAPÍTULO 8. APLICACIONES Y ACTIVOS DIGITALES EN BLOCKCHAIN	177
8.1 Introducción	177
8.2 Distributed Ledger Technology (dlt).....	178
8.2.1 Componentes de Distributed Ledger Technology	179
8.2.2 Tipos de tecnologías de registro distribuido	180
8.2.3 DLT vs Blockchain	181
8.2.4 Mecanismos de consenso y reglas de validación	182
8.2.5 Conclusiones DLT	183
8.3 Modelo de identidad en Blockchain.....	183
8.3.1 Identidad digital e identidad digital soberana.....	184
8.3.2 Aplicaciones de la identidad digital soberana	186
8.3.3 Credenciales verificables.....	186
8.3.4 Identidad digital autosoberana	188
8.3.5 Proyectos de identidad digital descentralizada.....	190
8.3.6 Administración de identidades habilitada por Blockchain	191
8.3.7 Modelos de identidad digital en Blockchain	191
 CAPÍTULO 9. INTRODUCCIÓN A LAS BILLETERAS (WALLETS).....	 193
9.1 Introducción	193
9.2 Tipos de billeteras	193
9.3 Billeteras de papel.....	196
9.4 Billeteras de hardware Trezor	197
9.5 Operaciones P2P (persona a persona)	198
 CAPÍTULO 10. TOKENOMICS	 199
10.1 Introducción	199
10.2 De las criptomonedas a la tokenización	200
10.3 Tipos de tokens	201
10.3.1 Utility Tokens	201
10.3.2 Security Tokens	202
10.4 Estándares ERC para tokens.....	203
10.4.1 Token ERC-20	204
 CAPÍTULO 11. FINANZAS DESCENTRALIZADAS (DEFI)	 207
11.1 Introducción	207
11.2 Finanzas descentralizadas	207
11.2.1 Aplicaciones para finanzas descentralizadas.....	208
11.2.2 Organizaciones autónomas descentralizadas (DAO).....	209
11.3 Otros proyectos.....	210
11.3.1 MakerDAO.....	211
11.3.2 Compound.....	211

11.3.3 Dharma.....	211
11.4 Conclusiones	212
CAPÍTULO 12. PROYECTOS CRYPTO	213
12.1 Introducción al concepto de mainnet (red principal).....	213
12.2 Kadena	214
12.2.1 Protocolo Tendermint	215
12.2.2 Seguridad en Kadena.....	219
12.3 Klaytn	219
12.4 Quant	220
12.4.1 Sistema Operativo Overledger OS.....	223
12.4.2 Funcionamiento de Quant Network.....	223
12.4.3 Token QNT.....	225
12.5 Cardano.....	225
12.6 Polygon: una Blockchain para Ethereum.....	227
12.6.1 Uso de Proof of Stake.....	228
12.6.2 Características de Polygon	229
12.6.3 MATIC: Token nativo de Polygon	230
12.6.4 Polymarket	231
12.6.5 Polygon Edge.....	231
12.6.6 Polygon ID	231
12.7 Telos Blockchain.....	234
12.8 Fantom Blockchain.....	237
12.8.1 Uso de Proof of Stake.....	238
12.8.2 Lachesis como algoritmo de consenso	238
12.8.3 Token FTM.....	238
12.8.4 Fantom Opera	239
12.9 Solana Blockchain.....	239
12.9.1 Funcionamiento de Solana.....	241
12.9.2 Proof of History	242
12.9.3 Gulf Stream	242
12.9.4 Token SOL.....	243
12.9.5 Proyectos basados en la Blockchain de Solana	245
12.10 Cosmos (atom)	245
12.11 Airdrops.....	247
12.12 Polkadot	248
12.12.1 Arquitectura de Polkadot.....	248
12.12.2 Parachains	249
12.12.3 Parachains vs Contratos inteligentes	251
12.12.4 Escalabilidad e interoperabilidad	251

12.12.5 Mecanismo de comunicación entre parachains.....	252
12.12.6 Conclusiones parachains	253
12.12.7 Parathreads.....	253
12.12.8 Bridges o puentes.....	254
12.12.9 Nominadores y validadores.....	254
12.12.10 Parachains Auctions (Subastas).....	255
12.12.11 Proyectos destacados que usan Polkadot	256
12.12.12 Shiden Network (SDN).....	256
12.12.13 OVM (Optimistic Virtual Machine)	257
12.12.14 LockDrop	259
12.12.15 Dapps Staking.....	260
12.12.16 Phala Network (PHA).....	260
12.13 Kusama: red de pruebas de Polkadot	262
12.13.1 Características de Kusama.....	264
12.13.2 Parachains en Kusama.....	264
12.13.3 Casos de uso en Kusama	265
12.13.4 Token de Kusama	265
12.13.5 Roles de usuarios en Kusama	266
12.13.6 Proceso de gobernanza en Kusama	267
CAPÍTULO 13. CIBERSEGURIDAD EN BLOCKCHAIN	269
13.1 Introducción.....	269
13.2 Uso de criptografía.....	269
13.2.1 Funciones Hash	270
13.2.2 Claves públicas y privadas	270
13.3 Descentralización	271
13.4 Protocolos de comunicación	272
13.5 Ataques en Blockchain	273
13.5.1 Ataque del 51%	273
13.5.2 Impacto del ataque del 51%.....	273
13.5.3 Ataque de doble gasto	276
13.5.4 Ataque Finney	278
13.5.5 Ataques Sybil.....	278
13.5.6 Ataque Eclipse.....	280
13.5.7 Ataque Replay	281
13.5.8 Ataque de enrutamiento.....	281
13.5.9 Ataque de Phising	281
13.5.10 Ataque de ransomware.....	282
13.5.11 Ataque a los exchanges.....	282
13.5.12 Ataque DEFI.....	282

13.5.13 Ataque Rug Pull	282
13.5.14 Ataque de denegación de servicio	282
13.6 Cryptomining.....	283
13.6.1 Cryptomining vía malware o cryptojacking.....	284
13.6.2 Ataques de cryptojacking	285
13.6.3 Protección frente al cryptomining.....	287
13.7 Seguridad Blockchain para la empresa.....	288
13.7.1 Uso de inteligencia artificial	288
13.8 Conclusiones	289
GLOSARIO DE TÉRMINOS	291
ÍNDICE ANALÍTICO	309

PRÓLOGO

SOBRE EL LIBRO

En este libro el lector aprenderá los conceptos fundamentales de la tecnología Blockchain, su historia, su arquitectura, protocolos y aplicaciones. Se analizarán los principales proyectos Blockchain que permiten el desarrollo de aplicaciones descentralizadas y se estudiarán los principales protocolos de consenso, las tecnologías utilizadas y sus aplicaciones.

OBJETIVOS

Los objetivos de este trabajo pueden ser definidos en los siguientes puntos:

- Conocer y explicar los fundamentos de las tecnologías Blockchain.
- Describir el funcionamiento de la cadena de bloques de Bitcoin, la cual asienta las bases de muchas de las funcionalidades de las cadenas de bloques que coexisten en la actualidad.
- Comprender las ventajas y características de la descentralización estudiando el minado de criptomonedas.
- Comprender las bases técnicas de las aplicaciones descentralizadas basadas en Ethereum/Blockchain.

- Describir el funcionamiento de la cadena de bloques de Ethereum comparándolo respecto a la tecnología de Bitcoin. A su vez, desarrollar algunas características más distinguibles de la tecnología Ethereum.
- Conocer los principales tipos de billeteras para almacenar criptomonedas.
- Comprender cómo Ethereum puede ser usado para la generación de contratos inteligentes.
- Dar a conocer los conceptos de tokenomics y Finanzas descentralizadas (DEFI).
- Describir las principales amenazas de ciberseguridad a tener en cuenta en los proyectos basados en Blockchain.

EL AUTOR

José Manuel Ortega es ingeniero de software e investigador de ciberseguridad con interés en nuevas tecnologías, open source, seguridad y testing. En los últimos años ha mostrado interés en proyectos de innovación utilizando tecnologías Big Data y lenguajes de programación como Python.

Actualmente se encuentra trabajando como ingeniero de software en proyectos de investigación relacionados con Big Data, Ciberseguridad y Blockchain. Ha impartido docencia a nivel universitario y colaborado con el colegio oficial de ingenieros informáticos. También ha sido ponente en varias conferencias orientadas a desarrolladores a nivel nacional e internacional. Más información acerca de las conferencias impartidas y otros trabajos publicados se puede consultar en su sitio personal <https://josemanuelortegablog.com>

BITCOIN: ORIGEN DE LA CADENA DE BLOQUES

1.1 INTRODUCCIÓN

En octubre de 2008, una persona o grupo de personas bajo el pseudónimo de Satoshi Nakamoto presenta un documento académico denominado “**Bitcoin: a peer-to-peer electronic cash system**” en una lista de correo electrónico sobre criptografía. Este texto introdujo las bases de un sistema de efectivo electrónico descentralizado entre pares, llamado Bitcoin. El documento se puede consultar de forma abierta en <https://bitcoin.org/bitcoin.pdf>.

El objetivo de este documento es crear un nuevo mecanismo de pagos en internet, ya que el sistema de pagos en internet se basa mayoritariamente en un sistema de confianza en terceros, ya sean bancos o cualquier otra entidad, que tienen como cometido mover el dinero y generar transacciones a petición de sus clientes, lo cual requiere de un cierto nivel de confianza en estas entidades para registrar y gestionar el dinero de cada usuario, siendo en su mayoría, de una forma bastante opaca y con total desconocimiento de lo que sucede realmente con el dinero.

El documento comienza con una introducción explicando el problema que trata de resolver. Hoy en día, las aplicaciones de comercio electrónico dependen en su mayoría de instituciones financieras que actúan como terceros de confianza.

Por ejemplo, cuando yo realizo una compra en una tienda y pago con tarjeta de crédito o débito, el dinero no va desde mi cuenta a la cuenta del proveedor de forma directa, sino que en su lugar hay un intermediario o tercero de confianza, normalmente el banco, que verifica la transacción y la aprueba.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figura 1.1: Abstract del documento que dio a conocer el Bitcoin

Este documento propone el uso de una nueva tecnología totalmente descentralizada, que permita realizar pagos entre pares sin la necesidad de una entidad intermediaria en un medio electrónico, todo ello, gracias a la criptografía y a la capacidad de cómputo de los dispositivos electrónicos, que garantizará la seguridad del sistema en sí mismo y de las transacciones que se lleven en ella.

En el documento, se define la tecnología como “Bitcoin”, pero a su vez, también se asientan las bases del funcionamiento de un sistema público y descentralizado que registra globalmente las transacciones realizadas en el sistema, la cadena de bloques descentralizada o “Blockchain”, que, con el paso del tiempo, ha ido evolucionando hasta la creación de nuevas cadenas de bloques más complejas y añadiendo más utilidades a estas. Hasta tal punto, que hoy por hoy se estima que existen miles de cadenas de bloques con distintas implementaciones, o incluso algunas de ellas de uso privado.

El propósito de Bitcoin es ser un medio de efectivo electrónico entre pares. Para ello, se apoya en un sistema de pagos electrónicos basados en pruebas criptográficas en lugar de emplear un tercero de confianza para validar ese pago.

Bitcoin es un protocolo de código abierto, que se caracteriza por ser descentralizado en su diseño, ya que no requiere de un nodo central que almacene y procese toda la información, sino un conjunto de nodos distribuidos alrededor del mundo que se comunican entre sí y todos tienen la misma información actualizada.

Bitcoin se creó para prescindir de una entidad centralizada que pudiera manipular la información o censurar el uso de Bitcoin. **Bitcoin** con mayúscula hace referencia al **protocolo**, a la red. Mientras que **bitcoin** con minúscula hace referencia a la **unidad monetaria**, la cual puede dividirse hasta 8 decimales. Esto significa que la mínima cantidad de bitcoins que se puede poseer es 0.00000001 BTC, que como homenaje al creador se conoce como un Satoshi.

Como dato curioso destacar que el 3 de enero de 2009, nació el primer bloque de transacciones de la red Bitcoin. Un bloque minado por Satoshi Nakamoto, con una recompensa utilizando el mecanismo de prueba de trabajo. Este bloque luego es verificado por todos los nodos de la red descentralizada de Bitcoin para darle veracidad al dato.

El protocolo Bitcoin posee mecanismos de consenso que hacen posible que la red funcione de forma descentralizada y tenga incentivos para validar las transacciones y añadir bloques a la cadena.

Las **transacciones** quedan registradas de forma pública en una base de datos y basándose en las transacciones procesadas en la red, el sistema determina el saldo que tiene cada dirección Bitcoin. Esta base de datos donde se registran todos los movimientos producidos es la llamada Cadena de Bloques, o Blockchain, que explicaremos más adelante.

En Bitcoin no es posible la falsificación ya que, al ser una secuencia de datos encadenados y una combinación de transacciones, la única forma de realizar una transacción fraudulenta sería cambiando una transacción, y la anterior, y la anterior, hasta el bloque cero, lo cual es imposible.

La red Bitcoin está compuesta por miles de nodos alrededor de todo el mundo, cada uno de los cuales contiene la copia exacta y actualizada de toda la cadena de bloques, y en cada bloque se almacenan transacciones, información de ese bloque y su vinculación con el bloque anterior. De manera que si un nodo dejase de funcionar

la red no se vería afectada, y a su vez no hay un nodo central que sea más importante que el resto de la red. En resumen, Bitcoin consiste de:

- Una red entre pares distribuida (el protocolo Bitcoin).
- Un libro contable público (la cadena de bloques, o Blockchain)
- Un sistema distribuido, matemático y determinístico de emisión de moneda (minería distribuida)

Actualmente existen unos 13.000 nodos como se puede ver en la página <https://bitnodes.io>

REACHABLE BITCOIN NODES

Updated: Thu May 25 18:41:45 2023 CEST

17228 NODES

CHARTS

IPv4: -2.6% / IPv6: -1.2% / .onion: +4.6%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	10600 (61.53%)
2	United States	1648 (9.57%)
3	Germany	1364 (7.92%)
4	France	470 (2.73%)
5	Netherlands	340 (1.97%)
6	Canada	298 (1.73%)

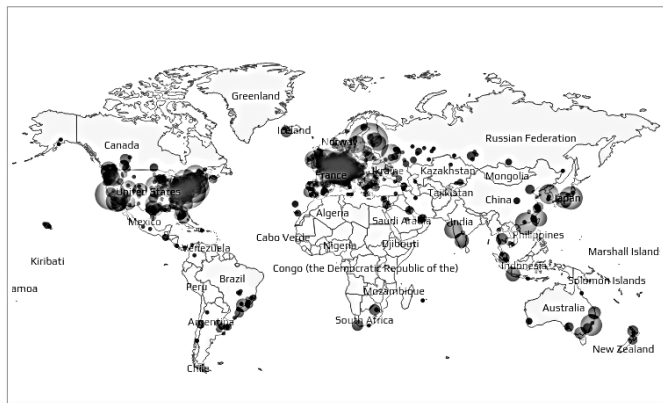


Figura 1.2: Distribución de los nodos por país

1.2 TRANSACCIONES EN BITCOIN

Una transacción se produce cuando un individuo, el propietario, le envía una cantidad de monedas electrónicas a otro, el beneficiario. Cada una de estas transacciones conlleva una serie de operaciones. En concreto, cada transacción contiene la clave pública del beneficiario, un hash y la firma del propietario. De esta manera, una moneda electrónica se define en este contexto como una cadena de firmas digitales.

Por tanto, cada vez que se realiza una transacción se genera un hash con la clave pública del beneficiario y la transacción previa, después con este hash y la clave privada del propietario se firma la transacción en curso; por último, se incluye la clave pública del beneficiario y con todo esto ya se tendría una transacción. Con todas estas operaciones se puede verificar cada transacción de forma sencilla. Para seguir de forma gráfica el proceso, se incluye el siguiente diagrama.

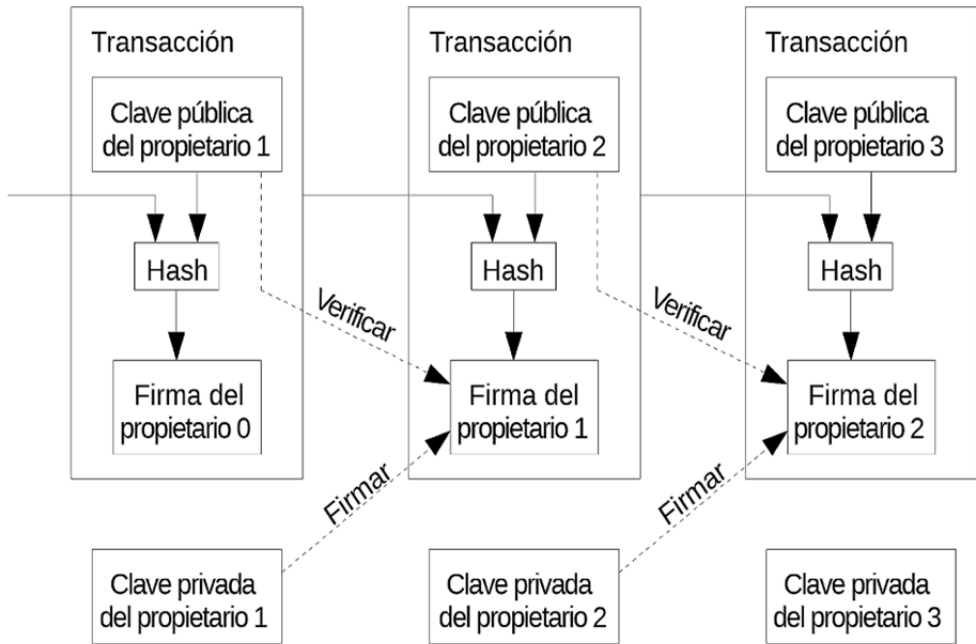


Figura 1.3: Diagrama de transacciones

Esta forma de trabajar no resuelve el problema antes mencionado, y no hay forma de verificar que uno de los propietarios no haya gastado dos veces la misma moneda. De esto se encarga la autoridad central de confianza, o casa de la moneda, que va comprobando cada una de esas transacciones para que eso no sea un problema. Con esta forma de trabajar, cada moneda debe regresar a la casa de la moneda para que esta distribuya una nueva, ya que solamente estas monedas son las que estarían libres de cualquier sospecha del doble gasto. El problema de esta solución centralizada es el que se ha comentado varias veces, todo depende de este sistema centralizado, como en un banco.

Para solucionar esto, Bitcoin propone que las transacciones sean públicas. De esta forma se puede tener un sistema en el que cualquiera pueda tener un historial de todas las transacciones y, al ser muchos, que el historial real sea aquel en el que la mayoría de los participantes estén de acuerdo. Así, el beneficiario tendría la certeza de que los propietarios previos no han firmado transacciones anteriores a la suya. En este sistema, la última transacción es la que cuenta y no se fija en el intento o no de dobles gastos posteriores.