Efac: sistema de información para el sistema educativo apoyado en blockchain

Abstract

1. Introducción

1.1. Contexto

La estructura de datos blockchain despertó la curiosidad de técnicos y académicos desde que vió la luz a finales de 2008 en foros de criptografía. En este año la persona o personas detrás del pseudónimo Satoshi Nakamoto publicaron en una lista de mail de criptografía la primera arquitectura de una red peer-to-peer de dinero electrónico(Nakamoto 2008), Bitcoin. Estaba basada en distintos conceptos entre los que encontramos blockchain, prueba de trabajo (PoW), merkle tree, minado, transacciones regulares y coinbase, Bitcoin Protocol, carteras, Bitcoin Script y criptografía asimétrica.

Este sistema de e-cash soluciona el problema de los generales bizantinos y permite, por primera vez en la historia, transferir propiedad digital a otro usuario de Internet, de manera que solo el propietario pueda hacer la transferencia, únicamente el destinatario pueda recibirla, todo el mundo pueda validar la transferencia y esta sea reconocida por todos los participantes, todo ello realizado de manera totalmente distribuida(Pérez Solà and Herrera Joancomartí 2014).

Los primeros años fue testado por expertos en ciberseguridad buscando debilidades; más adelante, académicos y emprendedores han buscado aplicaciones a una tecnología que permite prescindir de una entidad central de confianza entre las partes de una transacción o contrato.

Todo lo que rodea al ecosistema bitcoin se ha desarrollado desde el primer momento de forma pública, abierta a quien quiera participar en ella siguiendo el signo de los tiempos, el open-source.

Es importante saber que el ecosistema bitcoin-blockchain ha ido cambiando, conocer el pasado puede ser útil para saber hacia dónde irá el desarrollo de los próximos años. Contando con la arquitectura de Satoshi Nakamoto y su participación en el inicio del proyecto, distintos desarrolladores se fueron sumando y haciendo más grande la

comunidad. Una vez el proyecto estaba corriendo con normalidad en varios nodos, Satoshi dejó de participar en los foros y la comunidad siguió con el desarrollo. Las bases estaban claras, descentralización y prescindir de una tercera parte de confianza. Al cabo de los años, una vez probada la eficacia de bitcoin, comenzaron a surgir otras criptomonedas que presentaban pocas diferencias con Bitcoin: es el caso de Litecoin o la graciosa Dogecoin, en honor a Doge, el perro de internet. Estas monedas no aportaban demasiado a nivel técnico pero da una idea de la filosofía que tenía la gente que desarrollaba el ecosistema en ese momento, replicando Bitcoin o simplemente montando proyectos de broma.

La primera gran innovación vino con Ethereum, una blockchain que utilizaba un lenguaje Turing completo frente al lenguaje Script de Bitcoin, que no era completo. Si bien Bitcoin había planteado este lenguaje de manera intencionada para evitar bucles infinitos que invalidarían el sistema, Ethereum introduce el concepto de *gas* con el que evita que una ejecución gaste más poder de cálculo del esperado. Mientras Bitcoin solo tiene un pequeño número de operaciones permitidas, Ethereum siendo Turing completo y controlando el gasto de computación permite crear programas con más funcionalidad, los llamados *smart contracts*, que una vez subido a los nodos ejecutan el código si reciben el gas necesario.

También comenzaban a surgir distintas alternativas a las blockchain públicas, las blockchain privadas o permisionadas que solo utilizan parte de los componentes de Bitcoin y por tanto ofrecen características distintas. Las principales diferencias respecto a las blockchain públicas son un número mayor de transacciones por segundo a cambio de la pérdida de descentralización, transparencia y otras características de las blockchain públicas.

Por otro lado, la diversidad de opiniones sobre hacia dónde debería encaminarse la criptomoneda Bitcoin provocó lo que algunos llamaron “hash wars”: distintas bifurcaciones de la cadena principal llamadas *forks* en las que grupos de desarrolladores y mineros descontentos con las capacidades que ofrecía Bitcoin planteaban su alternativa. Mientras las personas que preferían mantener el protocolo como estaba seguían utilizándolo, quienes querían cambiar acordaban actualizar los nodos de tal forma que a partir de cierto bloque empezaban a utilizar un protocolo con diferentes características: mayor velocidad de minado del bloque, mayor número de transacciones por bloque, etc.

A lo largo de los años la blockchain de Bitcoin, por ser la original, se ha establecido como buque insignia de las blockchain, limitada a su caso de uso que es el de criptomoneda. Para el resto de casos de uso, Ethereum se ha situado como referente debido al uso de *smart contracts* que permiten bastante versatilidad. Por otro lado y con menor importancia, se encuentran infinidad de proyectos de blockchains públicas con diferentes variaciones frente a las características de Bitcoin o Ethereum que se han venido a agrupar como *altcoins* (alternative coins) y también otro grupo en el que se ubicarían tanto las blockchain privadas o permisionadas como una tecnología que no puede ser considerada blockchain llamada Distributed Ledger Technology (DLT), que en algunas empresas se consideran como alternativa a las bases de datos centralizadas y pueden tener cierto interés a la hora de crear consorcios de empresas para algún fin.

Actualmente están en fase de desarrollo dos conceptos investigados en los últimos años. Se trata de tecnologías de layer-2, por encima de la layer-1 que sería la red de Bitcoin o de cualquier otra blockchain. Por un lado se encuentra el concepto de *Sidechain* o Cadena lateral, una blockchain que se pega o adhiere con distintos mecanismos a la blockchain principal con la idea de ofrecer distintas características, las mismas que ofrecían las altcoins (mayores transacciones por minuto, etc.) pero mientras las altcoins generaban blockchains independientes las sidechain dependen de la blockchain principal.

En este Proyecto de Fin de Grado (PFG) se investigan todas las tecnologías mencionadas en este apartado Contexto y tras este estudio se desarrollan *smart contracts* en Ethereum por ser la blockchain que ofrece las características más apropiadas con el objetivo de resolver el problema que se plantea en la siguiente sección Descripción del problema.

En el ámbito social, el signo de los tiempos venía marcado por la colaboración frente a la competencia, las estructuras hosrizontales frente a las jerarquías, haciendo partícipes de las decisiones a todas las personas de un grupo. En resumen, democratización. Blockchain no solo ha traído innovación tecnológica sino que supone la herramienta para este cambio de filosofía en el mundo de la informática, y de aquí puede pasar a otros ámbitos de la sociedad que hasta el momento mantenían estructuras jerárquicas.

1.2. Descripción del problema

El sistema educativo en España y quizá en otros países, desde la escuela primaria hasta el graduado universitario, estructura sus clases de tal forma que el conocimiento fluye desde la profesor/a al alumna/o[1], de arriba abajo, o como se diría en informática, top-down.

En la mayor parte de los casos, personas con conocimiento en un tema: 1. crean contenidos que enseñar a personas sin ese conocimiento; 2. les imparten lecciones de forma oral, en ocasiones acompañadas por apuntes, otras sin ellos para que se mantengan atentos en clase; 3. evalúan los conocimientos adquiridos.

Poniendo el foco en este punto 2, se pueden encontrar algunas ventajas a este modelo tradicional como la monitorización que puede llevar el profesorado para corregir la falta de atención en alumnos que todavía no tienen un hábito de estudio. Sin embargo, este sistema mata la iniciativa del alumnado al relevarles al puesto de observadores, oyentes, como mucho con alguna participación en clase pero siempre controlada. Los alumnos tendrían que ser los protagonistas de la clase.

Por economizar, los grupos de personas que se juntan en las aulas de instituto suelen ser de entre 15 y 35 alumnos, algo que si bien proporciona sentimiento de pertenencia a un grupo y otros beneficios de cohesión social que al no tener estudios de Educación desconozco, suponen grupos demasiado grandes como para que los alumnos se sientan protagonistas.

Grupos más variables se encuentran en los grados universitarios donde hay clases desde los 5 alumnos hasta más de 100. Esto se debe a que se distribuyen las clases en función del tema que se imparte, por lo que algunos temas surgen más interés que otros o son objetivamente más necesarios y crean una aglomeración de alumnos. Estas aglomeraciones no facilitan la participación de todas las personas de la clase. Por otro lado, el criterio económico ha de tenerse en cuenta, si se contratasen demasiados profesores universitarios la viabilidad financiera de la universidad pública estaría en riesgo.

Es necesario buscar una nueva forma de enseñar que permita al alumnado ser independiente. Es necesario fomentar la iniciativa. Puede ser útil que los alumnos se junten en grupos más pequeños y autogestionados.

En primer lugar, es imprescindible plantear soluciones a estos problemas. Una vez hecho esto, el siguiente paso es investigar cómo la tecnología blockchain, pensada

[1] En adelante se usará el masculino por economía del lenguaje aunque no sea lo más correcto, la RAE debe proponer una solución más justa

para democratizar procesos, puede servir de herramienta en este caso. Por último, es útil idear un sistema informático que soporte las soluciones propuestas.

1.3. Objetivo principal y específicos

El objetivo principal de este proyecto es investigar la tecnología blockchain para aportar una solución estructural al sistema educativo de manera que sea motivador, se potencie la iniciativa individual, se ponga en valor la aportación al grupo y se fomente el espíritu crítico.

Con ese fin, se proponen los siguientes objetivos específicos que podemos agrupar de la siguiente forma:

- Investigación tecnología blockchain:
  - Desarrollar el concepto de blockchain
  - Conocer Bitcoin como blockchain original y base de las demás blockchain
  - Explicar los tipos de transacciones y sus características como base de datos.
  - Diferenciar entre transacciones en base de datos relacional y transacciones en blockchain
  - Introducir Ethereum y el concepto de Smart Contract
  - Evaluar la utilidad de los token
  - Comparar los distintos mecanismos de consenso, entre los que se incluyen Proof-of-Work (PoW), Proof-of-Stake (PoS), etc.
  - Redes públicas vs redes permisionadas o privadas
  - Revisar las características comunes a toda blockchain
  - Características diferenciadoras entre blockchains
  - Definir la utilidad de esta tecnología
  - Especificar la blockchain que mejor se adapta a distintos casos de uso
- Análisis educación pública
  - Histórico de la educación
  - Identificar aspectos a mejorar
  - Proponer soluciones
- Idear un sistema de información basado en blockchain
- Obtener conclusiones

1.4. Resumen de la memoria

2. Bases teóricas

2.1. Blockchain

Blockchain o cadena de bloques es un diario distribuido, público y completamente replicado de transacciones. Atendiendo a su finalidad de almacenamiento de datos, también se considera una base de datos, aunque su estructura es más parecida a la de un diario, un registro en el que se guardan todas las transacciones ocurridas desde la transacción inicial.

Este registro o diario se almacena replicado en diferentes nodos que se comunican en forma de coreografía, es decir, ningún nodo ejerce de autoridad central sino que cualquier nodo puede comunicarse con cualquier otro. Todos siguen el mismo protocolo y sus acciones las validan los nodos a los que están conectados. Por tanto puede asegurarse que ninguno controla la red. Los cambios en el protocolo han de realizarse de manera consensuada ya que es necesario el 51% del poder de computación para, tras hacer un cambio, mantener la cadena más larga en número de bloques, que será considerada válida frente a otras.

Blockchain fundamenta su operativa en estructurar los datos en base a criptografía. Podemos describir esta operativa de la siguiente forma. Una transacción candidata a formar parte del diario-blockchain debe quedar incluida en el siguiente bloque de transacciones que se añada a la cadena. El nuevo bloque incluye, además de las transacciones, unas cabeceras o headers entre las que se encuentra una referencia al bloque anterior o último bloque integrado en la cadena.

Esta referencia, llamada H() en la Figura 1, sirve para generar una línea temporal que evite el problema del doble gasto así como para verificar su inclusión en la cadena.

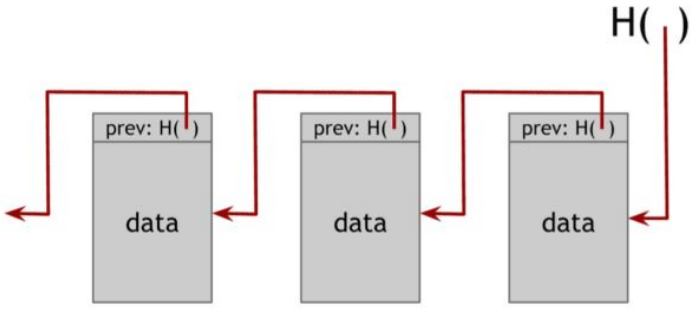


Figura 1. Referencia hash al bloque anterior. (Bitcoin and Cryptocurrency Technologies)

Con esta representación, se podría pensar en blockchain como un sistema de transiciones (transition system) en el que cada vez que se añade un bloque, se pasa al siguiente estado. Las transiciones entre estados serían las transacciones y el estado determinaría qué outputs están sin gastar en cada momento y quién está en posesión de la criptomoneda.

Se llama nodo minero a aquel tipo de nodo que añade bloques a la cadena. La forma en que un minero forma un bloque es juntando las transacciones que considere, de entre las que están esperando en el pool de transacciones. Una vez el minero ha formado el bloque, este bloque debe convertirse en el siguiente de la cadena. Sin embargo, podría ocurrir que existan dos bloques candidatos a continuar la cadena. Para evitar este problema la red considerará válida la cadena más larga, siendo habitual en estos casos que se pueda discernir la cadena ganadora después de dos o tres bloques. Una explicación más detallada se puede encontrar en Minería bitcoin.

Por tanto, una transacción se considera escrita en firme en el diario-blockchain cuando resulta evidente que pertenece a la cadena más larga.

Se puede añadir un bloque cuando se encuentra un número ("nonce") que cumple una regla: el hash del nuevo bloque (que tiene cabecera, cuerpo de transacciones y este número aleatorio nonce) debe generar un número que comience por una cantidad prefijada de ceros que va aumentando con el tiempo para que sea necesaria una mayor capacidad de cómputo cada vez. Se explicará con más detenimiento en la sección Proof-of-Work (PoW).

En el ámbito de blockchain aparecen tres grupos de interesados: los mineros, soportan la red con recursos informáticos almacenando la cadena y confirmando las transacciones; los desarrolladores, crean la blockchain en función del caso de uso, las

herramientas para interactuar con ella y hacen evolucionar el sistema; los usuarios, intercambian los activos propios de cada blockchain (tokens).

Más adelante se verá cómo blockchain asegura algunas características propias de una base de datos o un registro de transacciones tales como la integridad, consistencia, disponibilidad, seguridad y confidencialidad.

Debido a la existencia de varias versiones de blockchain creadas para dar soporte a distintas criptomonedas, al fin y al cabo el caso de uso más común de blockchain, se va a utilizar como objeto de estudio principal la blockchain original de Bitcoin implementada en bitcoin.org y descrita en distintos artículos, como el "Bitcoin Developer Reference" (Krzysztof Okupski 2016).

También se verán conceptos introducidos con posterioridad a Bitcoin como los Smart Contracts de Ethereum, las blockchain-DLT privadas o permisionadas y las tecnologías de layer-2 como Sidechain o Lightning Network.

2.2. Bitcoin

Bitcoin es el primer caso de uso de la tecnología blockchain. Dicho de otra forma, blockchain fue ideado para soportar Bitcoin.

Bitcoin es:

- un sistema informático de intercambio de valor basado en redes P2P
- una criptomoneda
- la primera solución al problema del doble gasto y al resto de problemas existentes hasta el momento, inherentes a la naturaleza de los archivos digitales
- un token único o no duplicable

Se llaman criptomonedas a los sistemas digitales, descentralizados y basados en criptografía de intercambio de valor pecuniario. Este es el caso de uso más extendido de la tecnología blockchain, aunque puede tener otros muchos usos al ser un sistema que permite prescindir de una tercera parte confiable. Algunos de ellos son el voto distribuido, la identidad digital, el intercambio de electricidad generada en hogares con paneles solares y un largo etcétera.

La mayor parte de los componentes del protocolo Bitcoin (en mayúscula es el protocolo, en minúscula la criptomoneda o token) ya existían por separado. Bitcoin combina la tecnología P2P que se usa por ejemplo en BitTorrent con la criptografía de

clave pública. Esta combinación junto a la estructura de incentivos de tokens, fomenta la utilización y participación en este protocolo.

La idea surge de Satoshi Nakamoto (una persona o grupo) a través de una publicación en noviembre de 2008, implementando un ejemplo en nodos voluntarios y participando a nivel técnico en las primeras fases de la actual criptomoneda.

Blockchain es solo un componente que se ubica dentro del ecosistema Bitcoin, el cual incluye:

1. Bitcoin Protocol: red descentralizada P2P.
2. Blockchain: registro o también, puesto que hablamos de una moneda, libro de cuentas público.
3. Sistema descentralizado de creación (minado) de la moneda.
4. Script: lenguaje no Turing completo en el que se basan los scripts de las transacciones de Bitcoin

En este PFG se explica la operativa de blockchain, pero también es necesario conocer unas pinceladas del resto del sistema de pagos de Bitcoin para que en conjunto tenga sentido. Por tanto, se explicará brevemente la red descentralizada y se explicará el sistema de minado y la verificación, entre otras cosas. No obstante, el foco se pone en las transacciones en sí mismas y en cómo se van añadiendo al diario que es blockchain.

Se va a estudiar en primer lugar para qué sirve esta tecnología desde un punto de vista funcional y después se hará una extensa explicación técnica.

2.2.1. Necesidad cubierta por Bitcoin

Pongamos una moneda convencional. Metálica, con inscripciones y soportada por una entidad central la cual define qué características determinan si una moneda es válida o no.

Intentemos trasladar esta idea al mundo de la informática. En una red centralizada existe una autoridad que determina si la moneda ha cambiado de propietario, lo cual trae consigo ciertas garantías pero necesitas confiar en esa autoridad central por lo que te vuelves dependiente. Es una buena aproximación y es la que se utiliza con el dinero digital en la mayor parte de las economías actualmente. Sin embargo, en la

práctica estos sistemas presentan bastantes deficiencias especialmente en transacciones internacionales, tan importantes hoy en día.

En una red descentralizada P2P distintos usuarios/nodos pueden intercambiar archivos directamente, sin una entidad central, como si fuese de mano en mano. Estos archivos pueden tener características específicas para identificar si son válidos, pero se pueden reproducir luego no se pueden utilizar como moneda. La solución propuesta por Bitcoin será no utilizar archivos, sino token asociados a cuentas/billeteras protegidas con criptografía asimétrica.

Las transacciones virtuales en euros realizadas a través de bancos europeos utilizan un sistema centralizado llamado SEPA en el que se compensan los saldos de las partes de la transacción. Un sistema parecido llamado SWIFT se utiliza a nivel internacional. Estos organismos centrales son necesarios para conseguir transacciones seguras, íntegras y sin interrupciones.

Con el objetivo de crear una moneda digital descentralizada surge la necesidad de un sistema en el que existan:

- garantías de que no se pierde el dinero
- seguridad en las transacciones
- incentivos para quienes soportan la red

2.2.2. Bitcoin a alto nivel

Se puede entender de una forma sencilla el funcionamiento de una transacción a través de la siguiente imagen:

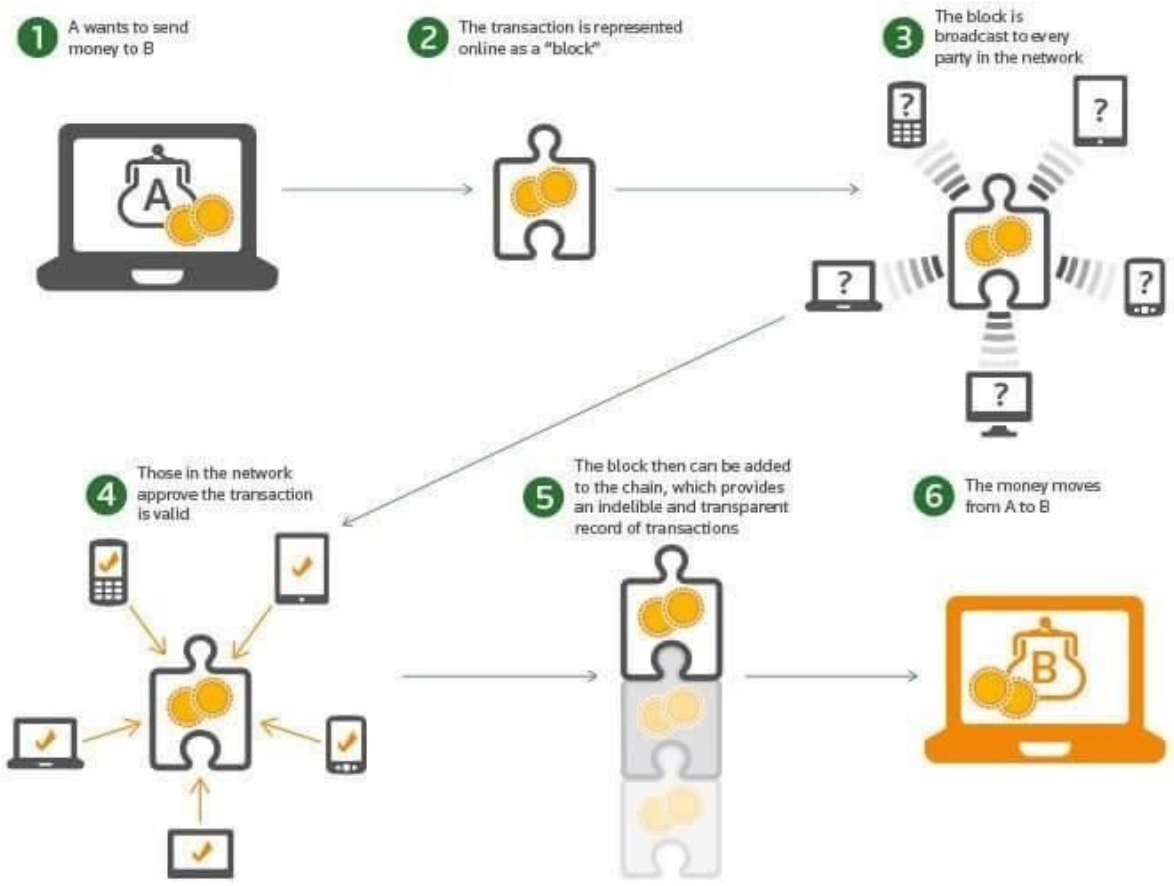


Imagen. Bitcoin, high-level explained (www.iotforall.com/blockchain-explained/)

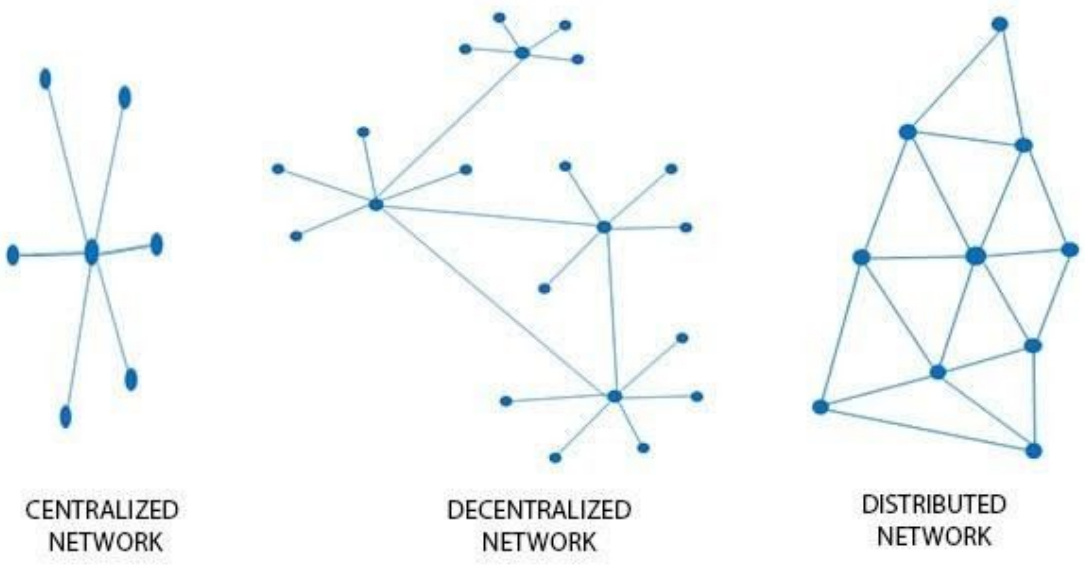
En la imagen, la transacción u orden de transferir dinero de A a B se añade a un bloque el cual busca ser validado por los miembros de la red en un proceso llamado minado. Una vez queda validada la transacción, el bloque se añade a la cadena almacenada en todos los nodos de la red haciendo que sea casi imposible de modificar, ya que está completamente replicada. Ya se puede decir que el dinero ha pasado de A a B.

El dinero no existe de forma física, se trata de un número en un diario de transacciones que guarda de manera pública todas las que ha habido desde el momento inicial, las que estaban incluidas en el primer bloque o bloque génesis.

Para que estas operaciones puedan ser ejecutadas es necesario un sistema que soporte toda la operativa. Se podrían dividir los elementos intervinientes en el protocolo en dos partes: la externo a las transacciones por un lado incluyendo la red P2P y la minería; las transacciones de blockchain por otro, junto con todo lo que les da soporte como las cuentas y carteras.

2.2.3. Red P2P

El protocolo de bitcoin utiliza una red P2P, un modelo distribuido en el cual cada nodo se comunica con los que tiene alrededor para intercambiar información. La siguiente imagen sirve para repasar el concepto de modelo distribuido frente a otros modelos como el basado en un servidor central o el descentralizado en varios servidores:



Las redes peer-to-peer se basan en el tercer modelo por lo que no existe un nodo que ejerza una autoridad sobre el resto. Hasta ahora existían modelos distribuidos de bases de datos pero no resolvían los problemas de confianza hasta que apareció blockchain.

El protocolo de red Bitcoin permite que los nodos completos (peers) mantengan de forma colaborativa una red punto a punto para el intercambio de bloques y transacciones. Los nodos completos (*full nodes*) descargan y verifican cada bloque y transacción antes de transmitirlos a otros nodos.

Los nodos de archivo (*archival nodes*) son nodos completos que almacenan toda la cadena de bloques y pueden servir como bloques históricos a otros nodos. Los nodos podados (*pruning nodes*) son nodos completos que no almacenan toda la cadena de bloques. Por último, los clientes SPV (*Simplified Payment Verification*) usan el protocolo de red Bitcoin para conectarse a nodos completos y confían en ellos para descargar solo las cabeceras de los bloques gracias a los cuales alcanzan un nivel de seguridad aceptable.

Las reglas consensuadas por la comunidad de desarrolladores de bitcoin no cubren las redes, por lo que los programas de Bitcoin pueden usar redes y protocolos alternativos, como redes de transmisión de bloque de alta velocidad utilizadas por algunos mineros y los servidores de información de transacciones dedicados que utilizan algunas billeteras (wallets) que proporcionan seguridad de nivel SPV.

En esta tabla que se encuentra en el artículo Cryptocurrency Networks: A New P2P Paradigm (Delgado-Segura et al. 2018, 1-16) se muestran las características de los diferentes nodos:

Node	Blockchain	Functionality	Connectivity	Protocol
Full client	F/P	V/R, W	L/NL	B
SPV client	H	W	NL	B
Non-SPV light client	—	W	—	S/SP
Solo miner	F/P	V/R, W, M	L/NL	B
Pool mining server	F/P	V/R, W, M	L/NL	B/S/SP
Pool mining client	—	W, M	—	S/SP

Tabla. (Delgado-Segura et al. 2018, 1-16)

La tabla presenta las características en función de 4 factores, en orden:

- el conocimiento de la blockchain, más transacciones guardadas implica más conocimiento, y pueden ser F (Full node), P (Pruning node) o H (Headings only)

- la funcionalidad que ofrece: W (Wallet o cartera de direcciones), M (Miner o minero) o V/R (Validation/Relaying o validación/transmisión)
- la conectividad a otros nodos, siendo L (Listening) y/o NL (Non Listening)
- el protocolo soportado, ya sea B (Bitcoin), S (Stratum, un protocolo de minería en grupo) o SP (Specific Protocols, otros protocolos)

En cuanto a la seguridad en la red, al ser P2P no es demasiado efectivo un ataque DoS (Denial of Service). Para provocar una inundación de transacciones, se podría pensar en un DoS centrado en un nodo concreto, haciéndole llegar transacciones inválidas. Sin embargo, éstas deben estar correctamente firmadas para probar que están autorizadas a enviar esos bitcoin y si no lo están son rechazadas y no se transmiten por la red. Además, las transacciones sin *fee* (comisión que se paga al minero) suelen ser rechazadas por defecto para evitar que sean transmitidas por toda la red indefinidamente sin que ningún minero quiera incluirla en un bloque. Por último, las transacciones que incluyen inputs más jóvenes, provenientes de transacciones más actuales, tienen unas fees mayores por lo que un ataque que trate de inundar la red usando continuamente el mismo dinero será cada vez más caro.

En cuanto a inundar la red de bloques no es aplicable ya que solo se transmiten bloques con una prueba de trabajo válida que, como se verá en la sección Proof-of-Work (PoW), es difícil de crear pero fácil de verificar.

Lo que sí se podría es crear una inundación de mensajes de red, los mensajes que utilizan los nodos para comunicarse entre sí. Estos mensajes no tienen ningún coste asociado. Para evitar esto, en Bitcoin existe un protocolo para que los nodos puedan ser baneados durante un día en función de su puntuación de comportamiento.

2.2.4. Minería bitcoin

Se llama minería al proceso de añadir un nuevo bloque de transacciones a la blockchain. Recordando lo que se veía en la sección Blockchain, las transacciones se incluyen en bloques y éstos se adhieren a la cadena incluyendo un hash del bloque anterior y la Proof-of-Work (PoW), de tal forma que con cada bloque se genera un sellado de tiempo o *timestamp*, el cual permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

La forma que tiene un bloque es:

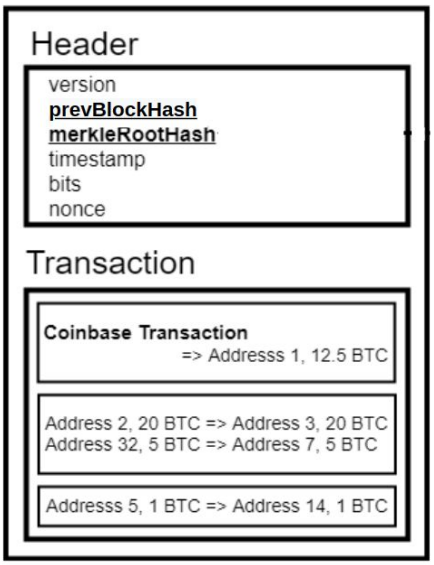


Figura. Bloque Bitcoin

En esta figura se divide el bloque en dos partes. Por un lado, las cabeceras o *headers* incluyen una ristra de 80 bytes de longitud, y está compuesta por el número de versión de Bitcoin de 4 bytes de longitud, el hash de las cabeceras del bloque anterior (prevBlockHash) de 32 bytes, el hash del elemento raíz del árbol Merkle de transacciones (merkleRootHash) de 32 bytes, la marca de tiempo del bloque de 4 bytes de longitud, y por último dos cabeceras utilizadas por los mineros para realizar la prueba de trabajo (PoW): el objetivo de dificultad del bloque (bits) de 4 bytes, y el nonce de 4 bytes de longitud utilizado por los mineros. Por otro lado, en el cuerpo del bloque está un entero con el número de transacciones y un vector con las transacciones que el minero creador del bloque decide incluir además de la transacción Coinbase.

La tarea de los mineros es, por tanto, añadir un nuevo bloque en la blockchain. Quedaría de la siguiente forma:

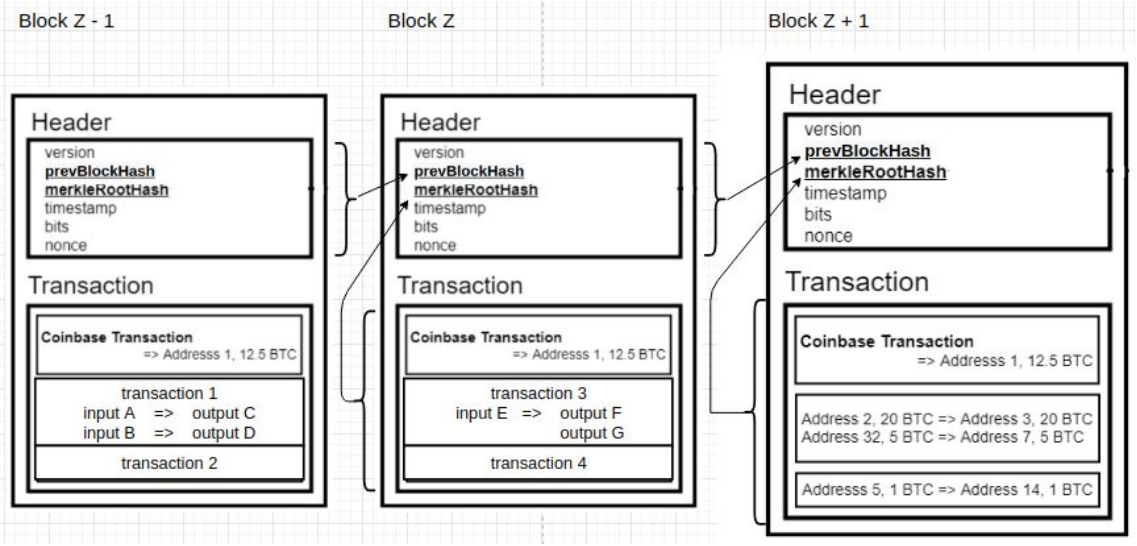


Figura. Nuevo bloque añadido

En la figura, Block Z sería el último añadido a la cadena y Block Z+1 sería el propuesto por un minero para ser el siguiente, lo que se llama en esta tesis bloque *aspirante*. El proceso de minado se basa en los siguientes pasos:

1. Tanto las transacciones como los bloques válidos se transmiten por la red Bitcoin entre todos los nodos.
2. Cuando un minero recibe las transacciones, las guarda en una memoria llamada *mempool*. De entre estas transacciones de la mempool, elige las que más le interesen, normalmente las que pagan mayor comisión. Comprueba que sean transacciones válidas y las agrega a su bloque aspirante junto a la transacción Coinbase.
3. Añade al aspirante las cabeceras vistas con anterioridad y comienza a realizar la prueba de trabajo para obtener un hash inferior al valor objetivo *bits*. El hash de la PoW es el resultante de variar el campo nonce manteniendo el resto de headers *ceteris paribus*, como se explica en Proof-of-Work (PoW).
4. Si es el primero en obtener la PoW, transmite el bloque a la red y comienza a trabajar en el siguiente bloque. En caso contrario, recibe el nuevo bloque de alguno de sus peers o nodos adyacentes, comprueba su validez, devuelve las transacciones no incluidas en el bloque ganador a la mempool y comienza la nueva iteración.

La PoW en Bitcoin está diseñada para que de media tarde en minarse 10 minutos. Las más actuales pueden consultarse en https://blockchain.info/es/blocks. Por ejemplo, a 24/05/2020 se tiene que las primeras son:

Bloques

Altura	Hash	Minado	Minero	Tamaño
631556	0..7f984ddec1990832da4781a36aacc1ec02d8c7ae1bdd0	5 minutos	Poolin	1.428.610 bytes
631555	0..110575a43c7538072c5e86bf3f1befb1fbfdc6fe25ac17	9 minutos	BTC.com	1.288.211 bytes
631554	0..c261be9a81f084929f599d02f760d0e018416e4c538f1	54 minutos	Poolin	1.360.073 bytes
631553	0..a0adcf0b4a4c7d3fdd060f0fa2ac4af5efeee2ca2d741	1 hora	F2Pool	1.351.003 bytes
631552	0..1079f3f8a7efc1ea9330fdd12ab5c2700098e8463a7f5d	2 horas	F2Pool	1.358.048 bytes
631551	0..554e5cef711a9b9f1e6750bac57bd7540324b3f058a5a	2 horas	Poolin	1.301.922 bytes
631550	0..3a001e7d0092b37bef708f17a897655d8dd6e6ea8a7f3	2 horas	Unknown	1.244.053 bytes
631549	0..c8f746cbbd3bda55ce91590f4cbacbc6501ca2cc09980	3 horas	BTC.TOP	1.408.192 bytes
631548	0..9b9bfcd3a6838708f685bd05c8113da73e1f91025ab5	3 horas	F2Pool	1.297.842 bytes
631547	0..e3ec9185c7d32ca78b36b7260d03f320dba99a0112326	3 horas	AntPool	1.397.463 bytes
631546	0..7a09b7e9b2358269cb253a6725614ae614e89832a6bdf	3 horas	ViaBTC	1.145.102 bytes
631545	0..6a0751820aad5a467a8ca4c4211466c978cdc00c705f5	3 horas	AntPool	1.423.352 bytes
631544	0..d45fbd6798400c5efe03325a17f75a0fd15c8a78a77a7	3 horas	Unknown	1.228.192 bytes
631543	0..868d580f79b59651c6fc83a5ad0f40ee53cdebf0ec0b5	3 horas	F2Pool	1.105.964 bytes
631542	0..5ee29c6cee15ce569eeaf86fda2917e1bf5afe2b284f6	4 horas	F2Pool	1.440.025 bytes
631541	0..43eaf36aded804fb5549567883f8ce145de51d7e1ccda	4 horas	ViaBTC	1.320.099 bytes
631540	0..7fd22049f75317e9994cf26d21f7424d33fa0052eeb8d	4 horas	SlushPool	1.354.127 bytes
631539	0..5807ffdd696b47e85acf654ce904a08ae94e1a922d76f	4 horas	Unknown	1.371.346 bytes
631538	0..109165b0a9555e9cc79a54e1322ddd2adf93dd38447d0d	5 horas	AntPool	1.258.667 bytes

Imagen. Últimos bloques minados

De aquí se puede sacar información como el bloque de la cadena por el que se llegan actualmente, el tamaño de cada bloque o el minero que ha resuelto la prueba de trabajo que ha permitido añadir el bloque a la cadena principal.

Puede darse el caso de que dos mineros consigan resolver la PoW aproximadamente al mismo tiempo y propaguen por la red dos bloques aspirantes a liderar la cadena más larga como se ve en la siguiente figura:

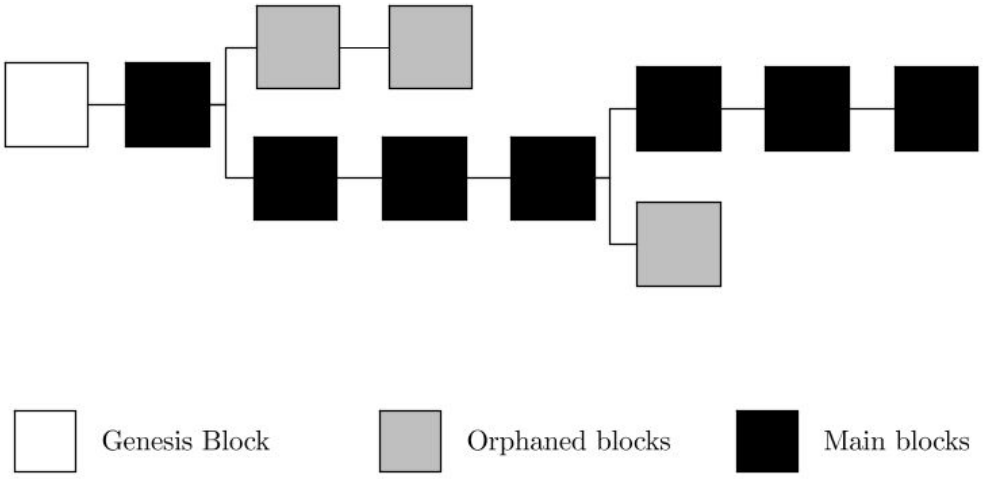


Figura. Cadenas alternativas (Krzysztof Okupski 2016)

Se llama *block height* o altura del bloque a la cantidad de bloques que había previamente en la cadena. Partiendo del bloque inicial o Génesis, con una altura de 0, se puede ver cómo el tercer bloque (altura 2) de la cadena tiene dos alternativas.

Parte de los mineros elegirán el bloque de arriba para continuar la cadena, el resto elegirá el de abajo. Podría ocurrir que, de nuevo, los dos grupos de mineros consigan minar un nuevo bloque al mismo tiempo pero eventualmente una cadena será más larga que la otra. En ese momento los mineros de la cadena más corta se pasarán a la más larga ya que la red no va a dar soporte a los bloques que han minado: no están en la cadena más larga por lo que las transacciones en esos bloques dejan de ser válidas.

Cada vez que se crean cadenas alternativas se produce un *fork*, una división. Puede darse porque se minen a la vez dos bloques con misma altura como se acaba de ver o por un cambio en el protocolo, lo que en cualquier software se llamaría update o actualización.

Un fork provocado por la primera razón no se suele mantener en el tiempo, pero los cambios en el protocolo son en cierta medida frecuentes. Puesto que el software de Bitcoin es libre y depende por completo de la comunidad, los debates son continuos y cada cierto tiempo las diferencias de opinión desembocan en un fork en el que se implementan los cambios que se consideran mejores. Mientras esta cadena paralela sea respaldada por un número suficiente de mineros, la cadena alternativa puede coexistir con la original.

Alguno de los fork hasta ahora han sido:

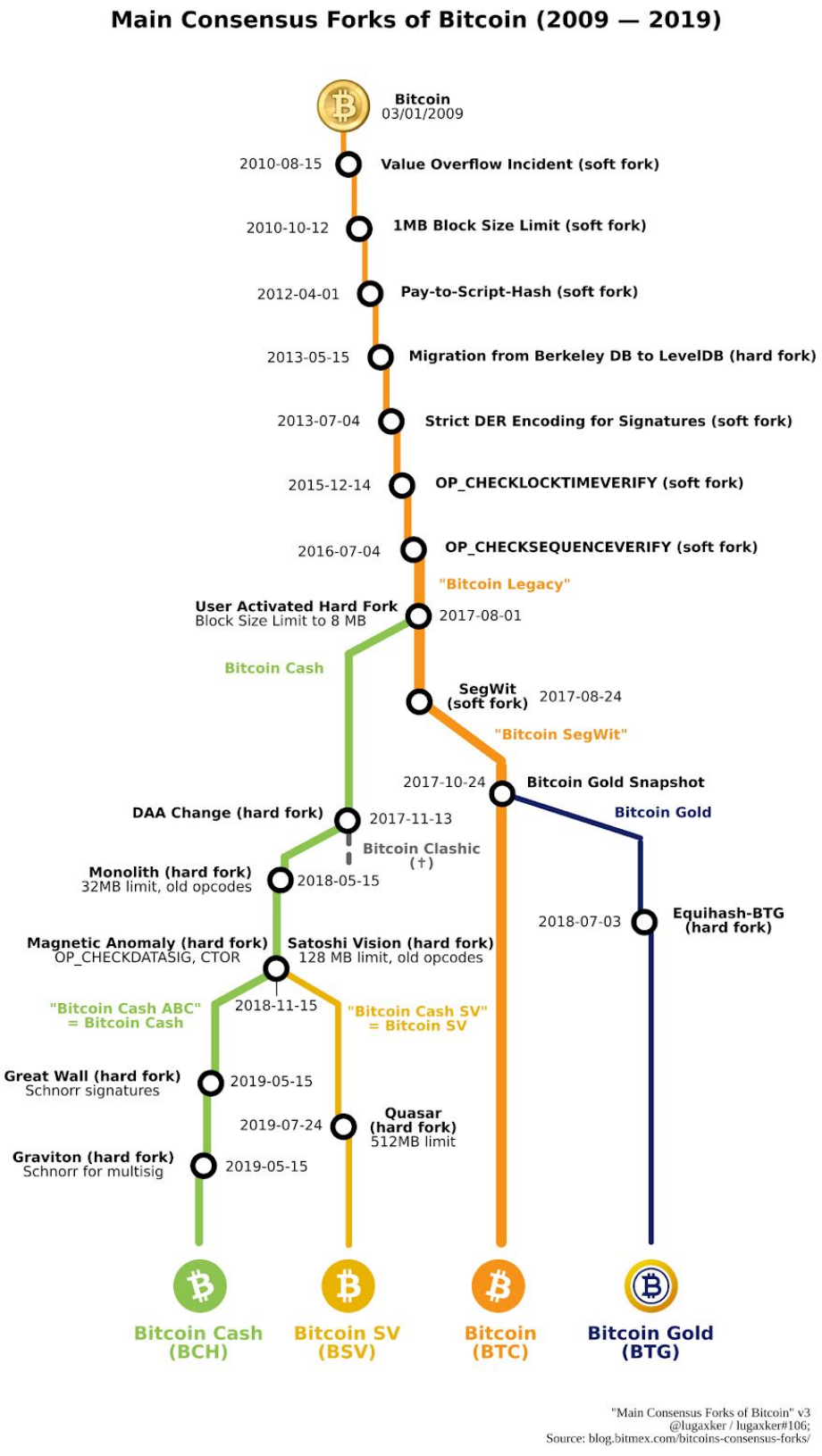


Figura. Bitcoin forks (A map of the major "Bitcoin" forks. : CryptoCurrency)

En la figura se aprecian dos tipos de fork. Se llama *soft fork* cuando el cambio en el protocolo tiene retrocompatibilidad (backward compatibility) y hard fork cuando no lo tiene, provocando así una bifurcación entre quienes implementan el cambio y quienes no.

La adopción de SegWit y por otro lado Bitcoin Cash son los mejores ejemplos de soft fork y hard fork, respectivamente. Era necesario aumentar la velocidad de las transacciones de bitcoin y puesto que mantener los 10 minutos en promedio de minado estaban fuera de toda discusión, la idea era aumentar el número de transacciones que se podían incluir en cada bloque. Para ello se propusieron e implementaron dos soluciones.

La primera de ellas, Segregated Witness (SegWit) o testigo segregado, proponía liberar espacio de cada bloque para que pudiera utilizarse en incluir un mayor número de transacciones. Esto se logró eliminando del bloque la clave pública y la firma asociada a cada transacción y enviándolas a través de un canal de mensajería diferente. Dado que la clave pública y la firma ocupan alrededor del 60% del tamaño total de la transacción, al enviarlas por separado era posible casi duplicar el número de transacciones en cada bloque. Este cambio en el protocolo se aplicó de manera que permitía a la blockchain tener bloques creados de la antigua forma y también de la nueva, por lo que era retrocompatible y consecuentemente más permisivo. Es el soft fork más famoso. Antes de SegWit, había un *tamaño máximo* de bloque de 1MB. Después, el concepto de tamaño máximo de bloque se eliminó y se sustituyó por el *peso máximo* del bloque (4MB actualmente).

La segunda, Bitcoin Cash, proponía cambiar el tamaño del bloque de 1MB a 8MB. Puesto que los bloques de 8MB no podían ser procesados por mineros que no actualizasen el software, esto hacía que dejasen de poder participar en la cadena por lo que no tiene retrocompatibilidad y se trata de un hard fork. Un dato importante de los hard fork es que la criptomoneda de la blockchain bifurcada también se bifurca, para evitar problemas de doble gasto. Por tanto, una poseedora de un bitcoin antes del fork tendría un bitcoin y un bitcoin cash al producirse la bifurcación, y cada moneda solo se podría gastar en su respectiva blockchain.

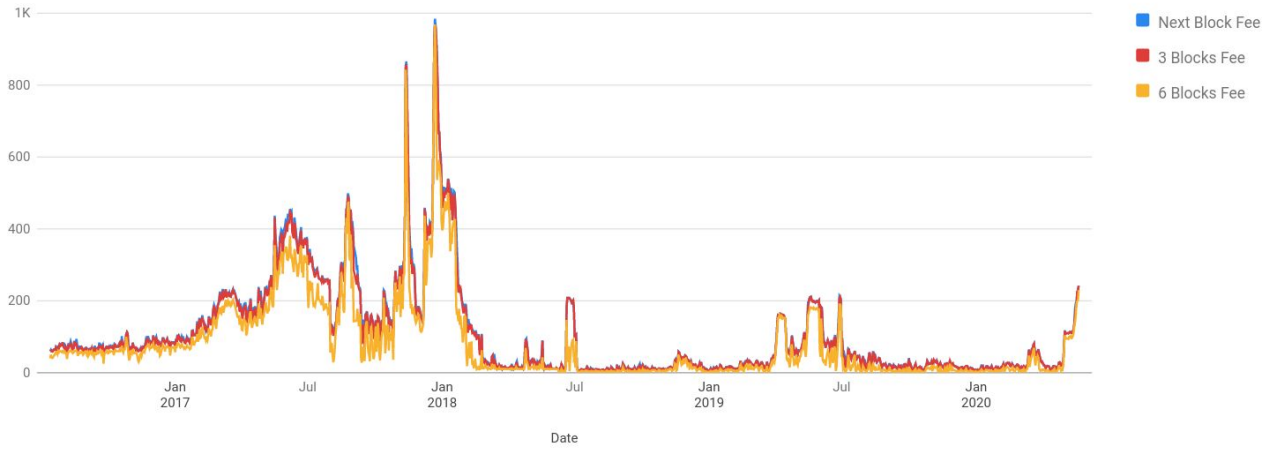
Otro concepto que resulta relevante en minería es el de los *mining pool* o grupos de minado. Varios mineros se coordinan para realizar la PoW de tal forma que cada uno prueba por su cuenta sin repetir las pruebas de los demás. Cuando uno de ellos consigue minar un bloque, reparte las ganancias entre todos en función del poder de

cálculo aportado. Es especialmente importante esta figura porque algunos controlan un porcentaje demasiado grande del poder de cálculo o *hashrate* lo que puede provocar una pérdida de la descentralización de la blockchain.

Para concluir esta sección de minado se va a hablar de las *fees* o comisiones. Junto a la transacción Coinbase, constituye el sistema de incentivos de Bitcoin para que los mineros soporten la red. Se trata de una pequeña cantidad de bitcoin que se obtiene de la diferencia entre los input y los output de la transacción, como se explicará en la sección Regular transactions. Esta comisión la define el usuario en función del tiempo que esté dispuesto a esperar para que la transacción sea incluida en un bloque teniendo en cuenta dos factores principalmente:

- La sobrecarga de la red, es decir, la cantidad de transacciones que se están lanzando en ese momento.
- El tamaño de la transacción, ya que las más pesadas conllevan mayor hashrate para ser procesadas por los mineros.

Las transacciones que incluyan menos comisiones para los mineros pueden sufrir inanición y quedarse en la mempool durante mucho tiempo. Una idea orientativa de los satoshis (unidad mínima de bitcoin correspondiente a 10^{-8} bitcoins) que puede costar cada byte de datos de una transacción en la blockchain es la siguiente:



Gráfica. Histórico de la media diaria de comisiones (satoshi/byte) en transacciones Bitcoin (https://billfodl.com/pages/bitcoinfees)

Cuantos más rápido se quiera incluir la transacción en la cadena, más satoshis/byte se pagarán de comisión. El tiempo se suele medir en bloques, sabiendo que aproximadamente se tardan 10 minutos en minar un bloque.

2.2.5. Transacciones

Existen dos tipos de transacciones en la arquitectura de Bitcoin: las regulares y las Coinbase. Las primeras sirven para que un participante de la red mande bitcoins a otro; las segundas son una recompensa a los mineros por usar su hashrate o poder de computación y tienen su origen en el propio sistema.

En esta sección se van a estudiar estas transacciones en detalle pero antes, siguiendo la explicación top-down que se está dando de Bitcoin, se va a estudiar la forma en que las transacciones se integran en el bloque.

Por un lado, el cuerpo del bloque contiene las transacciones salvo lo especificado en la sección anterior acerca de Segwit. Por otro, las cabeceras tienen el campo merkleRootHash, o raíz del árbol Merkle. Los merkle trees son árboles binarios usados para verificar integridad de datos, a través de la aplicación de hashes dos a dos en las distintas ramas del árbol como se muestra en la figura:

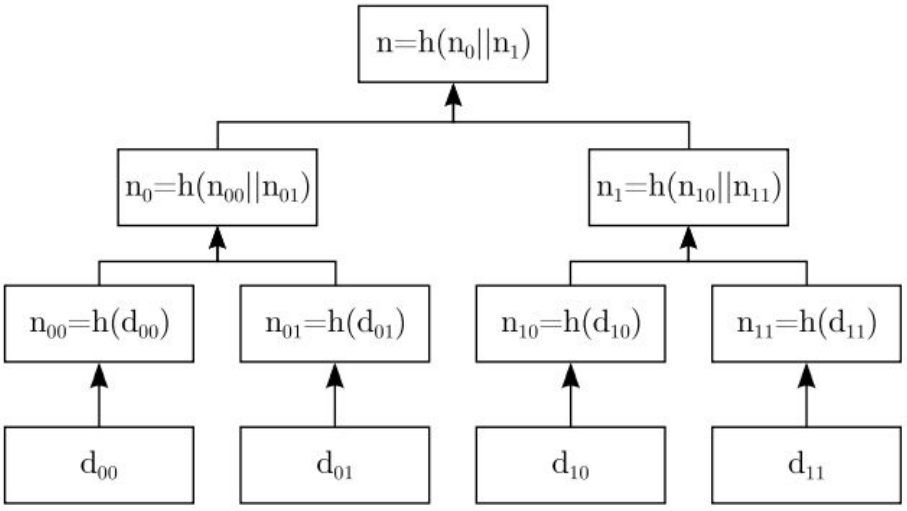


Figura. Árbol Merkle (Krzysztof Okupski 2016)

Utilizando como input la información que se pretende resumir, en el nivel más bajo de la figura, se hashea por parejas hasta obtener un único hash raíz o merkleRootHash. Debido a las propiedades de las funciones hash, un único cambio en cualquiera de los input haría que este hash cambiase por completo, rompiendo la integridad.

En el caso de Bitcoin las transacciones serían el input. Puesto que la prueba de trabajo se realiza sobre las cabeceras del bloque, incluyendo el merkleRootHash, resulta muy fácil validar la integridad de las transacciones de un bloque.

2.2.5.1. Cadenas de firmas digitales

La estructura de la criptomoneda Bitcoin es una cadena de firmas digitales. Se cambia de propietario en bitcoin firmando digitalmente el hash de la transacción anterior y añadiendo la clave pública del siguiente propietario.

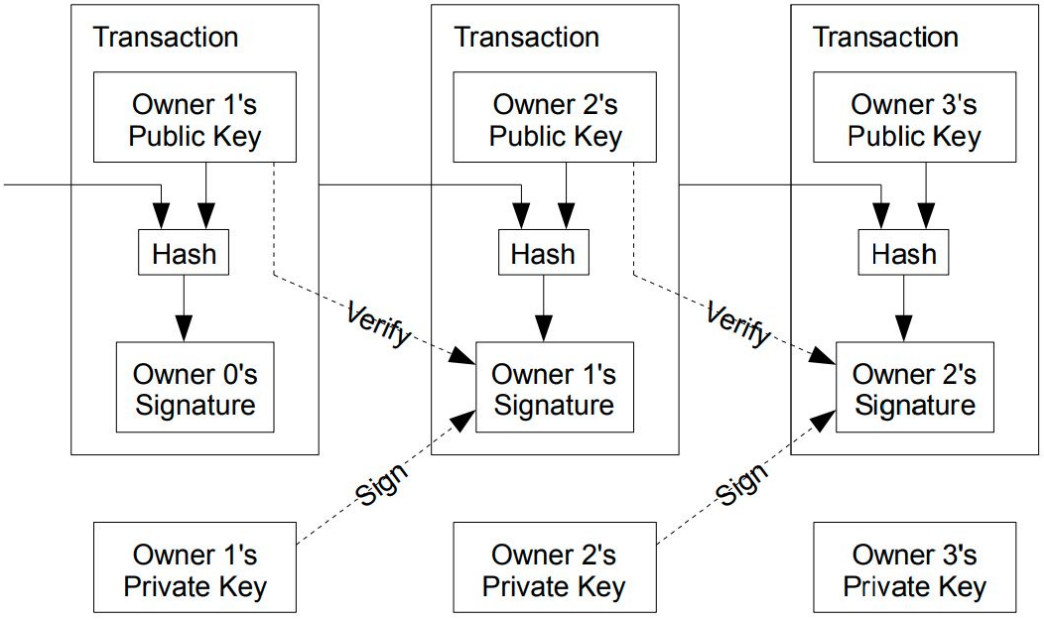


Figura. Cadenas de firma digitales (Nakamoto 2008)

Con esta información cualquier usuario puede verificar la cadena de firmas pero no es suficiente para saber si en algún momento se ha producido un doble gasto que invalide al completo esta cadena. Para comprobar esto en una red descentralizada es necesario que todas las transacciones sean públicas y cualquier nodo pueda acceder a ellas.

Aquí es donde entra la minería explicada en la sección anterior. Si hay dos transacciones que pueden incurrir en un doble gasto, se considera válida la primera transacción minada.

2.2.5.2. Addresses y wallets

Una *address* o dirección Bitcoin es un identificador que representa el posible destino para un pago Bitcoin. Consta de 26 a 35 caracteres alfanuméricos en Base58, un nuevo encoding introducido por Nakamoto parecido a Base64 pero evitando los caracteres no alfanuméricos y las letras que podrían llevar a confusión al transcribirlas

en papel como 0-O (cero u o mayúscula), I-l (I mayúscula o L minúscula), etc. La address típica es de 34 caracteres.

Es *case sensitive* si sigue el estilo antiguo o *insensitive* para transacciones con Segwit desde la Bitcoin Improval Proposal 0173. En el primer caso comienzan con el número 1 o el 3 y en el segundo con bc1.

Pueden ser generadas offline por cualquier usuario de Bitcoin de manera independiente utilizando alguna wallet o cliente como Bitcoin Core. También se puede obtener una address de Bitcoin utilizando una cuenta en una wallet online o en un *exchange*, que son casas de cambio muy utilizadas por usuarios que no quieren o no pueden descargar la blockchain o entrar en detalles técnicos.

Actualmente hay tres formatos de dirección:

- Las usadas para transacciones tipo P2PKH comienzan con el número 1, por ejemplo: 1BvBMSFYstWetqTFn5Au4m4GFg7xJaNVN2.
- Para tipo P2SH, explicadas en el siguiente apartado, que comienza con el número 3, por ejemplo: 3J98t1WpEZ73TNmQviecrnyiWrnqRhWNLy.
- Las usadas en transacciones Segwit tipo Bech32 comienzan con bc1, por ejemplo: bc1qar0srrr7xfkvy5l643lydnw9re59gtzwf5mdq.

Mención especial a un tipo de address que comienza por 3 llamada *multisig address*. Esta address tiene que ser firmada por varias claves privadas y es útil entre otras cosas para que exista un intermediario en una compra-venta. Cobrará una gran importancia en la tecnología Layer-2 que se explica en la sección Lightning Network.

Por su lado, las *wallets* o carteras de direcciones son programas que se encargan de gestionar estas address junto a sus correspondientes claves públicas y privadas. La siguiente figura muestra las tareas principales de una wallet:

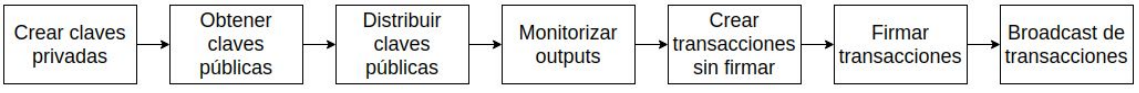


Figura. Servicios de una wallet

Las claves privadas en Bitcoin se crean con criptografía de Curva Elíptica, en concreto con el Elliptic Curve Digital Signature Algorithm (ECDSA). De la clave privada se obtiene una clave pública y con esta se construye el identificador o address.

En teoría la address debería usarse una sola vez para asegurar la privacidad en la red. Esta address se distribuye por la red y alguien realiza una transacción con ella como destino. La wallet monitoriza la blockchain para descubrir transacciones que envíen

bitcoins a esa dirección y una vez recibidos, estos bitcoins sin gastar ya están en posesión del propietario de la cartera.

Si desesa gastarlos, la wallet creará una transacción dirigida a otra address como se explicará en la siguiente sección Regular transactions. Después la firma y la transmite por la red para su inclusión en la blockchain.

2.2.5.3. Regular transactions

Regulares son las transacciones entre addresses. Su utilidad es principalmente transferir valor en bitcoins de una cartera a otra, por lo que la transacción siempre tiene una address origen llamado *input* y una address destino llamado *output*.

Como se veía en Cadenas de firmas digitales, el input de una transacción proviene del output de la transacción anterior, gracias a la cual hay fondos en esa address. Estos output se llaman *UTXO* (Unspent Transaction Output, o en español, salidas de transacciones sin gastar). Una vez gastados, no se pueden volver a usar en otra transacción previniendo así el problema del doble gasto.

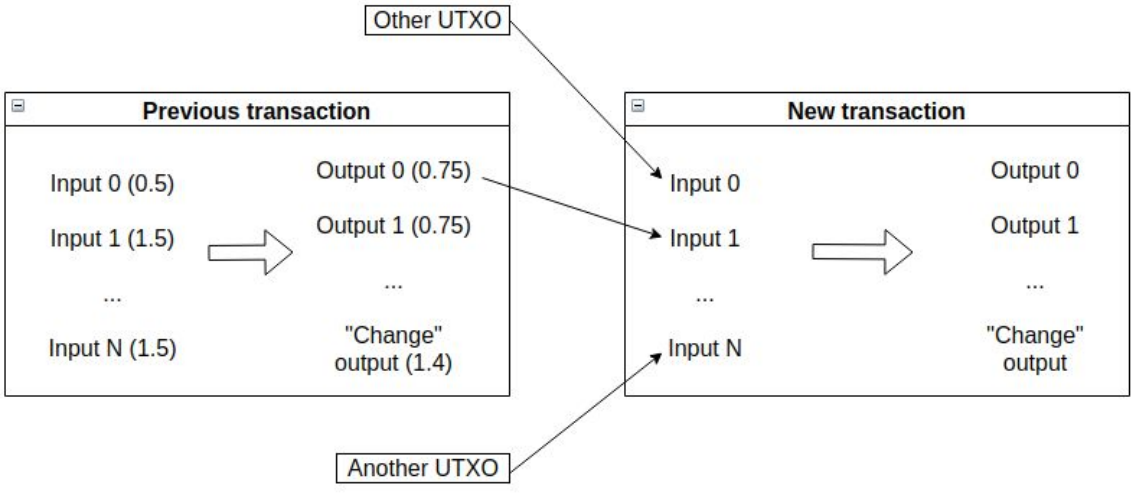


Figura. Transacción Bitcoin

Una transacción en la blockchain de Bitcoin puede tener varios inputs y varios outputs. Suponiendo que la *new transaction* es un pago de Alice a su equipo de trabajo, los input podrían ser fondos que tuviese Alice provenientes de distintas transacciones en las que ella resultase beneficiaria y los output podrían ser uno para cada trabajador.

Para poder utilizar esos UTXO como input, Alice tendrá que añadir en la transacción la prueba de que son suyos. En función de la prueba que tiene que aportar, las transacciones más comunes en Bitcoin son:

1. *P2PKH* (Pay to Public Key Hash), en la que se aporta como prueba la clave pública y una firma asociadas al hash que se indique.
2. *P2SH* (Pay to Script Hash), donde la prueba tiene que cumplir con lo que especifique un script.

Por la parte de los output, Alice utilizará con cada uno de los trabajadores el tipo de transacción que desee y estos tendrán que adjuntar sus respectivas pruebas cuando quieran gastar sus bitcoin, igual que hizo Alice con sus input.

Si Alice hubiese tenido un socio, Bob, y estuviesen usando la cuenta común de su empresa, podrían haber utilizado un tercer tipo de transacción:

3. *Multisig*, un tipo de transacción en la que se exigen distintas firmas para desbloquear el UTXO. Máximo 3 firmas, aunque puede ampliarse utilizando un script en una transacción P2SH.

Un último caso sería aquel en el Alice no quisiese realizar ningún pago, sino almacenar en la blockchain un archivo digital:

4. *Nulldata*, transacción a través de la cual se puede almacenar un mensaje en la blockchain para que permanezca en este registro inalterable. Permite un solo output con un mensaje de no más de 80 bytes.

Si bien puede parecer un número reducido de bytes, es suficiente para que Alice cree un hash del archivo que desea guardar, por ejemplo a través del sistema de archivos descentralizado IPFS, y guarde ese hash en la blockchain. De esta forma quedaría una prueba de que ese documento existió en el momento en que se incluyó la transacción nulldata en la cadena.

Se han descrito brevemente los tipos de transacciones, así como la utilidad de input y output. Existe un output que, aún teniendo las mismas características de los demás, cumple un propósito diferente. Se trata del *change output*, un output que representa “la vuelta” siguiendo la analogía del cambio que recibes cuando pagas con un billete. Al no ser habitual que los input coincidan con los output, se utilizan input de mayor cantidad que los output y el cambio se vuelve a enviar a una address propiedad de quien envía la transacción.

Nótese en la figura que en la *previous transaction*, la suma de los input (3,5) no es igual a la suma de los output (3,4). Esta diferencia es la *fee* o comisión que se lleva el minero por incluir la transacción en la blockchain.

Por último un apunte sobre el lenguaje utilizado para escribir los script, llamado Bitcoin Script. Es un lenguaje orientado a pila (stack-oriented) como el de Forth, diseñado deliberadamente para ser *stateless* (sin estado) y Turing incompleto. No tener estado asegura que una vez que una transacción es añadida a la cadena de bloques, no hay ninguna acción que la haga permanentemente inutilizable. Ser Turing incompleto, la falta de bucles o "gotos", hace que el lenguaje de scripts sea menos flexible y más predecible, simplificando enormemente el modelo de seguridad.

2.2.5.4. Coinbase transaction

Es un tipo especial de transacción por la cual el propio sistema Bitcoin recompensa al minero por el esfuerzo.

Antes de empezar a minar, el minero tiene que construir el bloque sobre el cual quiere realizar la prueba de trabajo. Incluirá por un lado las transacciones que tiene esperando en el mempool, y por otro la transacción Coinbase. La diferencia de esta transacción frente a las regulares es que no tiene un input de una transacción anterior, sino únicamente la altura del bloque (block height).

Originalmente la recompensa que ofrecía Bitcoin a los mineros en la transacción Coinbase era de 50 bitcoins. Cada 210,000 bloques, aproximadamente cada 4 años, es recompensa se reduce a la mitad. Ahora mismo es de 12.5 BTC tras el halving del 11 de mayo de 2020.

2.2.5.5. Estándares en las transacciones

Los estándares en las transacciones se definen como un conjunto de requisitos para cualquier nodo que utiliza el cliente de referencia para el procesamiento de transacciones. Las que no cumplen los requisitos se consideran no estándar y no se transmiten ni se minan.

Estos estándares pueden cambiar con las distintas actualizaciones por lo que en esta sección se intentarán recopilar las que se están utilizando más recientemente, según Krzysztof Okupski (2016) y también según la versión más actualizada de la guía de

desarrollo https://developer.bitcoin.org/devguide/transactions.html. Algunas de estas reglas estándar, a partir de Bitcoin Core 0.9.3, son:

- Tamaño de transacción: no puede exceder, como es obvio, el tamaño del bloque. Si bien antes de SegWit se hablaba de un block size de 1MiB, después se pasó a hablar de block weight, con un máximo de 4MiB. Es decir, una equivalencia de 1 a 4.
- Versión de transacción: la versión de formato de transacción es actualmente 1.
- Regla de transacción final: la transacción se considera final si se ha excedido el tiempo de bloqueo (locktime) o si todos los números de secuencia de los input están puestos al valor máximo 0xffffffff. Tiene que ser final para poder incluirla en un bloque.

  Esta regla está asociada con un mecanismo obsoleto llamado reemplazo de transacción. Está permitido reemplazar ciertas partes de una transacción hasta que todas las entradas de la transacción se finalizan o termina el tiempo de bloqueo de la transacción. Hay que tener en cuenta que la funcionalidad de reemplazo de transacción ha sido completamente eliminada de la implementación de referencia para reducir la complejidad del protocolo. La forma de reemplazar transacciones ahora es con el método Replace By Fee en el que se lanza una nueva transacción con una comisión mayor a la anterior.
- Cada signature script de la transacción debe ser menor de 1.650 bytes, suficiente para permitir una transacción multisig de 15 firmas usando claves públicas comprimidas en una transacción tipo P2SH. Además, no puede meter nuevos opcodes en la pila de evaluación, solo datos.
- Ningún output puede tener menos de ⅓ de los satoshis que costaría gastarlo (el satoshi es la unidad mínima en Bitcoin, equivalente a 10^{-8} bitcoins). A excepción de las transacciones nulldata por supuesto, en los que se manda 0 satoshis.

2.2.6. Características como base de datos

En cualquier base de datos distribuida, donde ningún nodo es responsable del resto de nodos involucrados en una transacción, garantizar las propiedades ACID en una transacción presenta complicaciones.

Las conexiones de red pueden fallar, o un nodo puede completar con éxito su parte de la transacción pero fallar en otros nodos y el sistema tendrá por tanto que deshacer todos los cambios, etc. Algunos protocolos, como el 2PC de confirmación en dos fases (no confundirse con el bloqueo en dos fases) proporciona atomicidad para las transacciones distribuidas para garantizar que cada participante en la transacción decida si la transacción debe realizarse o no. En pocas palabras, en la primera fase, un nodo (el coordinador) interroga a los otros nodos (los participantes) y solo cuando todos responden que están preparados, el coordinador, en la segunda fase, formaliza la transacción.

Sin embargo, Bitcoin y otras blockchain no tienen nodos coordinadores por lo que cobra gran importancia el algoritmo de consenso PoW. Junto al resto de conceptos explicados con anterioridad en este trabajo, permiten que la blockchain garantice las características esperadas en una base de datos distribuida.

2.2.6.1. Integridad

Blockchain asegura la integridad de los datos replicándolos en todos los nodos y además utilizando el hash del árbol merkle, de forma que si un nodo intentase cambiar un solo bit de las transacciones del bloque, cambiaría el hash por completo y los nodos adyacentes rechazarían ese cambio.

2.2.6.2. Disponibilidad

El registro es público por lo que siempre se puede acceder a él. Al estar replicado, basta con tener una copia de la cadena de bloques, la cual se puede conseguir en cualquier momento conectándose a los peers.

Dejaría de estar disponible si todos los nodos de la red perdieran los datos de blockchain.

No existe la posibilidad de interbloqueos porque solo un minero consigue realizar la prueba de esfuerzo en cada bloque. Cuando consigue minar el bloque, realiza un broadcast y el resto de mineros comienzan a minar el siguiente bloque. Si hipotéticamente dos mineros minasen distintos bloques en el mismo instante de tiempo, uno de los dos sería eventualmente rechazado como se ha explicado en Minería bitcoin y la cadena seguiría su curso.

2.2.6.3. Confidencialidad/Privacidad

La cadena es pública y por tanto cualquiera puede auditarla y revisarla. Sin embargo, la información que aparece en las transacciones es únicamente la de las addresses bitcoin, y éstas corresponden a personas anónimas. Una misma persona puede crear todas las addresses y carteras que quiera, puede incluso mover el dinero entre sus propias direcciones. La privacidad está garantizada por no saber a quién pertenece cada address, por tanto la confidencialidad en Bitcoin viene dada por el buen uso que se le dé a las carteras.

Un riesgo para la privacidad es el uso de la misma address para más de una transacción. El problema de esto es que cada vez que se usa aumentan las posibilidades de identificar al propietario de la address. Existen en el dominio público bases de datos que enlazan address con propietario.

Puede convertirse en un problema si una persona a quien has enviado bitcoins, o que están en la misma cadena de propiedad con posterioridad a tu transacción, gasta esos bitcoin en la compra de un bien ilegal: esto podría derivar en una investigación en la que tu transacción se viese implicada. Por tanto es mejor utilizar siempre una única address para cada transacción y no volver a usarla.

Si bien las transacciones en Bitcoin tienen una trazabilidad, existen formas de evitar que la traza llegue finalmente a la dirección original. Una de ellas es la llamada *CoinJoin*, mediante la cual distintos usuarios combinan sus input y output en una sola transacción de forma que se rompe la trazabilidad, al no ser relacionar los input con los output de cada usuario.

2.2.6.4. Seguridad

La seguridad viene dada por el propio sistema, incluida la verificación distribuida como se ha explicado en la sección Red P2P, y también por el algoritmo criptográfico double-SHA.

Este algoritmo podría ser roto por un hipotético ordenador cuántico en el caso de que la comunidad de desarrolladores no fuese capaz de desarrollar una solución. Sin embargo, el momento en que este tipo de ordenadores sea capaz de ejecutar un

ataque de fuerza bruta parece aún lejano y cuando se vaya desarrollando la tecnología cuántica también se podrá ir cambiando el protocolo de Bitcoin con contramedidas.

Por otro lado, un atacante podría mandar un bloque inválido pero el resto de nodos lo rechazaría. Si el atacante pretendiese modificar una transacción suya grabada en un bloque ya incluido en la cadena, sería necesario que generase una prueba de trabajo para todos los bloques siguientes de la cadena más larga, para lo que necesitaría como mínimo (en caso de que el bloque que pretenda modificar sea el último) tener más poder computacional que la mayoría de la red, es lo que se llama un ataque del 51%.

Este caso realmente no sería un ataque, ya que está creando la cadena más larga. Por esto quienes participan en la red son conscientes de que hasta que no se han añadido varios bloques después del suyo no se puede considerar escrito en firme.

2.2.7. Propiedades ACID de las transacciones

2.2.7.1. Atomicidad

Las transacciones en blockchain son atómicas por diseño.

Si tomamos como ejemplo una transacción de dinero entre Alice y Bob en una base de datos relacional, procesarla correctamente requiere un mínimo de 2 pasos, restar una cantidad de un campo y sumarla en otro, por no hablar de las comprobaciones necesarias. Ya que son varios pasos, comprobar la atomicidad resulta relevante.

En cambio, debido a la naturaleza de las transacciones en blockchain, la transacción se realiza en un solo paso. No se resta de un campo y se suma en otro sino que el antiguo propietario asigna un nuevo propietario con el uso de las firmas digitales. Todo ello queda escrito en un solo momento. cuando el bloque es minado.

2.2.7.2. Consistencia

Ninguna transacción puede romper la consistencia del diario (blockchain) porque los nodos mineros solo incluyen en los bloques candidatos a ser añadidos a la cadena aquellas transacciones que cumplen las reglas estándar del protocolo. En caso de incluir transacciones inválidas, su bloque nunca sería aceptado por el resto de nodos.

2.2.7.3. Aislamiento

El mecanismo de minado asegura la ausencia de concurrencia. Cada transacción está aislada en un bloque y es independiente de las demás. Los cambios de estado en la blockchain provocados por el último bloque quedan grabados en el momento en que se mina.

2.2.7.4. Durabilidad

Una vez el bloque en el que está grabada la transacción entra en la cadena, los cambios permanecen para siempre en esta. Están grabadas en orden todas las operaciones desde sus inicios en 2009, incluido el bloque inicial o Genesis Block.

2.2.8. Transacciones en base de datos relacional vs transacciones en blockchain

La principal diferencia entre bases de datos y blockchain es la versatilidad. Mientras las bases de datos se pueden utilizar para infinidad de casos de uso, blockchains como Bitcoin tienen uno solo, lo que les permite focalizarse en él y ofrecer descentralización, atomicidad y el resto de características anteriormente explicadas.

Blockchain es básicamente un sistema de transiciones, cada cierto tiempo se añade un bloque a la cadena y se cambia de estado según lo que indicasen las transacciones de ese bloque. Todos los bloques están guardados por lo que se mantienen todas las transacciones desde la primera a la última.

Las bases de datos, en cambio, solo guardan el último estado. Consecuentemente, una operación DELETE elimina la información para siempre. Es por eso que la blockchain desde un punto de vista funcional se equipara más bien a un registro diario de transacciones, con la salvedad de que está distribuido y replicado entre todos los nodos lo que proporciona seguridad.

Las bases de datos ofrecen mayor rapidez, mayor gama de operaciones permitidas, más facilidad de acceso, décadas de desarrollo y perfeccionamiento… En definitiva, blockchain no es un sustitutivo de las bases de datos relacionales.

Es importante conocer las limitaciones. Mientras que estas últimas pueden ofrecer confirmación de escritura en apenas milisegundos, cualquier blockchain realmente descentralizada necesita como mínimo varios segundos para que una transacción

quede incluida en un bloque de la cadena, y varios minutos para confirmar que el bloque pertenece a la cadena más larga.

Blockchain sí puede usarse para transacciones en las que lo más importante sea la inmutabilidad y el no repudio, ya que son sus características principales. También puede utilizarse cuando se quiera prescindir de intermediarios o terceras partes de confianza, garantizando así la neutralidad en la plataforma.

Este último punto tiene un "pero" que no se suele comentar en los entornos de desarrollo colaborativo y es que prescindir de un tercero de confianza es solo cierto relativamente, ya que las actualizaciones dependen de si existen desarrolladores y desarrolladoras con motivación para hacerlas, y cuando un proyecto deja de ser motivador puede resultar complicado de gestionar salvo que exista un interés monetario. En el caso de Bitcoin, la motivación de cambiar el sistema financiero confluía con las recompensas que obtendrían los desarrolladores si el proyecto seguía adelante.

Más que prescindir de un tercero de confianza, se puede afirmar que se deja de confiar en los anteriores actores del mercado y el propio protocolo se convierte en el tercero de confianza. Con la diferencia de que Bitcoin necesita consensuar los cambios mientras que los anteriores actores del mercado de dinero (gobiernos, grandes corporaciones financieras) podían tomar medidas de carácter discrecional. Mientras Bitcoin mantenga una filosofía justa, tiene posibilidades de convertirse en el sistema de pagos internacional. Y los gobiernos podrán tomar medidas a la hora de gastarlos, pero no a la hora de crearlos.

2.3. Ethereum

Ethereum es una blockchain que comienzan a diseñar Vitalik Buterin y su equipo en 2013 y sale a producción en julio de 2015. Se trata de la primera alternativa relevante a Bitcoin en cuanto a funcionalidad: mientras la primera es un medio de pago, Ethereum busca convertirse en una plataforma en la que desarrollar aplicaciones descentralizadas.

La principal diferencia técnica con Bitcoin es el uso de un lenguaje Turing completo. Esto implica que existen una gran cantidad de operaciones permitidas, incluida la operación JUMP utilizada en los bucles que por diseño se evitaban en Bitcoin Script. Y

es que el objetivo de Bitcoin al usar este lenguaje era reducir la funcionalidad al uso de criptomoneda, evitando la posibilidad de entrar en un bucle infinito que bloquease los nodos mientras procesaban la transacción.

Ethereum controla el gasto en computación con una unidad de medida interna llamada *gas*, cuantificando con ella la cantidad de cálculos que se ejecutan en una transacción. Al estar medidos, se pueden limitar, evitando así bucles infinitos y cualquier transacción que vaya a incurrir en un mayor gasto al previsto. El *gasprice* indica en cada momento cuánto gas se puede comprar con *ether*, la criptomoneda asociada a Ethereum. Dependiendo de lo congestionada que esté la red, tendrá un precio u otro, ya que el gasprice tiene la misma funcionalidad que tenían las comisiones en Bitcoin, recompensar a los mineros.

Los nodos de esta blockchain cuentan con una abstracción llamada Ethereum Virtual Machine (EVM). Esta máquina virtual utiliza para sus operaciones el lenguaje Turing completo que suele nombrarse como *EVM bytecode*, orientado a pila (stack-oriented). En ella se encapsulan todas las operaciones de la blockchain y además les permite disponer de espacio dedicado en el que almacenar datos de las transacciones, siendo este espacio de 3 tipos:

- La propia pila
- La *memory* o memoria, un almacenamiento volátil que dura mientras se ejecuta la transacción y, en su caso, el smart contract asociado
- El *storage* o almacenamiento clave/valor a largo plazo del smart contract

Como veíamos en Blockchain, se podría pensar en la cadena de bloques como un sistema de transiciones (transition system).

Por un lado, el estado en Bitcoin representaría los output no gastados y a quién pertenecen:

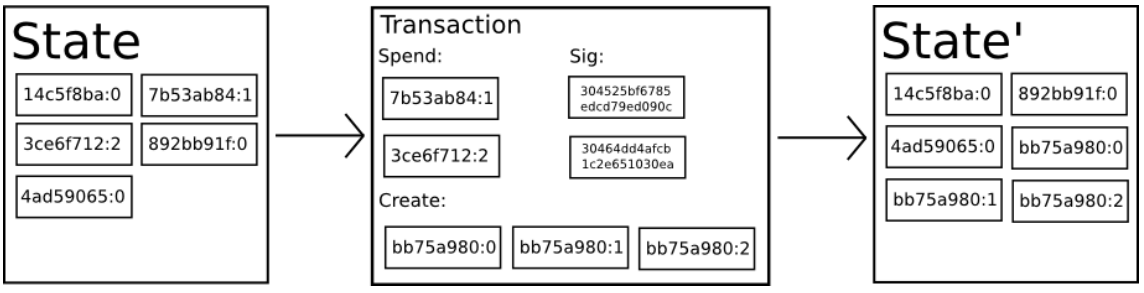


Imagen. Sistema de transiciones en Bitcoin (Ethereum whitepaper)

En Ethereum, el almacenamiento a largo plazo permite que el estado incluya otros datos:

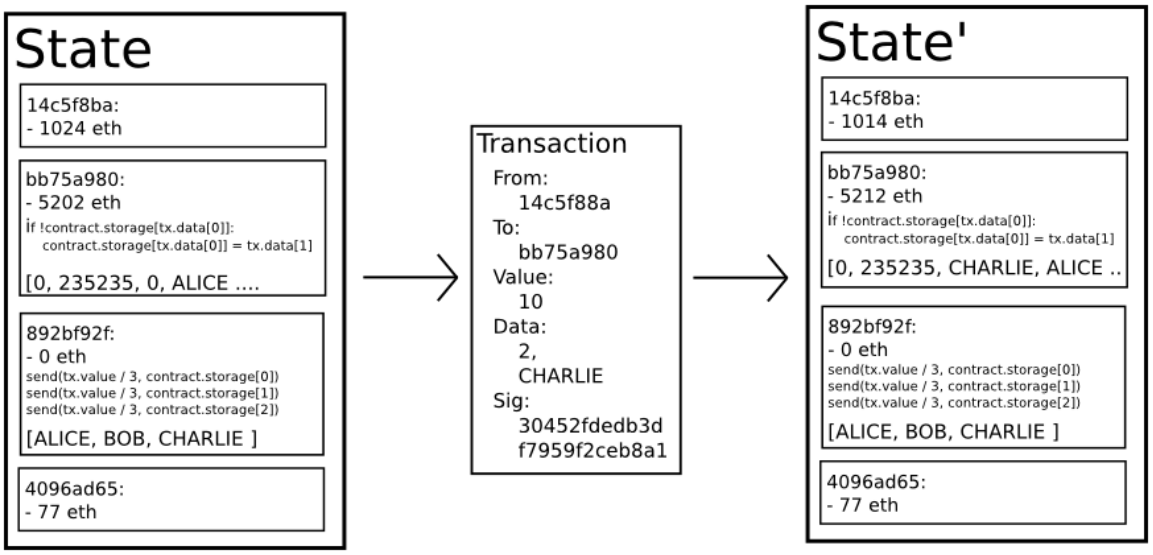


Imagen. Sistema de transiciones en Ethereum (Ethereum whitepaper)

En la transacción, además de la address de destino (el campo *To*) y la cantidad de ethers enviados (*Value*) existe otro campo, el campo *Data*. En el caso de que exista un *smart contract* desplegado en esa address, el campo Data servirá como input para el contrato que ejecutará un código y normalmente producirá algún cambio en el storage a largo plazo del contrato.

La versatilidad en Ethereum con su lenguaje Turing completo es mayor que en Bitcoin. Permite crear aplicaciones distribuidas (*dapps*) a las que cualquier participante en el sistema tiene acceso desde su propio nodo.

Por contra, el coste de esta versatilidad es una blockchain más compleja y potencialmente con más puntos de fallo.

2.3.1. Smart Contracts

La utilidad que ha hecho conocida la blockchain de Ethereum ha sido el uso de los *smart contracts* o contratos inteligentes, solo posibles gracias a usar un lenguaje Turing completo.

Se trata de código autoejecutable que se puede almacenar en una address de Ethereum. Este código se despliega en la address mediante una transacción y, una vez incluida en un bloque de la cadena principal y extendida por la red, cualquier participante puede ver en su propio nodo los métodos del contrato a través del *ABI* (Application Binary Interface). Conocidos los métodos, es sencillo ejecutar el servicio que ofrezca ese smart contract, pagando el gas necesario para la ejecución.

Este código se escribe con Solidity o Vyper, lenguajes de programación creados para interactuar con la EVM. El más común es Solidity, un lenguaje orientado a objetos, similar a Javascript pero tipado estáticamente y que se compila al lenguaje bytecode de la EVM.

Los smart contracts soportan referencias a contratos almacenados en otras addresses, la herencia, lanzar eventos y permiten el uso de interfaces. Además, existen palabras reservadas relacionadas con blockchain como por ejemplo *address*, *ether*, *wei* y también propiedades de las transacciones, bloques, etc. Las más comunes son, directamente desde la especificación de Solidity (https://solidity.readthedocs.io/en/v0.5.3/units-and-global-variables.html):

- `blockhash(uint blockNumber) returns (bytes32)`: hash of the given block - only works for 256 most recent, excluding current, blocks
- `block.coinbase` (`address payable`): current block miner's address
- `block.difficulty` (`uint`): current block difficulty
- `block.gaslimit` (`uint`): current block gaslimit
- `block.number` (`uint`): current block number
- `block.timestamp` (`uint`): current block timestamp as seconds since unix epoch
- `gasleft() returns (uint256)`: remaining gas
- `msg.data` (`bytes calldata`): complete calldata
- `msg.sender` (`address payable`): sender of the message (current call)
- `msg.sig` (`bytes4`): first four bytes of the calldata (i.e. function identifier)
- `msg.value` (`uint`): number of wei sent with the message
- `now` (`uint`): current block timestamp (alias for `block.timestamp`)
- `tx.gasprice` (`uint`): gas price of the transaction
- `tx.origin` (`address payable`): sender of the transaction (full call chain)

En los contratos la lectura es gratis, ya que puedes acceder a tu nodo para ello, pero la escritura implica un coste en todos los nodos de la red. Por tanto, las transacciones

que llaman a un método que realice algún cambio en el storage, son transacciones que tienen que ser minadas.

Para terminar, una puntualización: los contratos deben ser lo más simples posibles. Existen ciertas limitaciones, como el control de versiones, los fallos de seguridad en el código de los contratos, el coste de ejecución del contrato o de almacenamiento, etc. Estas limitaciones permiten afirmar que es una buena práctica reducir la lógica de negocio en el smart contract al mínimo y completarla con lógica de negocio en la parte cliente, fuera de la blockchain.

2.3.2. Tokenización

La versatilidad en Ethereum permite que cualquiera pueda crear su propio token o criptomoneda dentro de la blockchain. Esto es útil para proyectos que necesitan financiación o para dapps (distributed apps) que buscan tener cierto control sobre la moneda con la que se puede acceder a sus servicios. Por supuesto, todo lo desarrollado dentro del ecosistema Ethereum carece de la independencia que podría tener si crease una blockchain independiente con las características buscadas, pero a cambio se beneficia de las actualizaciones y garantías que ofrece Ethereum, que es el mayor proyecto de ecosistema blockchain con smart contracts.

Un nuevo token se implementa a través de un smart contract por lo que se compra con ethers. Durante 2017 se produjeron una gran cantidad de ICOs (Initial Coin Offering), ofertas de tokens cuyo objetivo era financiar un proyecto. Un par de ejemplos representativos de estas ICO en España fueron:

- Proyecto Aragon, un entorno para crear y gestionar organizaciones distribuidas. Busca crear una legislación internacional en la cual puedan existir organizaciones más allá de las legislaciones de los países.
- La cadena de restaurantes Nostrum, quienes a cambio de financiación entregaban tokens que se podía utilizar para programas de fidelización, pedidos a domicilio, etc

Los ICO recibieron una gran cantidad de dinero, pero no todos los proyectos prosperaron por lo que se dejó de confiar en este tipo de token para financiar proyectos.

Sin embargo, más allá de su uso para captar financiación, la idea de token puede ser útil para dapps en las que es necesario un control sobre la moneda de cambio. Por

ejemplo, en un sistema de puntos de fidelización solo tiene sentido si la empresa tiene cierto control sobre los puntos. De lo contrario, los clientes podrían comprar puntos directamente con ethers y los puntos dejarían de cumplir su función, que normalmente es guiar a los clientes a la compra del producto deseado por la empresa.

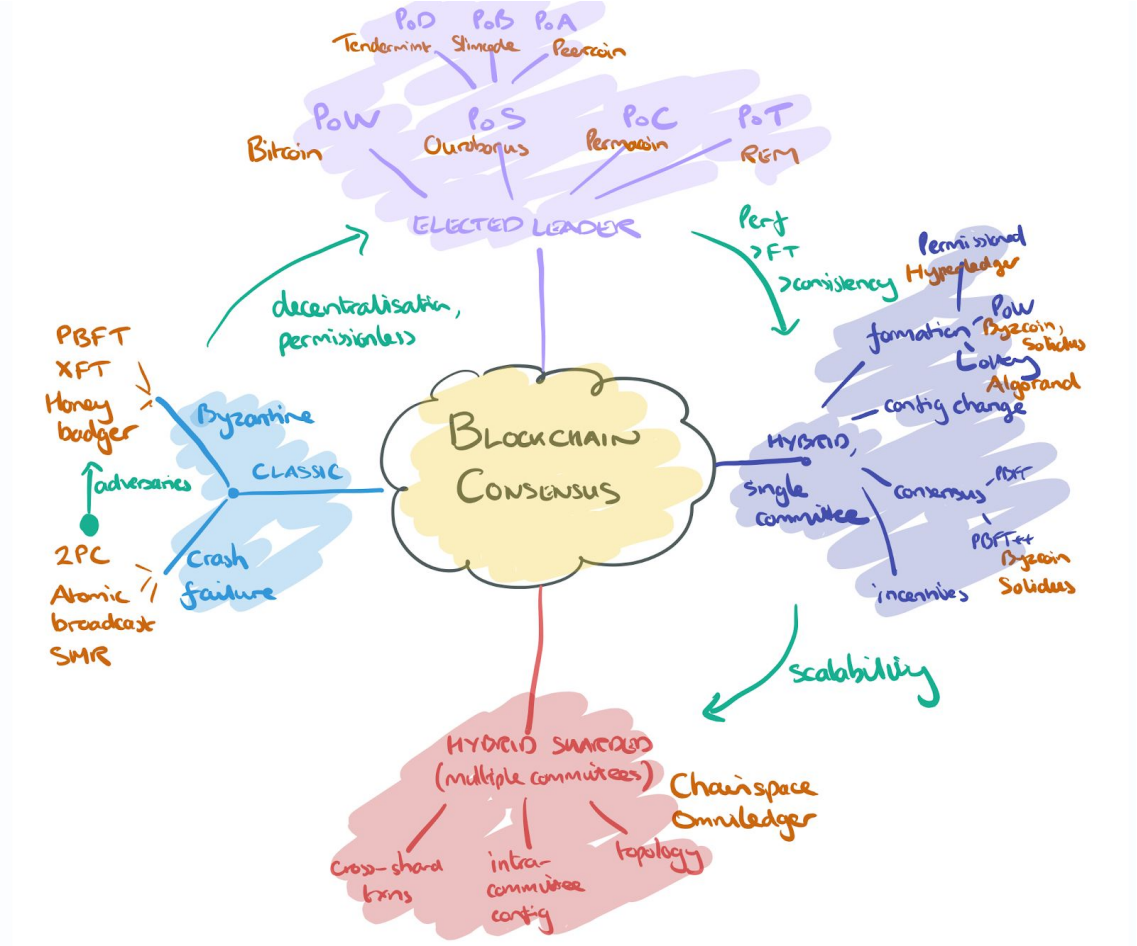
Un token puede ser útil también en un sistema de recompensa, por ejemplo en el sistema de créditos de libre asignación de las universidades. También en un sistema de reputación en el que los alumnos más participativos o que más ayudan a sus compañeros reciben tokens por parte del sistema educativo.

2.4. Más allá de las blockchain públicas

2.4.1. Mecanismos de consenso

Una de las partes más importantes y diferenciadoras de una blockchain es la forma en que todos los nodos llegan a un consenso sobre cuál es el siguiente bloque que debe formar parte de la cadena.

Existen distintos tipos de protocolos que actúan como mecanismo de consenso en computación distribuida. Estos protocolos son en mayor o menor medida descentralizados y en función de esto se encuadran mejor o peor en las distintas implementaciones de blockchain públicas o permisionadas, respectivamente.



2.4.1.1. Proof-of-Work (PoW)

El protocolo Proof of Work (PoW) o prueba de trabajo es un mecanismo de consenso que se basa en un puzle criptográfico que asegura la realización de un determinado esfuerzo para su resolución. Los nodos compiten por resolver esta prueba.

Se va a desarrollar el caso de Bitcoin con el objetivo de completar la explicación del apartado Bitcoin. El "nonce" de un bloque Bitcoin es un campo de 32 bits (4 bytes) que sirve para introducir cierta aleatoriedad en el bloque. El resto de campos de la cabecera del bloque (version, merkle_root, prev_block...) vienen preestablecidos para ese bloque por lo que siempre serán los mismos.

Cualquier cambio en un campo del bloque hará que el hash del bloque sea completamente diferente. En el caso de Bitcoin, se utiliza como prueba de trabajo la obtención de un número (nonce) tal que si se añade al resto del contenido de un bloque y se le aplica el hash double-SHA a todo ello, se obtiene un número de 256 bits menor que un número *target* T:

$$SHA256^2\,(nonce \,||\, resto\ de\ las\ cabeceras\ del\ bloque) \leq T$$

Este target lo calcula la propia red Bitcoin en función de la capacidad de cálculo utilizada por los mineros en cada momento, de tal forma que estadísticamente un bloque tarde en minarse 10 minutos de media.

Dado que es imposible predecir qué combinación de bits dará lugar al hash correcto, se prueba por fuerza bruta con muchos nonce diferentes y se recalcula el hash para cada valor, hasta que se encuentre un hash menor que el target. Como este cálculo iterativo requiere tiempo y recursos, el descubrimiento del bloque con el valor nonce correcto constituye una prueba de trabajo. Si bien la PoW requiere una gran gasto en computación, la comprobación es trivial.

Este número objetivo o target se ha ido decrementando con el tiempo con la finalidad de hacer cada vez más complicada la obtención de la PoW puesto que los nodos mineros han ido aumentando su capacidad y especializando su hardware.

Los pros de este protocolo de consenso son por un lado la justicia en el reparto de los incentivos, ya que la probabilidad de minar un bloque es directamente proporcional al gasto en computación realizado, y por otro la descentralización, ya que cualquier nodo puede obtener la recompensa. Por contra, el coste energético para mantener la red es elevado.

2.4.1.2. Proof-of-Stake (PoS)

La prueba de participación es otro grupo de algoritmos de consenso. En ellos, el bloque elegido para pasar a formar parte de la cadena no lo deciden los mineros, sino los nodos validadores. No dependen de la capacidad de cómputo, sino de la cantidad de participación en el sistema que puedan demostrar. En una criptomoneda se entiende como participación la cantidad de moneda de la que el nodo es propietario.

Si un nodo validador posee una gran cantidad de moneda, tendrá un desincentivo para producir un bloque inválido. Sin embargo, esto asunción presenta un riesgo y es que existen instrumentos financieros que permiten apostar por que un activo va a bajar de precio.

Un algoritmo PoS se está planteando en un futuro hard fork de Ethereum, que por el momento utiliza PoW al igual que Bitcoin. La implementación de este algoritmo en Ethereum, que se llama Casper, se basa en la idea de que cualquier nodo de la red

puede convertirse en nodo validador mandando una apuesta por el bloque que considera puede pasar a formar parte de la cadena.

Esta apuesta es una transacción especial por la que bloquea la cantidad deseada de ethers. Una vez conocido el bloque ganador, quienes apostaron por él reciben una recompensa proporcional a los ethers que apostaron. Por el contrario, si un nodo validador propone bloques inválidos o se muestra claramente actuando de forma maliciosa, el protocolo puede confiscar su participación.

Por supuesto, el pro más evidente de este mecanismo es el ahorro energético de la red por lo que no resulta necesario recompensar con tantas monedas cada bloque creado. En contra, los participantes con más ethers o participación tienen más probabilidad de recibir recompensa, y al ser proporcional reciben mayor parte.

2.4.1.3. Otros algoritmos de consenso

Existe una gran cantidad de algoritmos de consenso: Delegated Proof of Stake (dPoS), Proof-of-Importance (PoI), Federated Byzantine Agreement (FBA), Proof of elapsed time (POET), etc.

Quizá el más relevante es el Practical Byzantine Fault Tolerance PBFT (Castro and Liskov 1999) en el que se ofrece una solución al problema de los generales bizantinos. No se van a estudiar ya que no es el objeto de este trabajo.

2.4.2. Redes permisionadas o privadas

Podemos diferenciar dos tipos de blockchain, públicas y permisionadas, atendiendo a la posibilidad de acceder a la red.

En las blockchain públicas, cualquier nodo tiene acceso a la cadena de bloques y puede pasar a formar parte de la red. En cambio, en las permisionadas o privadas existen restricciones o incluso un nodo responsable de permitir o no el acceso a los nodos.

A las redes públicas cualquiera puede unirse y tienen gran cantidad de nodos, por tanto se debe dar por hecho que algunos nodos pueden actuar de manera fraudulenta. La forma de proporcionar seguridad es generar incentivos para los nodos que soportan la red, de forma que sea más rentable actuar de forma honesta.

Las redes privadas o permisionadas no se pueden considerar descentralizadas en este momento, ya que cuentan con pocos nodos participantes y basan su seguridad en la protección de esos nodos, de la misma forma que se haría en una base de datos centralizada. Por tanto, no se aplican las características que se veían en el apartado Características como base de datos y por tanto no se consideran para este trabajo.

2.4.3. Tecnologías blockchain Layer-2

2.4.3.1. Sidechain

2.4.3.2. Lightning Network

2.4.4. Utilidad de la tecnología blockchain

El dinero es el primer y más importante de los casos de uso de blockchain. Puesto que esta tecnología permite un intercambio de valor virtual, es entendible que su primer uso fuese el de moneda de cambio, equiparable al dinero fiat a día de hoy o al oro unos años atrás.

Existen tres conceptos entorno al dinero que conviene aclarar para conocer la relación que tienen con blockchain. Por un lado tenemos el dinero digital, por otro las monedas virtuales y como un subconjunto de estas últimas, las criptomonedas.

El dinero digital es la representación electrónica del dinero en efectivo o fiat que existía con anterioridad a internet. El uso de bancos hizo que la concepción que tenía la sociedad del dinero como papel moneda cambiase y pasase a ver el dinero como una anotación en cuenta en el sistema bancario, de tal forma que se podían hacer transacciones entre particulares o entidades pero siempre con la mediación del banco que actuaba como tercera parte de confianza.

Dinero digital es por tanto la mayor parte del dinero del mundo, aquél que es susceptible de ser enviado en forma de transacción electrónica. Si bien los bancos fueron y aún son los principales interfaces de la población con el sistema bancario que permite las transacciones con este tipo de dinero, es cierto que las últimas dos décadas han surgido otras empresas focalizadas únicamente en este tipo de transacciones como Paypal, Venmo, Stripe… En todas ellas se deposita la confianza para una transacción entre dos particulares.

Por otro lado, moneda virtual es un tipo de moneda que solo existe en formato electrónico y que según el Banco Central Europeo(European Central Bank 2015) no puede ser considerado dinero al no haber sido emitida por un banco central, una

institución de crédito o una institución de dinero electrónico. Al contrario, es emitida y mantenida por sus creadores. Una moneda virtual puede ser la que se utiliza en un videojuego para comprar características de personajes o la que se utiliza en un restaurante en forma de puntos, cuando se puede intercambiar por el dinero digital, pero en general de forma centralizada bajo el control de quienes emiten esa moneda, ya sea la empresa de videojuegos o el restaurante. También hace uso de terceras partes de confianza.

Dentro de estas monedas virtuales, encontramos unas con características particulares. En primer lugar, son descentralizadas. Todas las monedas que habíamos visto hasta ahora eran centralizadas ya que existían problemas como el del doble gasto en computación distribuida que no fueron resueltos hasta la llegada de Bitcoin. En segundo lugar, basan su operativa en criptografía con el objetivo de hacer seguras las transacciones ya que no hay una tercera entidad de confianza que pruebe que las partes de la transacción son quienes dicen ser.

Estas criptomonedas surgen a imagen y semejanza de Bitcoin y solucionan los problemas existentes en computación distribuida gracias al concepto de blockchain o cadena de bloques.

El resto de casos de uso de blockchain tienen que ver con las características observadas en Bitcoin y conservadas en otras blockchain: inmutabilidad, descentralización y no repudio.

La primera y la tercera hacen que esta tecnología sea especialmente atractiva en el mundo del derecho, ya que los contratos podrían quedar plasmados de forma virtual de forma inamovible. Se están creando proyectos de jurisdicciones online supranacionales.

Fomentando la descentralización surgen otros casos de uso como en el mercado de la energía, donde un sistema con múltiples nodos podría demostrar cuánto está aportando a la red eléctrica y por tanto ser recompensado en consecuencia.

Hasta ahora, lo más desarrollado ha sido:

- Identidad digital
- Votación
- Notaría
- Inmobiliario
- Cadena de suministros

- Liquidación y compensación bancarias
- Otros sistemas para los que se puedan escribir en un smart contract unas reglas acordadas por distintas partes.

2.4.5. Blockchain que mejor se adapta a distintos casos de uso

3. Parte práctica: diseñar un sistema informático apoyado en blockchain para el sistema educativo

Las instituciones educativas suelen esforzarse en dar todo a los alumnos, pero sin los alumnos. Estructuran la forma de transmitir el conocimiento, realizan sus investigaciones, debates, acuerdos, pero la sensación del alumnado es que solo se cuenta con él para realizar alguna encuesta. Les dan lo que creen que es mejor para ellos y ellas, pero no les dan el papel protagonista de dirigir su propia educación.

Esto puede tener dos motivos principales. Por un lado, se puede argumentar que los alumnos no están aún lo bastante formados como para decidir sobre su futuro, por lo que gente más preparada debe decidir en su lugar. Por otro, la sensación entre el profesorado es muchas veces que el alumnado no quiere participar cuando se le pregunta.

Sin embargo, estos dos motivos se relacionan: el profesorado no da al alumnado el papel protagonista y por tanto el alumnado no ve la mejora de su educación como algo que le corresponde, mostrándose más pasivo. El paternalismo lleva a la pasividad.

El objetivo principal de la metodología Efac es conseguir el protagonismo del alumnado en el sistema educativo, fomentando el aprendizaje independiente y la colaboración mediante la transmisión de lo aprendido.

Crear un método autosostenible en el que el alumnado se convierte en profesorado dando clase a sus compañeras y compañeros, en pequeños grupos de 5 a 8 personas, aumentando la responsabilidad sobre su propio trabajo, fomentando el espíritu crítico y otras competencias como el trabajo en equipo.

Esta metodología requiere que previamente se haya desarrollado el aprendizaje independiente del alumnado desde edades tempranas, realizando una transición a la metodología Efac en secundaria y adoptándolo como hábito hasta el final de la vida de las personas, y no hasta que se deja de pertenecer a una institución educativa. De esta forma también se fomenta la educación permanente o *lifelong learning* (Medel-Ationuevo, Ohsako, and Mauch 2001).

Vivimos en la sociedad de la información, ya es hora de que vivamos en la sociedad del conocimiento.

Por otro lado, ¿sería posible que, una vez alcanzada cierta edad, pudiesen decidir sobre la forma en que quieren ser educados, por ejemplo decidiendo la metodología que prefieren? Clase magistral, cooperativa, colaborativa, aula invertida… Para ello sería necesario dar una imagen fiel de cada una de estas metodologías, con sus fortalezas y debilidades, y a su vez acompañar al alumnado a lo largo de su paso por el instituto para que cuando quiera cambiar de metodología pueda hacerlo. De hecho, podría ser interesante pasar por distintas metodologías para tener una experiencia propia.

3.1. Análisis sistema educativo

En primer lugar, este análisis no es el objeto principal del trabajo puesto que la formación de quien escribe esta tesis no está centrada en el ámbito de la educación, sino en el de la informática. El análisis histórico de la siguiente sección pretende dar una idea general de la evolución de la educación, pero carece de la rigurosidad que podría tener un texto especializado. Sin embargo, cualquier alumno puede percibir la infravaloración de las TIC en el sector educativo público.

Los avances en educación durante las últimas décadas han sido notables, especialmente en lo relativo a habilidades y competencias adquiridas, más allá del conocimiento. Entre ellos se ha fomentado el trabajo en equipo, el aprendizaje por proyectos, la exposición oral, etc.

En el ámbito TIC, el sector educativo ha ido introduciendo poco a poco plataformas virtuales como moodle. Se han utilizado como repositorios de apuntes y para hacer

entregas de trabajos en su gran mayoría, aunque también ha habido profesores que han buscado sacar mayor rendimiento a las plataformas y han realizado tests online, foros y otras herramientas existentes.

3.1.1. Evolución histórica de la enseñanza

En la antigüedad la transferencia de conocimiento era limitada, por lo que la forma en que se transmitía era jerárquica, de una persona con experiencia en un tema a otra sin ella, normalmente mediante comunicación verbal. Esta forma de transmitir información resultaba la más eficiente ya que los manuscritos resultaban caros, aunque éstos también eran muy relevantes. En la antigua Grecia ya discutían diferentes formas de aproximarse al conocimiento, pero siempre poniendo el foco en la relación maestro-alumno.

Con la llegada de la imprenta, el acceso al conocimiento se democratizó en parte, ya que permitía reproducir bastantes copias de libros. Gracias a ellos, distintas personas podían formarse sin necesidad de comunicación verbal y las limitaciones que ésta tenía: coincidir en un mismo lugar geográfico y disponer de tiempo que poder gastar en común.

De esta forma, algunas personas de cada pueblo o ciudad leían estos libros y podían conocer las bases de materias como filosofía, matemáticas, lengua… o especializarse en ellas. Una vez aprendida la lección, podían enseñársela a otros. Sin ser historiador y sin ánimo de ahondar más en el tema, es fácil extrapolar esta forma de enseñar a la estructura profesor/a -> alumno/a[2] que todavía puede observarse en las escuelas, de manera que el alumno sin acceso al conocimiento puede adquirirlo a través de una persona que se lo transmite, en aulas de varias personas para economizar el tiempo.

Agrupando a personas por edades y dando las mismas lecciones a todos en función de su edad se consigue una escuela o un sistema educativo en el que la transmisión del conocimiento tiene unos resultados muy aceptables comparado con la población analfabeta que existiría sin el sistema y teniendo en cuenta el objetivo de formar a buena parte de la sociedad. Por contra, ya que tan solo el profesor posee el

[2] En adelante se usará el masculino por economía del lenguaje aunque no sea lo más correcto, es necesario que la RAE proponga una solución más justa

conocimiento o el acceso a los libros, se convierte en la única fuente confiable y los alumnos no tienen la posibilidad de contrastar la información.

Por supuesto, no todos los alumnos asimilan la información a la misma velocidad. Algunos alumnos necesitan más tiempo, otros menos. La única versatilidad que ofrece este sistema es dedicar más horas de estudio con el profesor, si tiene tiempo, o repetir curso si no se han alcanzado los objetivos previstos.

Con las mejoras en la eficiencia de las imprentas se democratizó aún más el acceso a libros de texto. Por otro lado, reconociendo el valor que tenía el conocimiento para las personas y la sociedad en su conjunto, los gobernantes impulsaron sistemas educativos cada vez más efectivos. Toda persona que acudía a su lugar de enseñanza podía contar con su propio libro, sin embargo el sistema venía heredado de años atrás y se mantuvo el esquema de clase magistral

……

…….

El sistema educativo actual establece una relación

EFAC ()

3.1.2. Modelos y metodologías

3.1.2.1. Modelos educativos

En el mundo académico se pueden encontrar varios modelos educativos. Cada uno de ellos pone el foco en aprendizajes distintos por lo que tienen puntos fuertes y débiles. A continuación se resumen brevemente los más conocidos:

- Modelo tradicional: el más antiguo, se basa en la transmisión de conocimientos del docente al alumnado. El foco está en la labor del docente poseedor del conocimiento que deberá inculcar al alumnado de una manera activa. Este último, por su parte, mantiene un rol pasivo y se limita a escuchar y a asimilar el conocimiento.

Si pensamos que la educación se limita al conocimiento adquirido y dejamos de lado las habilidades o actitudes, el modelo tradicional puede ser útil ya que dedica todo el tiempo disponible a transmitir conocimientos. Una profesora o profesor con motivación puede impartir clases realmente ilustradoras.

Sin embargo, no se puede pasar por alto la actitud pasiva que este modelo enseña al alumnado, ni tampoco la falta de habilidades para desenvolverse en la sociedad actual.

Además, no se puede pedir al profesorado que después de 20 o 30 años enseñando mantengan la misma ilusión del primer día. Esa desmotivación existente en ocasiones entre el profesorado se transmite hacia el alumnado.

- Modelo conductista: basado en la escuela psicológica del conductismo de B.F. Skinner, utiliza la repetición de conductas como manera de alcanzar las habilidades o conocimientos que se pretenden transmitir. Al igual que el modelo tradicional, el docente asume un papel activo mientras el alumnado se limita a recibir información, repetirla y memorizar.

  Este sistema emplea castigos y recompensas como estímulo, a discreción del docente. Una vez más, se pone el foco en el profesorado.

- Modelo constructivista: en este modelo, si bien existe transmisión de conocimientos por parte del docente, la relación con el alumnado cambia. El error se convierte en protagonista y hace que la relación docente-alumnado se torne en un diálogo: los errores del alumnado son interpretados por el docente como indicadores para redireccionar el proceso de aprendizaje.

  El conocimiento se construye de una manera más gradual pero de la mano del propio estudiantado. Como contra, este modelo presupone la predisposición del alumnado por aprender, algo que no se da siempre y menos aún cuando se parte de otro modelo en el que los alumnos son pasivos.

- Modelo proyectivo: el docente propone líneas de trabajo y es el propio alumno quien desarrolla proyectos siguiendo estas líneas. El profesorado actúa de apoyo mientras que el alumnado es libre de indagar hasta donde quiera, siempre en la línea de trabajo propuesta por el docente.

  El alumnado tiene un papel mucho más activo y toma sus propias decisiones mientras que el docente le guía y acompaña.

- Modelo Sunbury: el papel del alumnado es totalmente protagonista. La base es que el propio alumno descubra por sí mismo qué tiene que hacer. Mientras tanto, el docente le acompaña pero en ningún momento le indica el camino a seguir como ocurría en el modelo proyectivo.

Del primero al último, la gran diferencia de estos modelos es el rol del alumno, desde lo más pasivo a lo más activo. Podría pensarse que en los primeros modelos se transmite conocimiento y en los últimos se transmite motivación para adquirir conocimientos por voluntad propia.

Si bien en la antigüedad los conocimientos que necesitaba la población eran estáticos y no evolucionaban demasiado, en este siglo el conocimiento evoluciona con rapidez. Por tanto, antes se podía poner el foco en transmitir conocimiento pero ahora parece mejor opción poner el foco en inculcar esa voluntad de aprender por uno mismo. Es importante que los alumnos no salgan de una institución educativa con la sensación de que saben todo lo que necesitan saber, sino con la idea de que van a necesitar seguir formándose en su día a día, y con las herramientas para hacerlo.

Esto se llama educación permanente o *lifelong learning* (Medel-Ationuevo, Ohsako, and Mauch 2001). Para conseguirlo, un alumno activo parece más capacitado que un alumno pasivo.

3.1.2.2. Metodologías de enseñanza y aprendizaje

Por otro lado, existen multitud de metodologías educativas que permiten llevar a la práctica los modelos anteriores. Algunas de las más interesantes son la clase magistral, el aprendizaje cooperativo, el aprendizaje colaborativo, el aula invertida y el aprendizaje entre iguales. Se van a analizar brevemente con objeto de ser utilizadas en el modelo propuesto Efac.

La clase magistral consiste en la transmisión por parte del profesorado de conocimiento al alumnado, mediante exposición oral y de forma unidireccional. En Propuestas para la renovación de las metodologías educativas (Consejo de Coordinación Universitaria 2006) se exponen las principales fortalezas y debilidades de esta metodología:

Fortalezas	Debilidades
● Permite una estructura organizada del conocimiento. ● Favorece la igualdad de relación	● Fomenta la pasividad y la falta de participación del estudiante. ● Dificulta la reflexión sobre el

con los estudiantes que asisten a clase. ● Favorece la asimilación de un modelo consolidado en cuanto a la estructura y dinámica de la clase. ● Permite la docencia a grupos numerosos. ● Facilita la planificación del tiempo del docente.	aprendizaje. ● Provoca un diferente ritmo docente/ discente. ● Desincentiva la búsqueda de información por el estudiante. Limita la participación del estudiantado. ● No favorece la responsabilidad del estudiante sobre su propio proceso de formación.

Tabla. Fortalezas y debilidades de la clase magistral

En cuanto a los aprendizajes cooperativo y colaborativo, ambos tienen en común el uso del trabajo en equipo, es su elemento principal. Buscan acabar con la individualidad y enseñan al alumnado a interactuar con otras personas para conseguir un objetivo en común.

Sin embargo, existen diferencias importantes en la puesta en práctica de este trabajo en equipo. Las resume de una manera clara (Edmundo Urra Osses 2014) en la siguiente tabla:

CARACTERÍSTICAS	TRABAJO COLABORATIVO	TRABAJO COOPERATIVO
EL PROFESOR O FACILITADOR	Acompaña como mediador.	Estructura el trabajo del grupo.
TAREA	Se define por los miembros del grupo.	Es asignada por el profesor.
RESPONSABILIDAD POR LA TAREA	Individual y grupal.	Cada miembro del grupo es responsable por una parte de ella.
DIVISIÓN DEL TRABAJO	Realizan los trabajos juntos. Existe baja división del trabajo.	Cada miembro del grupo se responsabiliza por una parte de la tarea.
SUBTAREAS	Entrelazadas. Requieren trabajo conjunto.	Independientes.
PROCESO DE CONSTRUIR EL RESULTADO FINAL	Miembros del grupo con el acompañamiento del profesor.	Asumida por el profesor al estructurar el trabajo de alguna manera que le hace al pensar que el grupo aprenderá.
TIPO DE CONOCIMIENTO	No fundamental, se requiere razonamiento, cuestionamiento.	Básico, fundamental. Privilegia la memorización y en pocas ocasiones tendrá cabida el cuestionamiento.

Tabla. Características diferenciadoras del Trabajo Colaborativo y Trabajo Cooperativo

El hecho de que existan estas diferencias no quiere decir que exista disputa entre las dos metodologías, normalmente el aprendizaje cooperativo se dará en primer lugar y,

una vez el alumnado esté cómodo trabajando en equipo, ya puede evolucionar hacia un aprendizaje colaborativo.

Por otro lado, aula invertida o *flipped classroom* (Jacob Bishop and Matthew A Verleger Jun 23, 2013, 23.1200.1) es una metodología que desplaza del aula a casa las clases teóricas, normalmente grabadas en video, además de las actividades que el docente considere oportunas: todas las que se pueden realizar de manera individual y no requieran de interacción humana. El tiempo en el aula se dedica a actividades a las que sí aporta valor estar reunidos: debates, proyectos, ejercicios interactivos, etc.

La tutoría entre iguales o *peer tutoring* (Topping 2015, 1-29) pone en contacto dos o más alumnos de la misma o distintas edades de forma que uno enseña al otro. Se produce una relación *win-win*: una parte obtiene apoyo y la otra aprende a enseñar, a explicarse, además de afianzar conceptos.

Puesto que la propuesta educativa desarrollada en este proyecto es integral y afectaría a todas las asignaturas de varios niveles educativos, es positivo realizar un mix entre todas las metodologías nombradas anteriormente.

3.1.3. Blockchain en educación

La aplicación de la tecnología blockchain a la educación ya ha recibido la atención de algunas autoras y autores.

La primera idea que viene a la mente cuando se piensa en aplicar esta tecnología es la de un pasaporte educativo (Gräther et al. 2018). Las instituciones educativas actualizan este pasaporte con las calificaciones y logros del alumnado de manera pública, de forma que le acompaña durante su vida laboral como un curriculum estandarizado por todas las organizaciones de un país o del mundo.

En segundo lugar, blockchain puede facilitar un sistema de recompensa. En *The Blockchain and Kudos* (Sharples and Domingue 2016) se habla de *learning is earning* o aprender es enriquecerse, una frase que resume el uso de kudos, una criptomoneda creada en el proyecto, para obtener recompensas por el esfuerzo realizado.

En *Exploring blockchain technology and its potential applications for education* (Chen et al. 2018, 1-10) se comentan otros usos que podría tener la tecnología blockchain. Por ejemplo, en el aprendizaje colaborativo resulta a veces complicado realizar una evaluación justa de los individuos que componen el grupo, precisamente porque este tipo de aprendizaje pone en gran valor el trabajo del grupo y no el individual. Con

blockchain, todas las interacciones de los integrantes podrían quedar grabadas y realizar así una evaluación más justa.

También se propone usar blockchain para asegurar que los procesos de supervisión del alumnado y otras medidas que se toman desde las directivas de las instituciones llegan realmente a cumplirse, quedando grabadas en un registro imborrable.

Otros casos de uso que se contemplan en *Blockchain-Based Applications in Education: A Systematic Review* (Alammary et al. 2019, 2400) como por ejemplo:

- firma digital para excursiones y otras actividades que requieran consentimiento parental
- derechos de propiedad en libros de texto en formato ebook y otros materiales didácticos
- revisiones de exámenes

Como se puede ver, son muchas las propuestas para el uso de la tecnología blockchain en el sistema educativo.

3.2. Diseño del modelo educativo Efac

Tomando como base los modelos y metodologías mencionados en Modelos y metodologías, se va a proponer un nuevo modelo que sea útil para el sistema educativo y sobre el cual se diseñará el sistema informático.

El motivo de esta propuesta es proporcionar un modelo que se adecúe:

- al estado del arte de la tecnología, que ofrece posibilidades tangencialmente distintas a las de las décadas pasadas.
- a la actualidad social, con unas nuevas generaciones que han crecido en la colaboración, no en la competencia, y en la cultura de las redes sociales por lo que utilizan las conexiones virtuales con la misma naturalidad que las interacciones físicas.
- a los retos de la educación de este siglo, pasando desde la necesidad de competencias transversales hasta el lifelong learning.

Los modelos en los que se inspira el propuesto, al que se ha nombrado Efac, son los que intentan hacer del estudiante una persona más activa, capaz de construir su propio conocimiento.

Para el uso de este modelo se van a distinguir dos fases educativas:

1. Secundaria, donde los alumnos ya han aprendido a realizar un aprendizaje autónomo y comienzan a relacionarse de una manera más reglada con el conocimiento.
2. Educación superior: universidad, formación profesional en sus ciclos de grado superior, etc. En esta fase se va a incluir a las personas egresadas puesto que el propósito de Efac es que pueda ser continuado a lo largo de toda la vida del individuo.

Es un requisito que los alumnos se inicien en el modelo Efac solo cuando sean capaces de aprender por sí mismos. Por ello la educación primaria debe estar encaminada, como hasta ahora, a este propósito.

Este proyecto se va a basar en el modelo propuesto por Silva y Maturana en su *Propuesta de modelo para introducir metodologías activas en educación superior (Silva Quiroz and Maturana Castillo 2017, 117-131)*:

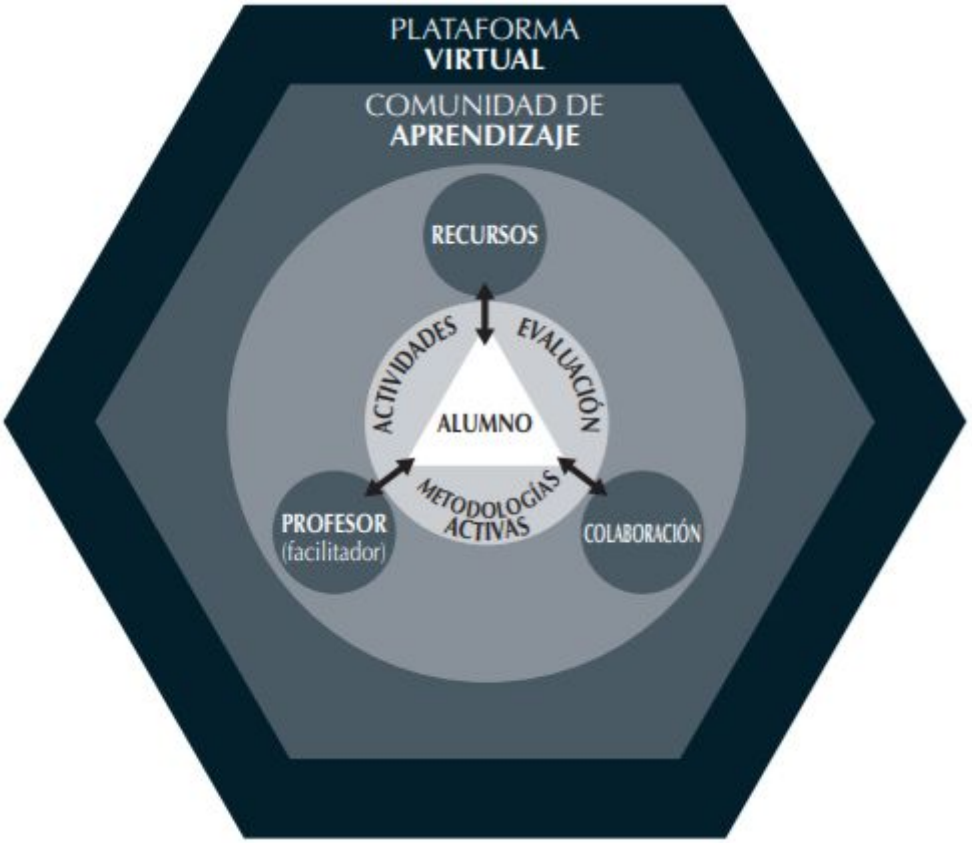


Figura. Modelo de metodologías activas centradas en el estudiante

Con esta base, se va a proponer un modelo que integra las metodologías comentadas en Metodologías de enseñanza y aprendizaje de una forma práctica y se va a

desarrollar el sistema informático que le dé soporte. Todo lo que aquí se propone es susceptible a cambios, mejoras y discusiones.

3.2.1. Fundamentos

En la primera fase, correspondiente a la educación secundaria, el modelo Efac propone la siguiente aplicación práctica de las metodologías educativas:

1. AULA INVERTIDA: el profesorado prepara los contenidos de la asignatura y los separa en bloques bien definidos que se estudian fuera del aula, antes de que se trabajen en clase. Aporta videos, libros de texto y cualquier material que crea oportuno, siendo lo ideal que todos los alumnos de la clase tengan una misma imagen de los contenidos, con objeto de realizar una evaluación justa.

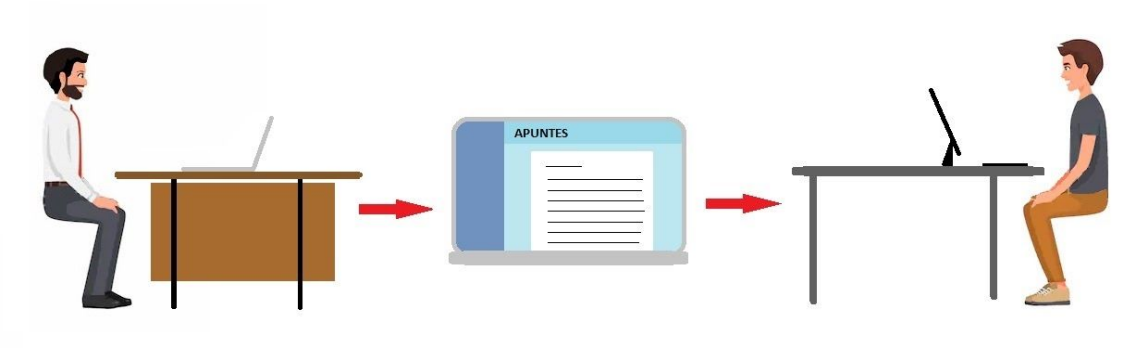


Imagen. Profesor elabora y sube apuntes completos para alumnos (Elaboración propia)

Si bien el alcance de estos contenidos está limitado a los objetivos de aprendizaje de cada asignatura y determinados, por ejemplo, por la información que aparece en el libro de texto, la persona docente (en adelante *"la docente"*) tiene libertad para aprovechar el tiempo en el aula para explotar la versión más creativa del alumnado. De esta forma, en la segunda mitad de la clase, la docente puede aplicar aprendizaje basado en proyectos, en problemas o cualquier otra metodología durante ese tiempo de clase que tiene disponible.

2. APRENDIZAJE COOPERATIVO: en la primera mitad de la clase, el alumnado es protagonista. Trabajando en grupos autónomos de 5 a 7 personas, una de ellas (a la que se llamará alumna-docente) estudia con mayor profundidad el temario que corresponde a esa clase y se lo explica al resto.

Imagen. Alumno dando clase a su grupo (Elaboración propia)

Cada persona del grupo tendrá su turno, en el que explicarán los contenidos correspondientes. La persona docente -el hombre de blanco en este caso- se unirá a los grupos el tiempo que considere necesario para conocer al alumnado y ayudarles a mejorar, intentando interferir lo menos posible.

Puesto que los contenidos de una clase normalmente se basan en los de clases anteriores y a su vez son base para las siguientes, el grupo tiene un incentivo en que cada clase sea lo más correcta posible. El *pasotismo* de algún compañero implica tener que estudiar más en casa. Los alumnos llegan a estas conclusiones por sí mismos basándose en su propia experiencia en los grupos.

Más allá de que se implementen sistemas de recompensa, feedback, etc. cada persona del grupo se fijará en lo que les gusta -y lo que no- de sus compañeros al explicar, mejorando en todos esos aspectos. Si es posible, con el apoyo de la docente trabajarán uno a uno en las dificultades individuales para asegurar una correcta evolución.

3. CLASE MAGISTRAL: la clase magistral la imparte el propio alumnado. Su exposición del temario puede ser detallada o puede ser un resumen, con objeto de que sus compañeros tengan una primera visión general.

   Al tomar el rol docente aumenta su responsabilidad sobre los contenidos, asumiéndolos como propios. De esta forma asimila con claridad los conceptos y aprende a enseñar. El rol pasivo no es inherente al alumnado, se le inculca

en sus años de formación con modelos en los que no toma protagonismo. Dejando que den las clases se les vuelve a confiar el papel principal en la educación.

4. APRENDIZAJE ENTRE IGUALES o peer tutoring: para las dudas que puedan surgir, tanto en la preparación del temario por parte del alumno-docente o del grupo de estudio, lo más conveniente sería una vez más contar con alumnos para resolver el problema.

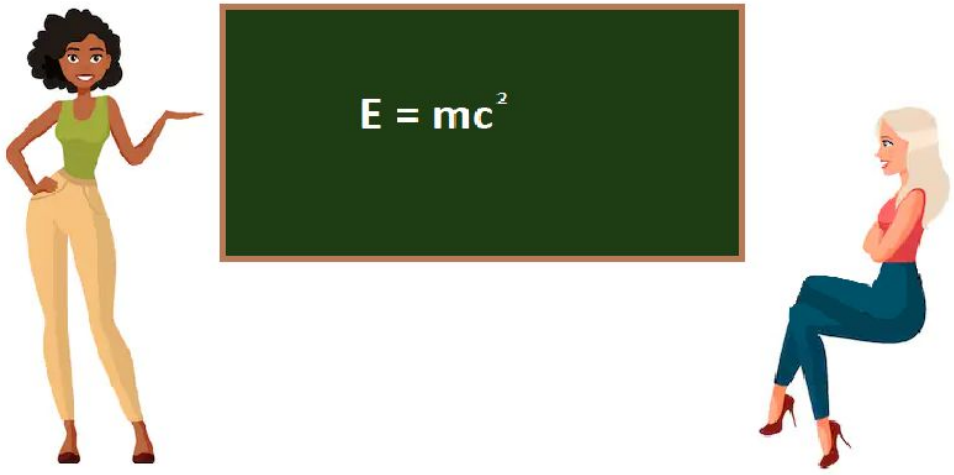


Imagen. Dos alumnas realizan una tutoría (Elaboración propia)

Cada grupo podría ser tutorizado por un alumno-docente de un curso superior, que afianzaría aún más los conceptos. La elección de qué persona debe actuar de apoyo para cada grupo debería corresponder a las docentes de ambas clases que, conocedoras de las aptitudes de su alumnado, priorizarán a alumnos más solventes, alumnos que necesitan repasar un poco las lecciones, etc.

También podría ser abierto y que cualquier persona pudiese tutorizar, fomentando así hacer públicas las dudas, igual que se hace en foros de internet.

Además, se introduce una figura complementaria: el alumno-supervisor (superV). Este supervisor no pertenece a la clase del alumno pero está presente en el día a día, chequeando sus progresos.

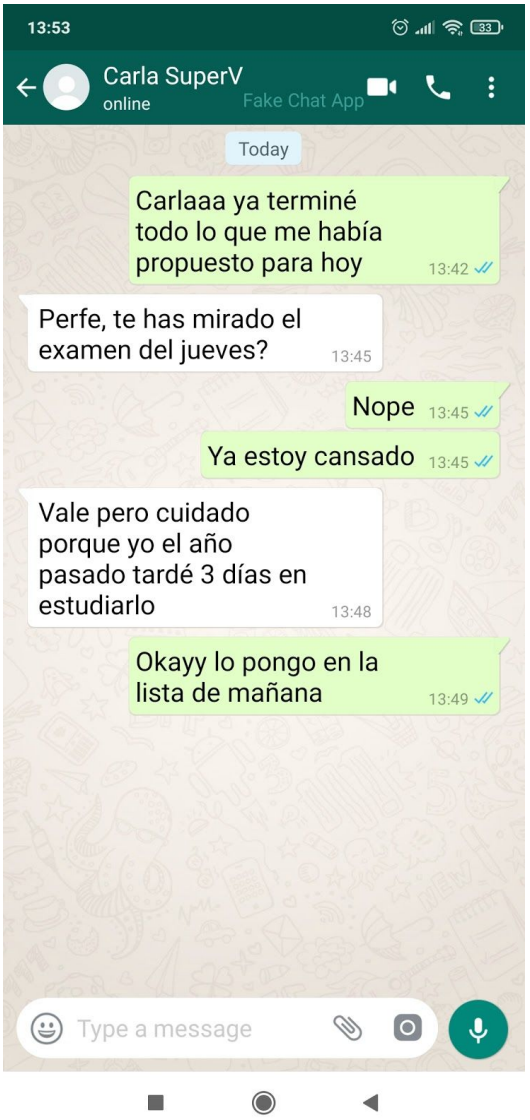


Imagen. Elaboración propia

Realiza un mentoring sincero desde una perspectiva familiar pero distante, por ejemplo siendo alumno de un curso superior o incluso de otra institución educativa. Se ha enfrentado a los mismos problemas y actúa como apoyo moral. Una guía con consejos sobre el aprendizaje entre iguales o P2P puede encontrarse en opencolleges.edu.au/informed/features/peer-teaching/.

Conforme a los anteriores 4 puntos, el alumnado rompe con la idea de que el conocimiento viene de una docente experta y comprende que cualquier persona puede convertirse en experta dedicando tiempo al estudio. Y es que cada alumno es experto en la materia que imparte, a ojos de quien todavía no ha alcanzado ese conocimiento.

3.2.2. Modelo evolucionado para educación superior

El nivel de independencia presupuesto en el alumnado de educación superior es mayor que el de educación secundaria. Como consecuencia, existen ciertos cambios en el modelo:

1. AULA INVERTIDA: se proponen dos alternativas, a elección de la docente o de un acuerdo entre docente y alumnado:
    a. La docente sigue preparando los contenidos de la asignatura pero deja que sea el alumnado quien elabore el contenido audiovisual. El alumno da la clase fuera del aula, al contrario que en secundaria, a través de un vídeo preparado que su grupo puede ver de forma asíncrona.
    b. La docente se limita a ofrecer un guión o unas pautas, siendo el propio alumnado quien desarrolla los contenidos que ofrecerá a su grupo, fomentando así el aprendizaje autónomo. Este formato podría ser usado en asignaturas optativas, ya que se imparten en los últimos años de los estudios superiores: con esta metodología el alumnado empieza a ser consciente de que el conocimiento no está limitado a lo que le entregan los profesores, sino que abarca todo aquello que les produzca interés y pueden construir el conocimiento por sí mismos.

    Es un empleo más ortodoxo del aula invertida, puesto que toda la carga teórica se produce fuera del aula y el tiempo en el aula se aprovecha para debates, proyectos u otras actividades para las que estar reunidos resulta más útil.

2. APRENDIZAJE COLABORATIVO: Frente al aprendizaje cooperativo de niveles inferiores de enseñanza, se da un aprendizaje colaborativo. Los alumnos ahora siguen trabajando en sus grupos, pero crean un grupo adicional de evaluadores donde toman decisiones y actúan en conjunto, como se explica en Evaluación. Adicionalmente, si es el alumnado quien elabora el contenido, lo hará formando un equipo en el que estén todos los alumnos-docentes que fuesen a impartir la lección en el que actuarán de forma colaborativa.

    La docente mantiene una presencia lateral, al mismo nivel que el alumnado. Les alienta a colaborar y a tener curiosidad. No acude a clase a explicar la misma lección durante 10 años sino que acude a disfrutar y a transmitir toda la energía que pueda transmitir.

3. CLASE MAGISTRAL: Las nuevas generaciones han aprendido a través de vídeos durante buena parte de su vida y la creación de este tipo de contenidos es una competencia necesaria hoy por hoy. Sea de calidad o no, el vídeo sirve al alumnado para aprender a estructurar el conocimiento y mejorar su expresión oral.

   En vez de impartir la clase de manera síncrona como se hacía en secundaria, lo harán de forma asíncrona. Con esto dan la posibilidad a su grupo de que estudien la lección en el momento propicio para ellos, ya sea por la mañana, tarde o noche. No podrán posponer mucho su estudio debido al sistema de evaluación propuesto en el siguiente apartado.

   Por supuesto, aunque la creación del contenido sea asíncrona, el visionado de ese contenido se puede realizar de forma síncrona. Por ejemplo, en los grupos donde crean que es mejor para ellos tener un horario bien marcado, programarán el visionado para hacerlo en conjunto.

4. APRENDIZAJE ENTRE IGUALES o peer tutoring: continúa igual que en secundaria, con alumnos que ya hayan superado las asignaturas.

3.2.3. Evaluación

La evaluación es clave para aumentar el nivel de responsabilidad del alumnado sobre su propio trabajo. Los conocimientos de los estudiantes pueden seguir evaluándose como hasta ahora, a base de exámenes, trabajos o cualquier otro método considerado por la docente. Adicionalmente, se va a añadir una evaluación diaria que no tiene por qué implicar trabajo de la docente ni contar para la nota de la asignatura.

El modelo Efac requiere un estudio constante, al menos en la parte teórica, ya que en muchas asignaturas resulta imposible explicar los contenidos si no se tienen claros los inmediatamente anteriores. Es necesario que los alumnos tengan motivos para llevar al día sus asignaturas y uno de los métodos más efectivos para esto son los exámenes.

Sin embargo, no se pretende sobrecargar a las docentes, por lo que esta evaluación va a corresponder a los propios alumnos (al igual que la impartición de las clases teóricas). Para cada lección impartida de una asignatura, los alumnos-docentes preparan de forma colaborativa una serie de preguntas y sus respuestas para la

posterior autoevaluación del resto de alumnos de la clase. Puede ser en formato test o en cualquier otro, en plataforma online o presencial.

Una opción extra sería dar acceso a las nuevas lecciones a quienes hayan aprobado las lecciones anteriores. Se estudiará su posible implementación en el sistema informático como una técnica de Gamificación.

3.2.4. Incentivos

El uso de técnicas que incentiven la buena marcha de los grupos puede ser una ayuda. Especialmente en secundaria, el alumnado aún necesita aprender a colaborar, a premiar a quienes más aportan y a pedir mayor colaboración a quienes ralentizan al grupo a propósito.

Para esto existen multitud de ideas a disposición de la docente y de los grupos. Una idea podría ser un sistema de feedback instantáneo con tarjetas que puedan utilizar los miembros del grupo :

- Tarjeta roja: los alumnos que reciben la clase magistral sacan la tarjeta roja cuando otro alumno interrumpe la clase magistral.
- Tarjeta amarilla: sirve como aviso.
- Tarjeta verde: se la entregan al alumno-docente cuando ven que se está desviando del tema.

Otro feedback instantáneo que podría usar la docente, o un grupo de evaluación formado por docente y alumnado-docente, sería puntuando cada parte del vídeo como básica, avanzada, interesante pero desviada del temario o de cualquier otra forma que se les ocurra.

Como no es el objeto de este trabajo, no se va a profundizar en estas técnicas. Lo que sí es necesario proponer, con objeto de que el alumnado sepa dónde puede mejorar, es un sistema de feedback a largo plazo. Además, para premiar los comportamientos que se consideren positivos, es necesario un sistema de recompensa que pueda implementarse en el sistema informático. Se desarrollarán en el apartado Sistema de feedback y recompensa.

3.2.5. Consideraciones

Los vídeos subidos por el alumnado en el sistema informático estarán accesibles únicamente para alumnos logados y por tanto cumplirán con el Reglamento General de Protección de Datos (RGPD). Sin embargo, nada impide a los mejores creadores de contenido subir sus propios vídeos en abierto a alguna plataforma como Youtube, con lo que esa información pasaría a ser pública.

Un miedo que quizá tienen las universidades presenciales respecto a impartir clases online abiertas y gratuitas es la falsa sensación de que matricularse deja de ser necesario. Esto podrían pensar especialmente las universidades que siguen el modelo privado británico o estadounidense, donde se difunde el mensaje “el conocimiento tiene un precio”. También universidades españolas pueden temer esa desbandada.

Sin embargo, liberar contenidos gratuitos y de calidad permite a las universidades posicionarse. De esta forma, el estudiantado elegirá universidad en función de la calidad de lo que ésta muestra en los vídeos de sus asignaturas, tomándolo como muestra de la calidad que espera recibir de la propia universidad.

Si bien puede ocurrir que algún estudiante decida no matricularse y seguir la universidad solo a través de vídeos, a largo plazo verá incentivos por obtener el título y buscará ingresar en la universidad. Si bien el alumnado no es consciente cuando entra a la universidad, los conocimientos son solo una parte de lo que se aprende en la etapa universitaria.

El estudiantado busca la universidad porque es un espacio de conocimiento e ideas, pero ese espacio no tiene por qué ser físico. Tener el contenido teórico online facilita el aprendizaje independiente del alumnado y permite a las instituciones y al profesorado centrarse en los debates, prácticas, evaluaciones y otros métodos pedagógicos que pueden desarrollar en las clases.

Por otro lado, hay que considerar que existe la posibilidad de que el comportamiento no sea el idóneo, especialmente en grupos de personas que nunca han sido tratadas como adultas. Aún existiendo un sistema de reseñas, es difícil o casi imposible saber si las tutorías se están dando de la manera propicia o si grupos de amigos se están dando buenas notas de manera interesada.

Algunas alumnas podrían pensar, por tanto, que su tiempo se ve recompensado de la misma forma que el tiempo de quien realiza una tutoría dedicando mucho menos esfuerzo o calidad de enseñanza. Sin embargo, es importante que los alumnos

entiendan que todo lo bien que expliquen o realicen cualquier actividad repercute directamente en su futuro, y su esfuerzo es muy valioso tanto para la gente a quien ayudan como para sí mismos.

Por tanto, los sistemas de recompensa o feedback que se planteen, así como cualquier actividad que no pueda ser evaluada de manera objetiva y cierta, deben servir al estudiante únicamente para conocerse a sí mismo, y nunca ser objeto de competición entre alumnos.

3.2.6. Lifelong learning

Con este modelo, el aprendizaje a lo largo de la vida se fomenta debido al hábito adquirido de realizar sesiones colaborativas.

Si bien en las primeras etapas educativas las sesiones que imparten los alumnos están limitadas al ámbito de la clase y las asignaturas propias del curso, en etapas posteriores estas sesiones podrían tratar temas que sean interesantes para el alumnado. Por ejemplo, aparte de impartir una sesión del tema 3 de matemáticas, un alumno podría ofrecer una sesión de filtros en Tik Tok. Otra alumna podría dar una sesión de trucos para algún videojuego.

Son temas que en ese momento son interesantes para el alumnado y por tanto empiezan a acudir a estas charlas por *motu proprio.* Es importante que sean ellos mismos quienes quieran ir y no lo vean como una imposición, por eso deben sentir la máxima libertad posible a la hora de elegir el tema de la sesión.

Estas charlas no tienen por qué estar incluidas en el marco académico formal, no son parte de ninguna asignatura, pero sería bueno que contasen con un espacio de tiempo dentro de las horas lectivas -no sería por tanto una extraescolar. Poniendo un ejemplo, podría ser un espacio de media hora después del recreo los viernes, en el caso de educación secundaria. Este horario sería bueno porque algunos alumnos decidirán alargar el recreo pero otros, acostumbrados al horario habitual durante la semana, preferirán acercarse al aula por curiosidad sobre la charla.

No reciben un incentivo por acudir a la sesión, aunque quienes proponen sesiones sí podrían recibir algún tipo de recompensa. Para esto sería necesario un sistema de recompensa global ya que no son sesiones de ninguna asignatura.

Estas sesiones se ofrecen públicamente. Lo mejor sería que existiese una app en la que cada sesión pudiese ser notificada puesto que el alumnado está acostumbrado a usar aplicaciones, ve los correos y por supuesto los tablones de anuncios como

herramientas del pasado y todo lo que les llega por esa vía pierde puntos. Lo que se pretende es motivar al alumnado y no se puede hacer con herramientas desmotivadoras sin una buena experiencia de usuario.

También podrían acudir a impartir sesiones personas ajenas a los centros, especializadas en temas de interés general.

Puesto que el formato de sesiones que propone Efac es dinámico y durante la etapa educativa se toma el hábito de acudir a sesiones por voluntad propia, es más fácil que al dar el salto a la siguiente etapa educativa se apunten a todas las charlas que les interesen, cada vez más relacionadas con su campo de especialización:

- Al pasar de secundaria a educación superior, irán viendo charlas más relacionadas con su campo.
- Al ser egresados de educación superior, se juntarán en función de su especialización o interés profesional.

Mientras puedan proponer y recibir estas sesiones, algo que no acaba cuando se abandona la institución educativa, las personas continuarán formándose y compartiendo el conocimiento creando una sociedad culturalmente más rica.

Además, esto hace que las universidades y otras instituciones educativas tengan una gran presencia en la vida posterior de las personas ya que, por su labor en la sociedad, las sesiones que aquí se impartan actuarán como referente a la hora de impartir estas charlas.

3.3. Aplicación del sistema informático como soporte al sistema educativo

Se plantea una primera iteración del diseño del sistema de información que va a dar soporte al modelo educativo Efac. El diseño que se pretende conseguir define desde una perspectiva global el sistema, analizando los requisitos y los elementos que serán necesarios pero sin entrar en detalles de implementaciones software o de bases de datos.

El ámbito del sistema de información es el propio de un sistema educativo, engloba a los actores principales y toda la información que pueda ser utilizada para conocer o mejorar su desempeño. Se incluyen las calificaciones obtenidas en los métodos de

evaluación formales, las reseñas y feedback de los compañeros, el número de tutorías impartido por un alumno y cualquier otra información que pueda ser relevante.

El objetivo de este sistema de información es servir tanto a cada alumno como al profesorado para la toma de decisiones sobre su desarrollo educativo, así como para generar un entorno más activo entre los estudiantes. También dar soporte a todas las operaciones necesarias para que alumnado, profesorado y otros actores del universo educativo puedan utilizar el modelo Efac, incluyendo el feedback en las clases colaborativas, los sistemas de recompensa, etc.

3.3.1. Análisis

El análisis busca conocer qué tiene que hacer el sistema. Se trata de entender las necesidades del sistema de información y transformarlas en requerimientos del sistema, de la forma más explícita posible para evitar en esta primera etapa los errores que puedan producirse por asunciones o inexactitudes.

Las características del modelo Efac, definidas en el apartado anterior Diseño del modelo educativo Efac, han de llevarse a la práctica con una implementación determinada del modelo educativo. Por tanto, se van a explicar la operativa diaria, los sistemas de feedback y el resto de características del modelo llevándolas al uso concreto en una institución educativa ficticia, siempre consciente de que en algunos casos sería mejor abstraerse para dejar margen a los distintos usos que puedan darle distintas instituciones educativas.

Se van a definir las necesidades que deben cubrir los sistemas de feedback y recompensa, la gamificación o el uso de blockchain dentro de este análisis y no en el apartado anterior porque, aún siendo una parte importante del modelo Efac, son más susceptibles a cambios en las distintas iteraciones del proceso de diseño del sistema de información (en futuros trabajos).

Todo lo que se proponga estará enfocado a proporcionar una solución que no tiene por qué ser la óptima y por tanto es susceptible de ser mejorada ante cualquier propuesta.

3.3.1.1. Operativa diaria

Son varios los grupos involucrados en este sistema de información:

- El alumnado
- El profesorado
- Los administradores del sistema, rol que en la parte relacionada con los alumnos será ejercido por una docente
- Los representantes de instituciones educativas

El comportamiento de la alumna Alicia en un día normal con el modelo Efac sería:

- En cada clase, recibe o imparte una sesión de cada asignatura en su grupo de 5 a 8 personas.
- En algunos casos, realizará un test preparado por ella o por sus compañeros.
- Realizará otras actividades durante la clase, las cuales dependerán de la docente.
- Puede asistir a sesiones sobre temas que interesantes que no se incluyen en ninguna asignatura -a las que podemos llamar sesiones alternativas- fuera del horario lectivo. Tiene que conocer y ser capaz de apuntarse a esas sesiones, y también puede crearlas.
- Cuando termina el horario lectivo, estudia las sesiones impartidas por sus compañeros ese día y lee el contenido del día siguiente. Prepara las sesiones que tenga que impartir ella y sus correspondientes exámenes y respuestas.
- Imparte las tutorías que le pidan y acude a las que necesita.
- Al final del día, comenta a su alumna-supervisora su progreso brevemente y recibe feedback. Hace lo propio con el alumno a quien supervisa. Una vez a la semana, al mes, al trimestre/cuatrimestre o cuando lo necesite tendrá una charla más larga con él en la que recapitularán un poco sobre sus vidas.
- Tiene un horario/calendario que se actualiza automáticamente donde puede ver todas sus clases, las sesiones alternativas y también las tutorías asignadas.
- Puede acceder a estadísticas y gráficos sobre su rendimiento educativo en los últimos años.

A su vez Próximo, profesor del centro:

- Decide la composición de los grupos, o deja que se formen por sí mismos.
- Da formación a los grupos sobre las mejores prácticas para explicar.

- Monitoriza los grupos y evalúa su comportamiento para identificar actitudes a mejorar lo antes posible.
- Durante el tiempo que tiene disponible de clase, realiza las actividades que considera oportunas.
- Evalúa a los alumnos.

Adriana, la administradora del centro educativo:

- Elige las sesiones alternativas que se van a impartir de entre las ofrecidas por el alumnado.
- Es responsable de formar a profesorado y a alumnado en el uso del sistema.
- Recoge las propuestas y mejoras planteadas por los distintos actores.
- Configura el sistema en función de las peculiaridades del centro.
- Elige las analíticas más representativas para generar los informes de evolución del alumnado que enviará a la responsable de la institución.

Por último Inmaculada, la responsable de la institución educativa:

- Recibe informes de la evolución del alumnado
- Toma las decisiones concretas del centro.
- Emite el boletín de calificaciones.

3.3.1.2. Sistema de feedback y recompensa

Incluir un sistema de feedback para que el alumnado se conozca a sí mismo y un sistema de recompensa para que se sientan a gusto trabajando para los demás -una parte vital del trabajo colaborativo- es una de las necesidades que justifican el uso de un sistema de información.

Comenzando por el sistema de feedback:

1. La alumna Alicia debería ser capaz de:
    a. ver su evolución a lo largo de una asignatura, en el trimestre o a lo largo de su vida como estudiante
    b. conocer la opinión que tienen sus compañeros sobre las sesiones que imparte. A ser posible, el feedback debería estar fundamentado en varios puntos, como la facilidad para entenderla, la calidad de los contenidos, etc.

    c. saber la opinión de cada tutoría que realiza.
    d. si no está de acuerdo con alguno de estos feedback, debe ser capaz de ponerse en contacto con la persona que generó el feedback y pedir una explicación más detallada con el fin de mejorar. De la misma forma, quien puso el feedback debería ser capaz de cambiar su feedback si hubiera sido erróneo.
    e. también debe ser capaz de emitir su feedback sobre los demás.
2. El profesor Próximo:
    a. es mediador en los conflictos que puedan surgir
    b. es espectador en las explicaciones de todos los grupos por lo que al cabo de un tiempo conoce aproximadamente las características de cada alumno. Compara su punto de vista con los feedback que recibe un alumno para detectar desviaciones en los feedback.
    c. también aporta su opinión al alumno cuando le escucha explicar, con opiniones bien fundadas de gran utilidad para el alumno.
3. La administrativa Adriana:
    a. Configurará el sistema de feedback en su centro.
4. La responsable de la institución educativa podría tomar muchas decisiones sobre cómo se recogerá el feedback en su centro, pero para simplificar el sistema, Inmaculada decidirá:
    a. las gráficas que se mostrará al alumnado de entre las que ofrece el sistema.

En cuanto al sistema de recompensa, debe servir como refuerzo positivo para las actitudes que se pretenden potenciar, como ser personas más activas, la solidaridad entre compañeros, etc.

Probablemente no sea buena idea recompensar con beneficios, regalos u otros métodos que puedan generar competencia entre los alumnos. El sistema y la contribución de cada alumno al resto puede, por sí mismo, ser la recompensa si aplicamos el concepto de *social currency* o moneda social: la marca que desprende nuestra persona en redes sociales. Mejorar nuestra marca es una recompensa en sí misma.

1. El sistema de recompensa permitirá a la alumna Alicia:

    a. conocer cuáles son las actitudes y actividades que van a ser recompensadas.
    b. guardar un registro de todo por lo que ha sido recompensada.
2. Próximo:
    a. puede recompensar actitudes positivas que ve fuera del aula. Dentro del aula la recompensa debería ser con nota de la asignatura -o de cualquier otro tipo- pero no con este sistema de recompensa.
3. Adriana:
    a. resuelve los conflictos que pueda haber por el uso fraudulento del sistema de recompensa.
    b. tiene información global y personalizada de las recompensas de los alumnos, la cual podrá analizar para llevar a cabo la tarea del anterior punto a).
    c. configura las especificaciones del centro.
4. Inmaculada, la responsable de la institución:
    a. decidirá cuáles son las actitudes a reforzar, en función del punto de vista filosófico de cada institución.
    b. es responsable de que todas las personas conozcan las actitudes y actividades recompensadas.

Además de lo que se permite configurar a cada institución con el objetivo de personalizar la educación en función de su filosofía, habrá actitudes y actividades recompensadas en todas las instituciones de la misma manera. Esto servirá para generar un estándar y será acordado por todas las personas responsables de la educación pública.

Este sistema debería permitir exportar su información a los alumnos mejor recompensados -por trabajar más para los demás- para que puedan añadirlo a su currículum, ya que dice mucho de ellos. Esto podría provocar competencia, por lo que habrá que revisar con expertos educativos su implementación.

De la misma manera en que se ofrecen recompensas, se podrían poner castigos. Por ejemplo, una acción muy grave podría tener un castigo de un año de *gap* sin registros en el sistema. Esto resulta un castigo grave dado que los registros del sistema proporcionan un currículum, una imagen fiel del progreso del alumno.

3.3.1.3. Gamificación

Utilizar técnicas de gamificación como se propone en “La gamificación como estrategia metodológica en el contexto educativo universitario” (Oliva 2016) puede resultar de gran ayuda.

En este modelo se utilizan, sin poner limitaciones a que en el futuro se utilicen más técnicas, las siguientes:

- bloqueo se sesiones: las sesiones impartidas por los alumnos aparecen bloqueadas. Para desbloquearlas se han de aprobar los test de las lecciones anteriores.
- logros o medallas: impartir cierto número de tutorías, ofrecer por primera vez una charla alternativa, etc. se verían recompensadas con una medalla.
- niveles de expertise: conseguir ciertas medallas haría pasar al alumno de usuario novato a intermedio, experto, embajador...

Los responsables de las instituciones educativas deciden los detalles en conjunto.

3.3.2. Diseño

Tras analizar los requerimientos de la etapa de análisis, se va a proponer un diseño que integre todos los elementos del modelo educativo y dé solución a los requerimientos de los diferentes actores.

3.3.2.1. Uso de blockchain

Habiendo realizado el estudio de blockchain como tecnología en Bases teóricas, así como sus posibles aplicaciones en educación Blockchain en educación, es momento de definir su uso en el sistema.

Se plantean las siguientes CONSIDERACIONES:

1. Cada transacción implica un coste, por lo que el número de transacciones debe ser reducido. El coste de las transacciones en Ethereum es, en promedio, más barato que en Bitcoin y además cuenta con las facilidades que ofrece un lenguaje de programación de alto nivel para smart contracts como es Solidity.
2. A mayor complejidad en la funcionalidad de la parte blockchain, mayor probabilidad de generar fallos en un sistema de almacenamiento inmutable.

Las transacciones que sirvan para guardar información en la cadena de bloques deben ser lo más simples posibles.

3. No se puede pedir a las familias que mantengan un nodo blockchain. Una de las características revolucionarias de Bitcoin, que mantienen blockchain públicas como Ethereum, es prescindir de una tercera parte de confianza. Pero no cualquier persona tiene los recursos para costear un nodo de la red comprobando todas las transacciones, ni conocimientos técnicos para gestionar de manera correcta sus claves de cifrado asimétrico.

   Por ello, los usuarios de este sistema de información sí que van a confiar en la veracidad de la información ofrecida por el sistema (proveniente de blockchain). Si quieren hacer la comprobación, cualquier persona puede acceder a un servicio externo online que lea la blockchain o incluso montar su propio nodo.

4. La información guardada en la blockchain va a ser pública. Si consideramos que este sistema de información puede usarse en regiones en las que está vigente la normativa GDPR (General Data Protection Regulation) donde se garantiza el derecho a la supresión (“derecho al olvido”), ninguna información personal puede almacenarse en blockchain debido a su inmutabilidad.

Teniendo en cuenta estos puntos se propone lo siguiente. Los datos guardados en blockchain serán únicamente los hashes que sirvan para comprobar que un documento existía en el momento de producirse la transacción, a modo de prueba de existencia.

Los documentos serán certificados de notas expedidos por la institución educativa y certificados de los sistemas de feedback y recompensa expedidos por el propio sistema de información. También incluirá un campo que determine si el certificado es válido o no, ya que debido a plagios o conductas poco honestas la institución podría verse obligada a revocarlo.

Para ahorrar costes:

- se utilizará la blockchain de Ethereum, en la que a día de hoy se pueden lanzar transacciones por menos de 1€.
- los certificados se emitirán al final del periodo académico, ya sea el trimestre, cuatrimestre o el año.

Puesto que las transacciones tienen un coste que las instituciones no pueden asumir por cada alumno y periodo académico, se ofrecerán dos opciones al alumnado: a) que paguen una tasa por cada certificado emitido, lo que supondría al alumno pagar 1 ó 2€ por periodo académico; b) agregar un número alto de documentos y utilizar el hash de la agregación, de forma que se prueba que todos ellos existían en ese momento.

Por otro lado, habría que plantear quién firmaría las transacciones. Si bien podrían ser las instituciones educativas, para probar que son ellas las que emiten el certificado, se plantearía una situación parecida a la del punto 3 de las consideraciones ya que cada institución tendría que gestionar las claves, lo que es más propenso a fallos, y añadiría complejidad al sistema.

Lo más sencillo es que la institución emita el certificado y lo suba al sistema, éste le pregunte al alumno que confirme si su certificado es correcto y si lo es el sistema emita una transacción que pruebe su existencia. Se requiere una tercera parte de confianza -que en vez de ser la institución es el sistema informático- pero a cambio se obtiene un registro inmutable con el que poder probar la existencia del certificado.

La funcionalidad descrita solo necesitaría el siguiente smart contract:

```
pragma solidity ^0.5.0;
contract Registro {
// el registro solo puede modificarlo el admin del
// sistema informático con su clave privada
address owner;
struct Record {
   uint mineTime;
   uint blockNumber;
 }
// mapa que relaciona el hash con el número de bloque en el que se minó
mapping (bytes32 => uint) private hashesDeDocumentos;
constructor(bytes32 _name) public {
   owner = msg.sender;         // quien despliega el contrato es el propietario
 }
function anadirHashDeDocumentos (bytes32 hash) public {
   if (msg.sender == owner) {
      hashesDeDocumentos[hash] = block.number; // número de bloque minada la txn
```

```
    }
  }
function encontrarDocumentosPorHash (bytes32 hash) public constant returns(uint) {
    return (hashesDeDocumentos[hash]); // si existe, devuelve el bloque en que se minó
  }
}
```

En resumen: la institución educativa, a través del sistema de información, entregará a los alumnos un documento con sus notas u otra información relevante y se guardará la prueba de que ese documento existe en la blockchain. El documento, por ejemplo un archivo PDF, está en manos del alumno y se lo enviará a las personas o empresas en las que esté interesado, las cuales podrán comprobar la veracidad del documento recibido.

No se plantean otros usos a la tecnología blockchain ya que plantea más inconvenientes que beneficios. Por ejemplo, emplear una criptomoneda para el sistema de recompensa sería inmensamente caro y además podría crear competencia entre alumnos.

Podríamos utilizar multitud de smart contracts para ampliar la funcionalidad, si usásemos una DLT (Distributed Ledger Technology) o una blockchain privada. Por desgracia, a día de hoy y de mañana, estas tecnologías no proporcionan las características estudiadas en las blockchain públicas de Bitcoin o Ethereum. Especialmente carecen de la seguridad necesaria para asegurar la integridad de los datos.

3.3.2.2. Diseño del sistema

En la anterior etapa de Análisis se ha comprobado que la mayor utilidad del sistema es generar herramientas de análisis para alumnado y profesorado. También generar un currículum que les acompañará a lo largo de la vida.

Este diseño del sistema se centra en generar las siguientes salidas:

- análisis de la evolución de las notas del alumnado
- presentación del feedback
- vista de las recompensas
- certificados con soporte blockchain de los anteriores informes

Para ello se usarán las siguientes entradas recogidas de distintas fuentes:

- notas de cada alumno provenientes de moodle
- feedback de alumnos y docentes
- recompensas
- participación en sesiones y actividades

La arquitectura propuesta es una SOA (Service Oriented Architecture). Dada la clara independencia de los servicios que dan soporte al sistema, con esta arquitectura se consigue que permanezcan débilmente acoplados y posibilitan la implementación de los servicios de manera completamente independiente, por lo que es más sencillo su mantenimiento.

En concreto se utilizarán servicios web RESTful. Estos servicios web, aparte de la interoperabilidad, ofrecen facilidades cuando se trata de un gran número de usuarios como el balanceo de carga o el paso de mensajes en formato ligero JSON. Esto supone una gran ventaja teniendo en cuenta que los usuarios potenciales de este sistema son millones. La forma en que se comunicarán estos servicios es a través de API REST.

4. Conclusiones

Del estudio de la tecnología blockchain:

- Como los cambios en el protocolo han de hacerse de manera consensuada por más del 50% de los nodos, esto puede ser un desincentivo a crear cambios: el protocolo se puede quedar obsoleto
- No se debe hablar de protocolos descentralizados cuando el algoritmo de consenso es poco o nada descentralizado. Se está utilizando blockchain como clickbait para proyectos que en realidad no cumplen con las características propias de una blockchain pública, como el nivel de seguridad. Para este tipo de proyectos sería mejor hablar de tecnología DLT (distributed ledger technology).

-

De Efac:

- Este modelo colaborativo de microsesiones docentes puede generar un hábito entre los estudiantes de
- Al no tener que dedicar todo su tiempo a explicar, el profesorado puede explorar de forma más individualizada al alumnado, conociendo sus características, potenciando las positivas y ayudando a mejorar las negativas.
- La pandemia del covid-19 ha puesto de manifiesto que quienes mejor afrontan una situación excepcional son quienes ya han probado todos los medios a su alcance. Instituciones o profesores que ya habían probado las clases online conocían las herramientas con las que resolver la situación, trabajadoras en empresas que ya hacían teletrabajo no han sufrido un colapso.

  Una de las tareas del sistema educativo es dar herramientas al alumnado, en forma de conocimiento, para que puedan solucionar problemas cuando se les presenten. Y sin embargo el sistema educativo no es capaz de darse herramientas a sí mismo, de probar modelos alternativos, de conocer las formas de educar que va permitiendo la tecnología. Desde mi punto de vista, el sistema educativo no solo debería conocerlas. Debería crearlas.

- Algo

5. Bibliografía

- UNA PERSONA PODRÍA HACER FORK DE LA CADENA EN EL BLOQUE 1 Y EMPEZAR A MINAR MÁS RÁPIDO DE LO QUE SE MINABA EN ESA ÉPOCA:

  SERÍA POSIBLE ADELANTAR A LA CADENA MÁS LARGA? COMPENSARÍA EL GASTO ENERGÉTICO EN HASHRATE? Y creando bloques vacíos?

- Cada vez que se hace una txn, todos los UTXO que se usan como input tienen que ir a algún output. Si Bob lanza una tx con los UTXO disponibles en ese momento en su address, el resto va al minero. Pero qué pasa si mientras se

mina, Alice le manda a esa misma address de origen más bitcoin. Irían para el minero los nuevos fondos?

- Sería más barato pasar la clave privada a aquella persona a quien quieres realizar una txn aunque para eso tendría que ser igual el input que el output

- Qué pasa si los nodos mineros se guardan para ellos las transacciones con más comisiones en vez de hacer broadcast por la red?

https://developer.bitcoin.org/devguide (accedido 1/3/2020)

https://en.bitcoin.it/ (accedido 7/3/2020)

https://www.opencolleges.edu.au/informed/features/peer-teaching/ (accedido 15/8/2020)

Bibliography

Alammary, Ali, Samah Alhazmi, Marwah Almasri, and Saira Gillani. 2019. "Blockchain-Based Applications in Education: A Systematic Review." *Applied Sciences* 9 (12): 2400. doi:10.3390/app9122400. https://search.datacite.org/works/10.3390/app9122400.

Castro, Miguel and Barbara Liskov. 1999. "Practical Byzantine Fault Tolerance." *Engineering Science and Education Journal*.

Chen, Guang, Bing Xu, Manli Lu, and Nian-Shing Chen. 2018. "Exploring Blockchain Technology and its Potential Applications for Education." *Smart Learning Environments* 5 (1): 1-10. doi:10.1186/s40561-017-0050-x. https://search.datacite.org/works/10.1186/s40561-017-0050-x.

Consejo de Coordinación Universitaria. 2006. *Propuestas Para La Renovación De Las Metodologías Educativas*. https://sede.educacion.gob.es/publiventa/propuestas-para-la-renovacion-de-las-metodologias-educativas-en-la-universidad/universidad/12114.

Delgado-Segura, Sergi, Cristina Pérez-Solà, Jordi Herrera-Joancomartí, Guillermo Navarro-Arribas, and Joan Borrell. 2018. "Cryptocurrency Networks: A New P2P Paradigm." *Mobile Information Systems* 2018: 1-16. doi:10.1155/2018/2159082. https://dx.doi.org/10.1155/2018/2159082.

Edmundo Urra Osses. 2014. *Aprendizaje Colaborativo Versus Aprendizaje Cooperativo*.

Gräther, Wolfgang, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. 2018. "Blockchain for Education: Lifelong Learning Passport."European Society for Socially Embedded Technologies (EUSSET), . doi:10.18420/blockchain2018_07. https://search.datacite.org/works/10.18420/blockchain2018_07.

Jacob Bishop and Matthew A Verleger. Jun 23, 2013. "The Flipped Classroom: A Survey of the Research."American Society for Engineering Education-ASEE, . https://search.proquest.com/docview/2317876294.

Krzysztof Okupski. 2016. *Bitcoin Developer Reference*.

Medel-Ationuevo, Carolyn, Toshio Ohsako, and Werner Mauch. 2001. *Revisiting Lifelong Learning for the 21St Century*.

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Oliva, Herberth Alexander. 2016. *La Gamificación Como Estrategia Metodológica En El Contexto Educativo Universitario* UFG Editores. https://www.openaire.eu/search/publication?articleId=od_____3056::71af0847054dc2e5c39984b9567dda92.

Pérez Solà, Cristina and Jordi Herrera Joancomartí. 2014. *Bitcoins Y El Problema De Los Generales Bizantinos* Universidad de Alicante. https://www.openaire.eu/search/publication?articleId=od_____935::afd9f074be40ba594c8f19b895d7fd61.

Sharples, Mike and John Domingue. 2016. *The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward* Springer International Publishing. doi:10.1007/978-3-319-45153-4_48. https://search.datacite.org/works/10.1007/978-3-319-45153-4_48.

Silva Quiroz, J. E., & Maturana Castillo, D. (2017). Una propuesta de modelo para introducir metodologías activas en educación superior. *Innovación Educativa, 17*(73), 117-131. Retrieved from https://dialnet.unirioja.es/servlet/oaiart?codigo=6070623.

Topping, Keith. 2015. "Peer Tutoring: Old Method, New Developments / Tutoría Entre Iguales: Método Antiguo, Nuevos Avances." *Infancia Y Aprendizaje* 38 (1): 1-29. doi:10.1080/02103702.2014.996407. http://www.tandfonline.com/doi/abs/10.1080/02103702.2014.996407.