Blockchain Academy México
Enero de 2020
Blockchain 101

1. Guía de apoyo para el curso de Blockchain101

1.1. Introducción a Blockchain

¿Por qué aprender blockchain?
Blockchain está ocupando lugar en los medios tecnológicos, blockchain nos ayudará a construir la siguiente generación de productos, servicios y starups.

Origen
Cypherpunks: Grupo de científicos, programadores, matemáticos que de acuerdo a una necesidad de privacidad nacen para proponer alternativas a esta problemática, esta solución es el uso de las criptomonedas. El 16 de septiembre cae un banco en EUA, esto quiere decir que cada vez las nuevas generaciones están depositando su confianza a pequeños grupos en lugar de grandes instituciones. El blockchain intenta solucionar la confianza de los usuarios. *Internet*:
Fue concebido para distribuir información. Un problema del internet es que la información está en un punto bajo el control de unos cuantos, esto quiere decir que estamos usando información centralizada. Las personas que tienen acceso a ese punto central, tienen acceso a la información. Uno de los problemas que querían solucionar los Cypherpunks era precisamente que la información estubiera descentralizada. Un ejemplo es Facebook que tiene un gran poder político y económico al tener información de millones de usuarios. Internet 2.0: busca compartir información. Blockchain: busca transferir valor o activo sin la necesidad de un intermediario.

Cypherpunks
Este movimiento nace en un momento difícil, había mucha falta de privacidad ya que el Internet recién había nacido (1967). En esta época había mucho espionaje ya que había una mezcla de intereses entre gobiernos y empresas. Los Cypherpunks reaccionan de forma rebelde a una problemática (la falta de privacidad) con el uso de la tecnología y la criptografía. En 1991 se difunde en la revista *wired* el cifrado simétrico que es la base con la que hoy en día funcionan muchos de los blockchains públicos. El objetivo de difundir este cifrado simétrico es el de resistir a la pérdida de la privacidad del usuario en la era del Internet.

Los Cypherpunks diseñaron las principales propuestas al bitcoin, su filosofía está plasmada en cuatro puntos de su manifiesto Cypherpunks.

1. La privacidad es necesaria para una sociedad abierta en la era electrónica.
2. Privacidad != secretismo
3. La privacidad es la capacidad de revelarse selectivamente al mundo.
4. La privacidad con una sociedad abierta requiere sistemas anónimos para efectuar transacciones.

¿Qué es el dinero y qué es Bitcoin?
Estamos en la revolución más importante que podría cambiar la forma como utilizamos el dinero. El dinero es cualquier cosa que se pueda intercambiar por productos o servicios. Ninguna moneda está respaldada por oro sino en bases de datos que tienen los gobiernos. El petróleo es un buen ejemplo de recurso natural que puede ser usado como dinero, su valor está determinado por el uso que le da el mercado.
El dinero se crea imprimiendo o emitiendo. Tiene valor porque es un monopolio del gobierno, pues solo con eso puedes pagar impuestos. El petróleo por su parte también tiene su proceso de emisión, que debe ser regulado como la emisión de monedas.
La mayoría del dinero que conocemos no existe en papel sino en bases de datos.

El patrón oro es un sistema monetario que da valor a una moneda en términos de una cantidad en oro, en este sistema el dinero se respalda en oro, tú puedes ir a cambiar tus monedas al banco y a cambio te dan cierta cantidad de oro, a este dinero se le conoce como *fiduciario*, esto es, dinero con respaldo, representa un valor atesorado por el gobierno que lo imprime. Este sistema dejó de existir en todo el mundo a partir de 1971 cuando Estados Unidos rompió con él.

Hoy el día el dinero que manejamos se le conoce como *fiat* que significa *hágase* o *qué así sea*. Tiene dicho nombre porque existe por decreto, por orden de la autoridad que gobierna. No se puede cambiar por oro o plata. No tiene un respaldo.

Características del dinero:

- Intercambiable.
- No consumible.
- Portable.
- Durable.
- Muy divisible.
- Seguro (no falsificables).
- De fácil transacción.
- De existencia limitada.

- Soberano. ?
- Descentralizado.
- Inteligente (programable).

Criptografia simétrica y asimétrica:
Conozcamos los tipos de criptografía:

Criptografía simétrica ó cifrado simétrico: Es ocultar cualquier dato dentro de un algoritmo cifrado con el cual **el emisor puede enviar el mensaje oculto**, la parte receptora tiene que tener el mismo algoritmo de cifrado y utilizarlo a la inversa. SI alguien en medio logra tener acceso a ese algoritmo criptográfico puede desencriptarlo sin problema.

Criptografía asimétrica: Por lo anterior nace la criptografía asimétrica. Se crean simultáneamente dos llaves, una será pública y otra privada. La pública la puedo compartir con cualquier persona para que a través de ella me pueda mandarme información cifrada y solo yo con el otro par, mi llave privada, pueda descifrarlo.

OJO: La llave privada no se debe compartir.

Cifrado asimétrico.
Nos va a dar tres principales cosas.

- **Anonimato**: No necesitamos decir quiénes somos.
- **Inclusión**: Cualquier persona va a poder interactuar con una red blockchain en cualquier parte del mundo.
- **Seguridad**.

Criptografía: el cifrado de mensajes se ha practicado desde hace más de 4,000 años. Criptogragía viene del griego, escritura oculta.

Encriptación simétrica: Los algoritmos de Criptografía simétrica utilizan la misma clave para los dos procesos. Cifrar y descifrar. Suelen ser sencillos de utilizar y bastante eficientes.

1.2. Fundamentos de blockchain

¿Qué es Blockchain y DLTs?
Blockchain hace parte de un conjunto de tecnologías distribuidas o DLTs (Distributer Ledger Technologies). Existen otras tecnologías a la par como DAG (Directed acyclic graph) y TEMPO. Blockchain en este caso es la más conocida. Ten en cuenta que DLT y Blockchain son cosas distintas. DLT es el conjunto de tecnologías y Blockchain es una de ellas.

¿Qué problemática resuelve blockchain?
Resuelve la necesidad de confianza que tenemos mediante un tercero para realizar una actividad económica o comercial. Resuelve los principales problemas del dinero digital. La tecnología detrás de un sistema de pagos como paypal funciona de la siguiente manera. Voy a una plataforma, decido comprar algo y cuando doy a pagar, el sistema dice que yo tengo un saldo que puedo usar para

transferir a la plataforma, esto es, através de una plataforma centralizada puedo acceder a realizar compras.

La propuesta de blockchain es que podamos transferir cualquier valor o activo eliminando las bases de datos centralizadas, en lugar de esto usamos un sistema descentralizado de consenso.

Propuestas de innovación.

- Descentralización: es un proyecto descentralizado de alcance mundial. No hay un origen ni hay un destino.
- Emisión pública de dinero: El dinero se emite de manera pública por primera vez.
- Transferencia de valor entre pares: Transferencia de activos sin la necesidad de un tercero.

Blockchain es la tecnología detrás de Bitcoin.

Los Nodos son servidores, un servidor es un computador que está de alguna manera anotando todos los movimientos de las monedas y auditándose. Hay miles de nodos conectados en todo el mundo y cada uno tiene el mismo libro contable público distribuido. En español: libro de registros públicos distribuidos.

Caracaterísticas de Blockchain:

- Es distribuido
- Es un sistema de consenso: las cuentas dan porque dan, todos tienen toda la información.
- Es global: si yo tengo acceso a internet, tengo acceso a Blockchain
- Es veloz: las transacciones duran de 10 minutos a 30 minutos.
- Funciona a base de criptografía
- Es transparente: es un libro contable público distribuido, puedo ver todo lo que ocurre.
- Es inmutable: no se puede eliminar información, todo lo que yo haga queda registrado.
- Sin intermediarios: no hay una empresa o ente que administre la red.

Problema del doble gasto;
El problema del doble gasto es un defecto potencial del dinero digital por el que una misma moneda digital puede gastarse más de una vez.

El problema de los generales bizantinos. Es un problema que resuelve blockchain, al estar todos los nodos conectados se comparten la misma información y todos la ven, se toma la decisión en la que estén a favor la mayoría. Tiene que ver con la comunicación ¿Cómo comunicas a todas las entidades?

Tecnologías que conforman Blockchain

- **Criptografía**: las transacciones en blockchain están cifradas por una llave pública y una privada que permiten guardar la información de forma anónima. En el leadger podemos ver cierta información de las transacciones por ejemplo: que transacción existe, que cantidad de crypto fue manejada pero no sabemos a quién le corresponde dicha transacción ni quién la hizo.

- **Red P2P**: es una red descentralizada en la que todos los nodos están conectados, si quisiéramos eliminar la blockchain tendríamos que apagar todos los servidores donde corre la red, eliminar los incentivos de los mineros. Esto es muy difícil, al ser descentralizado está pensado en que viva en todo el mundo.
  Las redes P2P hacen que no todo ocurra en un punto central, es decir, nos da descentralización, seguridad porque es difícil hackear muchos puntos en lugar de uno solo, al estar la red blockchain distribuida en muchos nodos nos da una gran escalabilidad.
  Una topología *centralizada* un nodo es el principal, si se cae éste toda la red deja de funcionar.
  Una topología *descentralizada* tiene nodos en la misma jerarquía que están por encima de otros.
  Una topología *distribuida* se enfoca en que todos los nodos estén en la misma jerarquía.

- **Protocolo**: decide cómo se van a seguir organizando los bloques y cómo alimentar esta red.
  Es un acuerdo entre varias personas, crear un acuerdo es difícil ya que no muchas personas coinciden en las decisiones, el problema se vuelve aún mayor si hablamos de una red como blockchain en donde el número de usuarios es aproximadamente entre 9,000 y 11,000. El Protocolo de consenso busca poner de acuerdo a las personas para que en el caso de bitcoin minen un bloque cada 10 minutos de forma constante.
  Este Protocolo de consenso obedece a la necesidad de poder plantear la creación de dinero digital. El crear dinero digital es un gran reto ya que surgen preguntas como:

  - ¿Cómo hago para que se respete el orden de los registros?: qué pasa si una persona quiere modificar las transacciones, es decir, coloque más dinero del que en realidad tiene.
  - ¿Cómo proteger la integridad del libro contable?: qué pasa si el lugar donde tengo los registros desaparece.
  - ¿Cómo evitar colisiones/alguien más escriba?: que otras personas escriban lo que quieran en la red.
  - ¿Cómo incentivo a la comunidad a mantener el libro?: tiene que haber un incentivo para que la gente esté registrando información.

- **Leadger**: es el libro contable donde se encuentras todas las transacciones que se han hecho desde el día cero, estas transacciones se encuentran en bloques.

Nodos

Un nodo es cualquier servidor (computadora o celular) que está conectado a una red y que cumpla con los requerimentos de esta red. Para formar parte de la red blockchain descargas una wallet a tu computadora y de esta manera formas parte de la red. La red blockchain pesa aproximadamente entre 250 GB y 300 GB

Tipos de nodos:

- **Full node**: son los nodos que verifican las reglas de blockchain, bajan cada bloque y transacción y la verifican. En la red bitcoin estos nodos verifican que las transacciones sean correctas, es decir que un usuario no pase bitcoin que no tiene a otra cuenta. Si una transacción o bloque viola las reglas, esta es rechazada. Cada *Full node* debe bajar todas las transacciones desde el principio de los tiempos y los encabezados de cada bloque.

- **Miner node**: los mineros toman las transacciones y ejecutan un proceso llamado minería, este proceso es encontrar un hash que debe estar precedido por cierto número de 0's según la dificultad. Un bloque puede tener información de aproximadamente 2,500 transacciones, también hay bloques vacíos, los mineros nunca paran y siguen minando bloques que puede o no que coloquen información de transacciones en ellos. Al desbloquear un bloque obtienes una retribución económica en bitcoins.

Blockchain pública, privada, semi-privada y consorcio.

Hay 4 tipos de redes de Blockchain:

- **Pública**: Es una red blockchain a la que cualquiera puede tener acceso.
- **Privada**: Blockchain implementada en una empresa u organización para aprovechar todas sus características mediante uso interno.
- **Semi-Privada**: Implementación privada con acceso parcial a una blockchain pública o a personas especificas externas.
- **Consorcio**: Es un conjunto de blockchains privadas distribuidas en diferentes empresas con acceso entre ellas.

1.3. Tipos de Blockchain

1.3.1. Blockchain 1.0

La red Bitcoin es lo que se conoce como *Blockchain 1.0* usada principalmente para enviar y recibir transacciones de valor. Es capaz de procesar alrededor de 5 transacciones por minuto. Esto permite que la red Blockchain se ejecute como un medio para transaccionar dinero digital. Actualmente existen 18,159,400 BTC y quedan por minar 2,840,600 BTC

1.4. Blockchain 2.0

Cuando nació la red Ethereum empezamos a hablar de un nuevo termino llamado *Blockchain 2.0* lo que incorpora la utilización de *smart contracts*, es una blockchain en la que se pueden hacer desarrollos *DApps* (que veremos más adelante). Procesa cerca de 25 transacciones por minuto. Aquí es donde podemos almacenar programas en la red Blockchain.

1.5. Blockchain 3.0

Por su parte la *Blockchain 3.0* es un nuevo enfoque de criptomonedas cuya principal propuesta es mejorar la escalabilidad de sus aplicaciones, e incorporar nuevas características de utilización como sistemas de votaciones. Es capaz de procesar entre 2000 y 4000 operaciones por minuto. EOS, ARK y NEM son conocidas por estar creadas como Blockchain 3.0

1.6. Blockchain 1.0 -Bitcoin

¿Qué son las criptomonedas:
Todo empieza con Bitcoin y el paper de satoshi nakamoto.
Piensa en Bitcoin como un organismo vivo que no depende más que de su popularidad. Tiene incentivos para que muchas personas al rededor del mundo minen un base de datos descentralizada que se va poblando con distintas transacciones. Después de Bitcoin empezaron a salir otros proyectos de manera paralela, un ejemplo es Ethereum que te permite hacer contratos inteligentes. En Bitcoin puedes guardar información y hacer transacciones mientras que en Ethereum puedes programar un espacio para tomar decisiones, después le siguieron otros proyectos. Bitcoin fue la primera criptomoneda, pero a ella le siguieron otras como Ethereum, ZCash, ICO. *ICO*: initial coin offering, esto es cuando alguien lanza una nueva criptomoneda y ofrece token's a cambio de transacciones digitales, esto generó nuevos proyectos como Aragon, cibyc, OMG. En coinmarketplace puedes ver las transacciones de distintas criptomonedas la más popular es Bitcoin pero no es la única.

Las **criptomonedas** son un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, las criptomonedas son una revolución tecnológica que trae consigo todo lo que esto implica, como fraude, inversionistas, etc.

Muchas de las criptomonedas no están pensadas para ser usadas como monedas, como sí es el caso de Bitcoin, en su lugar están pensadas para ser usadas con otras funciones como: en el desarrollo de aplicaciones, para hacer una red social o para almacenar datos en la blockchain, entre otras cosas. Es por esta razón que es preferible llamarlas criptoactivos. Todas las criptomonedas diferentes a

Bitcoin, son conocidas como alternative coins o ALTCOINS (monedas alternativas).
Ethereum es la segunda criptomoneda más importante.

Qué es Bitcoin?

Cuando enviamos mensajes, correos, imágenes, videos, etc. lo que enviamos y recibimos son copias. Es muy fácil hacer una copia en el mundo digital, lunchar contra la pirateria es algo muy dific, por otro lado, cuando hablamos de dinero o de activos transmitidos por internet, se vuelve un problema ya que podríamos llegar a “copiar"dinero y éste perdería su valor. El bitcoin es la moneda virtual que se puede intercambiar sin realizar una copia, la unidad mínima de BTC son los Satoshis. El BTC nace como una protesata a la inflación y a realizar una nueva economía. Bitcoin fue creado en el 2009 por Satoshi Nakamoto. Un bitcoin es divisible hasta en 8 decimales. Los centavos del bitcoin son conocidos como Satochis. Bitcoin nace como una protesta a la moneda tradicional y a las transacciones bancarias.

Algunas características de Bitcoin son:

- No permite doble gasto: no podemor realizar copias de BTC.
- Sin riesgo de terceros: no vas a realizar una transacción en BTC sin el peligro de que roben alguna empresa de un tercero perjudicando nuestro dinero.
- Costo insignificante: cobra una comisión sin importar la cantidad de dinero transferido.
- Veloz: una transacción puede tardar de 10 minutos hasta 30 minutos.
- Sin derecho de admisión: es un sistema inclusivo, no te pide edad, ni ninguna otra información personal.
- Internacional: cualquier persona en todo el mundo puede hacer una transacción.
- Sin confiscación posible: es un sistema distribuido que a nadie le pertenece, por ende no puede llegar un ente centralizado a confiscar BTC.
- Limitado: existe un límite de BTC.

“Bitcoin es un increíble logro criptográfico y la habilidad de crear algo que no se puede duplicar en el mundo digital tiene un valor enorme."

Los bicoins se generan utilizando operaciones matemáticas que construyen la seguridad criptográfica. Existe un algoritmo llamado bitcoin miner (minería de bitcoin) que genera procesos matemáticos para hacer transacciones de bitcoin entre sí y generar nuevos bitcoins, un bitcoin es una exansión de la base de datos.

La base de datos de bitcoin es como la base de datos de los bancos centrales cuando imprimen dinero, cada billete tiene un número que tiene un equivalente en una base de datos, esa base de datos se llama blockchain y todas las personas que hacen mineria tienen una copia de esta blockchain esta base es una red P2P como un torrent.

El dinero fiat tiene valor porque es un monopolio del estado, tú no puedes pagar impuestos com manzanas. El petroleo tiene valor debido a la oferta y demanda en consecuencia de una necesidad. Así como existen distintos tipos de monedas (USD, MX, etc) también existen distintos tipos de cryptos. Una crítica común al bitcoin es que es muy caro ó volatil pero el petroleo también es muy

volatil y ha cambiado mucho de precio, también el dinero mexicano ha sufrido una baja. El dinero fiat no existe en papel sino en bases de datos, a esta se le conoce como hoja de cuentas, libro mayor o leadger.
El dinero fiat es un monopolio del estado, si imprime más dinero el valor disminuye.
El dinero es difícil de rastrear cuando se encuentra en estado físico.
El dinero es fácil de rastrear cuando se encuentra en estado digital.

Cuando los gobiernos imprimen dinero sin limite el valor baja, este es el caso de venezuela. Blockchain es una base de datos que registra el historial de todas las transacciones. Cuando una persona mina bitcoins distribuye la base de datos de las transacciones, replica las transacciones y descubre nuevos espacios dentro de la base de datos.
Cada vez que creo un registro nuevo la operación matemática se vuelva más compleja, esto con el objetivo de que no haya más bitcoins posibles, esto para evitar el problema de imprimir más billetes. La gente que mina ya no tiene incentivos a nivel de recoger bitcoins nuevos.

Cuando hay mineria se crean nuevos bloques se les da un porcentaje de bitcoin a los mineros que participaron en la creción de dicho bloque.

Puedes ver las transacciones de todo el mundo, lo que no puedes ver es quiénes son los dueños de dichas transacciones, cuando eres dueño de un bitcoin de lo que en verdad eres dueño es de una llave criptográfica que permite tomar un bitcoin y darselo a alguien más.

Bloques:

- Hash pointer: cada bloque tiene un hash pointer, un hash es un identificador único que además nos dice cuál fue el blque anterior.
- Tiemstamp: es la "estampa de tiempo.[en] que fue creado, es ell momento en el tiempo en el que fue creado el bloque.
- Datos de transacción: quién mandó la transacción, qué cantidad, fee que se hizo por esto, etc.

Los bloques no se pueden modificar, las transacciones no son reversibles y todo queda registrado para todo el mundo. Hay un espacio extra en los bloques en el que los mineros pueden utilizar de la forma en que deseen. Es decir, los mineros pueden inyectar el texto que prefieran en el resto del espacio. Durante el minado del bloque génesis, Satoshi Nakamoto utilizó este espacio para escribir lo siguiente:

"The Times 03 / Ene / 2009 Canciller al borde del segundo rescate para los bancos".

De esta forma, los mineros pueden agregar información a cada bloque para personalizar el mismo, enviando un mensaje que no podrá ser alterado por nadie y custodiado por la seguridad de la blockchain.

Transacciones:

Características de las transacciones

El valor de cada transacción está unido a la recompensa del bloque actual y es afectado por el *halving* que este activo en ese momento para dicha criptomoneda. En bitcoin las recompensas empezaron con 50 BTC, luego bajaron a 25 BTC y actualmente (principios del 2020) es de 12.5 BTC, se estima que para mayo del 2020 la recompensa sea de 6.25BTC. El *halving* ocurre cada 210,000 bloques Debido a que el minero es quién construye la transacción, existe la posibilidad de manipularla. Para evitar esto la recompensa no puede ser gastada hasta que haya pasado las 100 confirmaciones. Las transacciones

contienen la dirección Bitcoin del minero que ha realizado la minería del nuevo bloque, se indica cual fue la recompensa del bloque. Cada transacción ocupa 100 bytes de datos

Cada transacción tiene una firma digital y se requieren dos llaves:

- **Pública**: para identificar a cada una de las personas que hacen las transacciones. La puedes compartir para que alguien más interactúe con tu wallet.
- **Privada**: cifra cada una de estas transacciones. La tienes que cuidar, con esta puedes ejecutar transacciones.

Esto es como usuarios y passwords.

¿Qué es minería?:

El concepto de minería viene del proceso para extraer oro en minas. Así como las criptomonedas, el oro ha ido incrementando su valor y el proceso de minarlo se vuelve más valioso por lo que se recibe a cambio de hacerlo.

Existen equipos especializados en la mineria de bitcoin, estos equipos se conectan a la red eléctrica y a la red de internet, hacen procesos de cómputo hasta que uno de estos procesos es el ganador y la red de bitcoin premia al minero con una cantidad de bitcoin que es proporcional al trabajo que realizó.

Pools de Minería

Las Pools de minería son grupos de personas que se unen o se asocian usando su(s) equipo(s) de minería individual(es) con el propósito de formar granjas virtuales de minería, y así tener mayor poder de procesamiento en conjunto que pueda competir con otras granjas o equipos mineros muy potentes por la recompensa en el procesamiento de transacciones de una blockchain.

Si llegara a darse el caso de que una Pool de minería tenga en su conjunto 51 % o más del poder de procesamiento de toda la red blockchain en la que se encuentra, se correría el riesgo de lo que se conoce como un Ataque del 51 %, en el que los administradores de esta pool tendrían el poder de manipular las transacciones a su antojo, pudiendo generar dobles gastos, invalidando y aprobando confirmaciones de bloques, entre otros.

¿Por qué minar?

Por la seguridad que brindan los mineros, pues agregan una capa de seguridad, protegiendo a los usuarios de los abusos, con transacciones falsas. Dentro del protocolo no es posible gastar una moneda dos veces. Los mineros validan las transacciones. Todas las transacciones que suceden dentro de un tiempo determinado se guardan en la base de datos como un bloque y se confirman. Cuando se crea un bloque a través de la minería se crean nuevas monedas y esto lleva al tercer beneficio. Minando es posible ganar dinero: cuando se genera un nuevo bloque se generan monedas que son depositadas en la cuenta del minero.

¿Es rentable minar Bitcoin?: En principio si, pero es importante tener en cuenta costos de equipos y electricidad. Si puedes construir un entorno en el que se cubran estos costos fácilmente tendrás retorno de inversión en alrededor de 6 o 7 meses. También considera que la dificultad para minar va aumentando con el paso del tiempo, entonces para una persona que recién va a empezar a minar puede ser más dificil que para alguien que ya lleva un tiempo minando.

¿Cómo funciona la minería de Bitcoin?: La función SHA256 genera una cadena de caracteres de 256 bits. El minero recibe toda la cabecera del bloque anterior y del nuevo bloque que se va a crear, con esto se crean dos variables que se van a utilizar en el proceso de minado. El proceso funciona como un ciclo que comienza con un número aleatorio.

De qué trata el paper de Satoshi: Satoshi Nakamoto es un personaje anónimo y su paper es un documento que explica qué es Bitcoin. Bitcoin es una red de pares que generan un sistema de transacciones financieras descentralizadas.
El documento presenta la idea de que no haya necesidad de una tercera parte para hacer transacciones bancarias, y que el sistema no esté basado en confianza frente a una entidad regulatoria sino a datos encriptados.
En la primera parte habla sobre cómo las instituciones financieras siempre tienen que regular las transacciones. El hecho de crear transacciones irreversibles es de hecho un beneficio en cuanto a lo que propone el paper.
Para que la red funcione es necesario que exista una recompensa para quienes están minando. Los mineros reciben incentivos por participar en esta red de pares al minar o validar transacciones. Para verificar que una transacción existe es fácil hacer consultas a través de los headers de cada bloque.
El documento también habla sobre cómo evitar que existan ataques en las transacciones, y esta es quizás la parte más compleja de toda la explicación.

en una línea temporal ¿Quién es este hombre? Satoshi Nakamoto es el nombre del creador del protocolo usado para dar vida al bitcoin. Satoshi Nakamoto es sin lugar a dudas el pionero en el mundo de las criptomonedas y a la vez el personaje más enigmático relacionado con este tema. Al día de hoy no está claro aún, si él o ella, es una persona o un personaje ficticio creado por un grupo de hackers anónimos. Lo único que se conoce a ciencia cierta, es que Satoshi Nakamoto publicó este documento en 2008 que dió inicio a todo el desarrollo de las criptomonedas, y que además da su nombre a la fracción mínima con la que opera el bitcoin, el satoshi (0.00000001 bitcoins).Hay incluso especulaciones (leyendas urbanas) que dicen que el nombre Satoshi Nakamoto no es más que un nombre "fabricado" que está formado por fragmentos de las los nombre de las empresas asiáticas: Samsung, Toshiba, Nakamichi y Motorola y que pudiera dar algunos indicios de grandes empresas o grupos de poder que podrían estar detrás de todo esto. (sin embargo, no hay pruebas que lo demuestren). Los puntos del papel

1. **Introducción**: Habla de los problemas que tiene el sistema financiero de hoy en día, como el hecho de que haya una entidad reguladora sobre la validez de una transacción. Así como de un sistema descentralizado, también señala que este sistema puede ser dañado con nodos corruptos.

2. **Transacciones** (Transactions): Esta parte define lo que es el blockchain, y que define una criptomoneda o divisa electrónica como una cadena de firmas digitales, cada comprador transfiere la moneda a otro así creando una cadena de bloques de transacción a lo largo de la vida de cada moneda.

3. **Estampa de Tiempo** (Timestamp Server): Se necesita una estampa de tiempo para cada transacción y permite verificar la transacción anterior con la nueva transacción.

4. **El Minado** (Proof-of-Work): Para minar se requiere mucha capacidad de CPU, para poider encontrar un algoritmo complejo que al resolverlo, obtiene una recompensa, es decir una nueva moneda en la cadena de bloques.

5. **La Red** (Network): Transmite las transacciones a los nodos-Recolectar las transacciones en un nuevo bloque-Verifican el Proof-of-Work para crear un nuevo bloque-Una vez sucedido todo este proceso, se transmite una transacción verificada a todos los nodos

6. **Incentivos**: Como hacer que esta red funcione de una forma particular, señalan que recompensarían a los mineros, a quienes creen un nuevo bloque. Cuando se terminen las bitcoins, pueden existir comisiones que se repartirían entre los nuevos bloques.

7. **Reclaiming Disk Space**: Qué pasará con el número de transacciones cuando comience a crecer. Todo el leadger va quedando guardado y cada vez hay más transaccione, aquí habla de ideas para cuidar el espacio de almacenamiento, una de ellas es guardar los headers para acceder a las transacciones. Consideraron la ley de moore que indica que en el futuro se tendrá mayor capacidad de cómputo del que había en la época.

8. **La Verificación** (Simplified Payment Verification): Para verificar que un pago sucedió no necesitas tener el leadger completo de transacciones de tu moneda para verificar que la transacción existe, puedes buscar simplemente con los headers, esta información es muy transparente y existen muchos repositorios públicos donde puedes ir a consultar transacciones por el hash o navegando.

9. **Combinar y Dividir Valores** (Combining and Splitting Value): Como hacer lo que dice en el título, en diferentes transacciones dentro de un bloque, bitcoin como muchas otras, aunque particularmente esta permite que se manejen transacciones en decimales, es decir que no necesariamente debes comprar una unidad entera si no también fracciones de la misma.

10. **Privacidad**: En bitcoin en contraste al sistema tradicional, las identidades están desconectadas de las transacciones, y las transacciones son públicas ya que el P2P se mantiene bajo el anonimato. Existe una criptomoneda llamada ZCash, que es mucho más anonimizada que la bitcoin.

11. **Cálculos**: Estima lo que puede pasar en caso de un ataque al blockchain, como se puede evitar la corrupción de este ecosistema, las ecuaciones y cálculos de probabilidad son simplificadas y traducidas el lenguaje de programación C. Esta es la parte más compleja de todo el paper.

12. **Conclusión**: Para una red de pares ya no se necesita confianza de ningún intermediario, solamente transacciones, sistema encriptados, software distribuido y con incentivos. El paper de Satoshi Nakamoto, es la introducción de este mundo, y algo básico que cualquiera debe leer antes de introducirse en las cryptocurrencies.

13. **Referencias**: Aunque blockchain y bitcoin nace con este paper ya se había hablado de esto antes.

1.7. Protocolos

Proof of work y Proof of stake son dos caminos para validar transacciones. El primero aplica fuerza bruta a través de cómputo matemático para extraer la criptomoneda, el segundo es como un sorteo para ver quién se queda con ella.

- **PoW**: extraer oro de las minas, es un proceso pesado.
- **PoS**: obtener oro mediante un sorteo.

PoW (Proof-of-work): Lo utilizan muchas monedas pero es un proceso ineficiente pues necesitamos equipos especializados costosos, que gastan una gran cantidad de energía. Es un concepto que existe incluso antes de las criptomonedas, pues se utilizaba, por ejemplo, para validar si un email era Spam. El sistema funciona a través de funciones criptográficas que garantizan que cada entrada (input) tenga una sola salida (Hash sum). Cada bloque tiene un hash que es la identificación única. PoW fue el primer algoritmo de consenso que se creó. Es empleado por Bitcoin y muchas otras criptomonedas. El algoritmo Proof of Work es una parte esencial del proceso de minado. **PoS (Proof-of-stake)**: Elimina toda la capa de cómputo pesado y utiliza un solo servidor que puede ser pequeño. Entre más bitcoins tienes en tu poder mayor es la capacidad de minado. El proceso es similar a cuando haces un depósito en el banco y empiezas a recibir intereses por tener ese dinero guardado ahí.

PoI (Proof of Importance): es el sistema de consenso empleado por la red NEM, y se basa en la reputación o historial de transacciones realizadas por cada nodo sobre la blockchain. A mejor reputación, mayor probabilidad para validar bloques.

Casper: es un sistema híbrido de Ethereum que mezcla PoW con PoS y para poder ser un nodo de esta red se requiere una cantidad importante de dinero puesta en garantía para aspirar a la validación de bloques.

¿Por qué importan los Algoritmos de Consenso para las Criptomonedas?:

Los algoritmos de consenso son importantes para la seguridad de una red de criptomonedas. Son los encargados de ponerse de acuerdo respecto al .estado.actual de la blockchain, es esencial para que un sistema económico digital funcione correctamente.

El algoritmo de consenso Proof of Work se considera una de las mejores soluciones al Problema de los Generales Bizantinos, que permitió la creación de Bitcoin como un Sistema Tolerante a Faltas Bizantinas (Byzantine Fault Tolerant System). Esto significa que la blockchain de Bitcoin es altamente resistente a un tipo de amenazas denominadas .ataques del 51 %.o .ataques mayoritarios", no sólo porque la red esté descentralizada, sino también gracias al algoritmo PoW. Los altos costes involucrados en el proceso de minado hacen que sea muy difícil e improbable que los mineros inviertan sus recursos para perjudicar a la red.

Masternodos:

Los masternodos son una versión más rentable que la minería *PoS* tradicional, la minería con masternodos necesitas mínimo 100 mil monedas, esto genera una mayor rentabilidad.

Los masternodos se han popularizado por el tema de estafa. Debes asegurarte de que tus monedas sean serias y no caigas en estafas. El 90 % de los masternodos son estafa y pueden ser esquemas

piramidales. Estos usualmente prometen una rentabilidad gigantesca. Es por esto que tenemos que conocer la criptomoneda y conocer su proyecto, cualquiera puede crear una criptomoneda que no tenga ningún valor.

1.8. Blockchain 2.0 -Ethereum

¿Qué es *ethereum*?

Actualmente es la segunda criptomoneda más importante porque tiene la mayor capitalización después de Bitcoin. Ethereum fue creada en 2014 por *Vitalik Buterin*, un ex desarrollador de Bitcoin que introdujo los contratos inteligentes o smart-contracts en la tecnología blockchain.

Un **smart contract** es como un contrato tradicional de los que se usan para establecer acuerdos entre dos o más personas pero que en lugar de recurrir a una tercera persona como un notario para garantizar su cumplimiento, recurre a la blockchain como garantía de confianza distribuida para ejecutar lo acordado.

Ethereum fue la criptomoneda que dio paso a Blockchain 2.0

¿Qué es un Token?

Un token es cualquier forma de digitalización de un activo. Los token no se pueden minar, a diferencia de las criptomonedas. El *ERC20* es uno de los tokens mas populares. Un token utiliza la blockchain de una criptomoneda. Es un activo digital o *smartcontract* que convive con otros ecosistemas sobre otra plataforma, es decir, depende de un tercero y su valor inicial puede ser asignado por una empresa.

Un token globalmente es la digitalización de cualquier activo. El ERC20 es un smartcontract basado en Ethereum y es el token más popular entre las ICOs o representaciones de acciones de un proyecto. Estos tokens funcionan sobre una blockchain ya existente

¿Qué es un contrato inteligente

Un **contrato** es un acuerdo en el que dos o más partes se comprometen a respetar y cumplir una serie de condiciones.

Los contratos inteligentes o **smart contracts** son contratos que tienen la capacidad de cumplirse de forma automática una vez que las partes han acordado los términos.

En contratos en papel se redactan condiciones, términos que se tienen que cumplir las partes que firman éste. El cumplimiento de dicho contrato está sujeto a la interpretación de las partes, que puede llegar a favorecer a una más que a otra.

Los contratos inteligentes son programas informáticos. Son un tipo de software que se programa para llevar a cabo una tarea o serie de tareas determinadas de acuerdo a las instrucciones previamente introducidas. Su cumplimiento no está sujeto a la interpretación de ninguna de las partes: si el evento A sucede, entonces la consecuencia B se pondrá en marcha de forma automática. No se requiere de ningún intermediario de confianza (como una notaría), pues este papel lo adopta el código informático, que asegurará sin dudas el cumplimiento de las condiciones. Por tanto, se reducen tiempo y costes significativos.

¿Qué es una Dapp? Una DApp o **Descentralized application**, es una aplicáión que toma las características de descentralización de las criptomonedas. Puedes crear cualquier juego y dejarlo sobre una blockchain.
Algunos ejemplos son los *Cryptokitties* o *Fishbank*.

Los **CryptoKitties** son mascotas virtuales que se deben alimentar. Estas son *smart contracts* que funcionan sobre la blockchain de Ethereum. Cada gatito es único, y puede llegar a ser muy costoso.

Fishbank es un juego de unos peces que se alimentan y juegan por el mar. Este también funciona sobre la blockchain de Ethereum como un *smart contract*.

Otras DApps

- **Civic** es como un documento de identidad del futuro. Funciona sobre la blockchain de Ethereum y es un token. Quiere protegerte contra el robo de identidad.
- **Status** es un token sobre la blockchain de ethereum, un conjunto de smartcontracts y es como un whatsapp. Te permite hacer pagos a través de un chat.
- **Golem** es un token de Ethereum. Busca que al ser parte de un nodo, puedas alquilar poder de cómputo. Puedes alquilar capacidad de RAM, de almacenamiento, entre otros.
- **Substratum** busca desentralizar el internet, es decir, cuando me conecto a facebook, google, twitter, etc me conecto a un servidor. Substratum busca que no nos conectemos a un servidor centralizado sino a un servidor desentralizado alojado en la red blockchain, de esta manera los gobiernos no podrán bloquear servidores ya que tendrían que bloquear miles de servidores.

2. Material general de apoyo

2.1. Artículos

- ¿Por qué el dinero es dinero?
- Paper de Satoshi Nakamoto
- Explicación del white paper de satoshi
- Algoritmos de consenso
- Tokens ¿Qué son?
- Diferencia entre token y criptomoneda
- ¿En qué se respalda el dinero?
- Último bitcoin
- ¿Por qué un bloque pesa 1MB
- Blockchain Pública y Privada
- ¿Qué es ethereum?
- ¿Qué es el gas?

2.2. Videos

- Privacidad
- ¿Qué es Blockchain
- ¿Cómo funciona bitcoin?
- ¿Por qué a los bancos les gusta Blockchain
- Criptomonedas (Documental)
- Entiende Bitcoin y Ethereum
- ¿Qué es Blockchain en 5 minutos.
- Las matemáticas de Blockchain

2.3. Sitios web

- CoinMarketCap
- Número de transacciones blockchain
- Bitso
- LocalBitcoin
- Coinbase
- Fishbank
- CryptoKitties
- Civic
- Golem
- Substratum
- Stauts

2.4. Noticias blockchain

- Cointelegraph
- CriptoNoticias

2.5. Libros

- Cryptoassets
- Digital Gold
- Mastering Bitcoin
- Blockchain Revolution
- Blockchain