Seminario 9: Introducción a Blockchain

Sistemas Distribuidos

Pablo García Sánchez y Salvador Gutiérrez Salcedo

Departamento de Ingeniería Informática
Universidad de Cádiz
Pablo García Sánchez

Curso 2019 – 2020

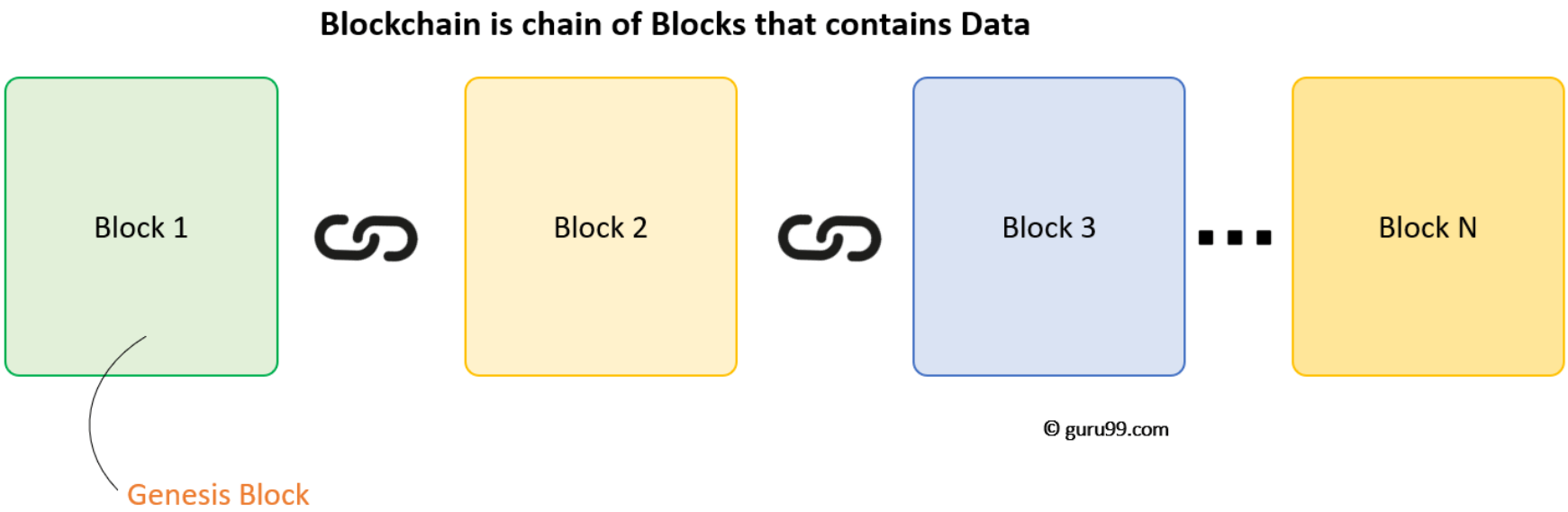
Indice

Sección 1 | Arquitectura Blockchain

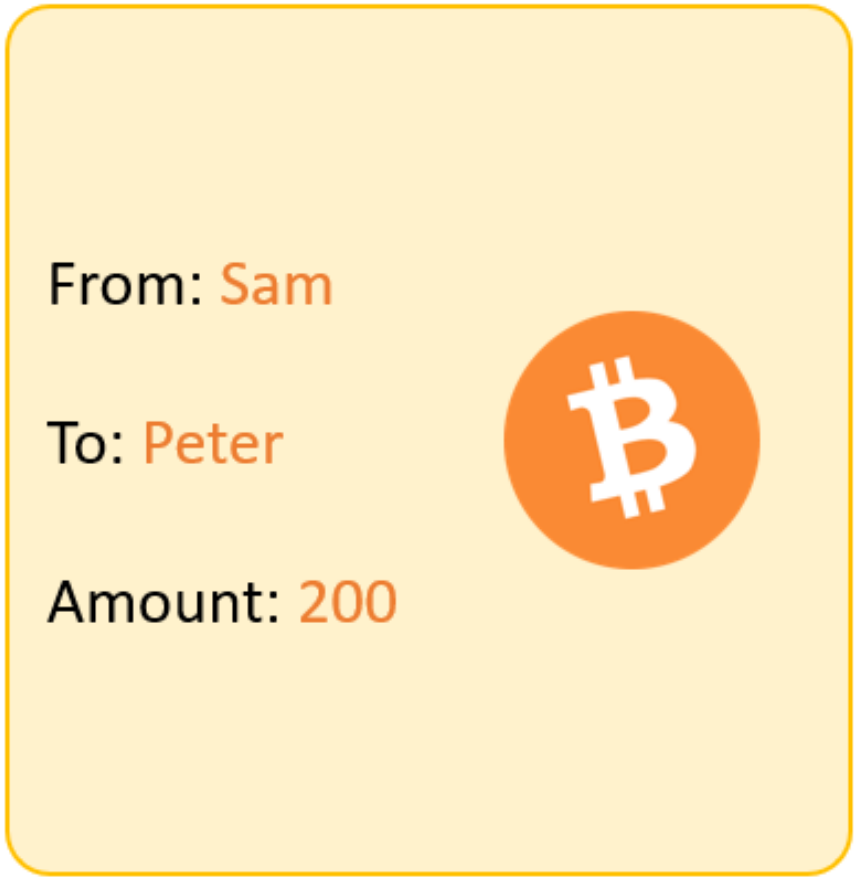
Qué NO es blockchain

- No es bitcoin, pero es la tecnología detrás de Bitcoin
- Bitcoin es el token digital, y Blockchain es el libro de cuentas
- No puede existir Bitcoin sin Blockchain, pero sí blockchain sin Bitcoin

Arquitectura Blockchain



Ejemplo de Bloque



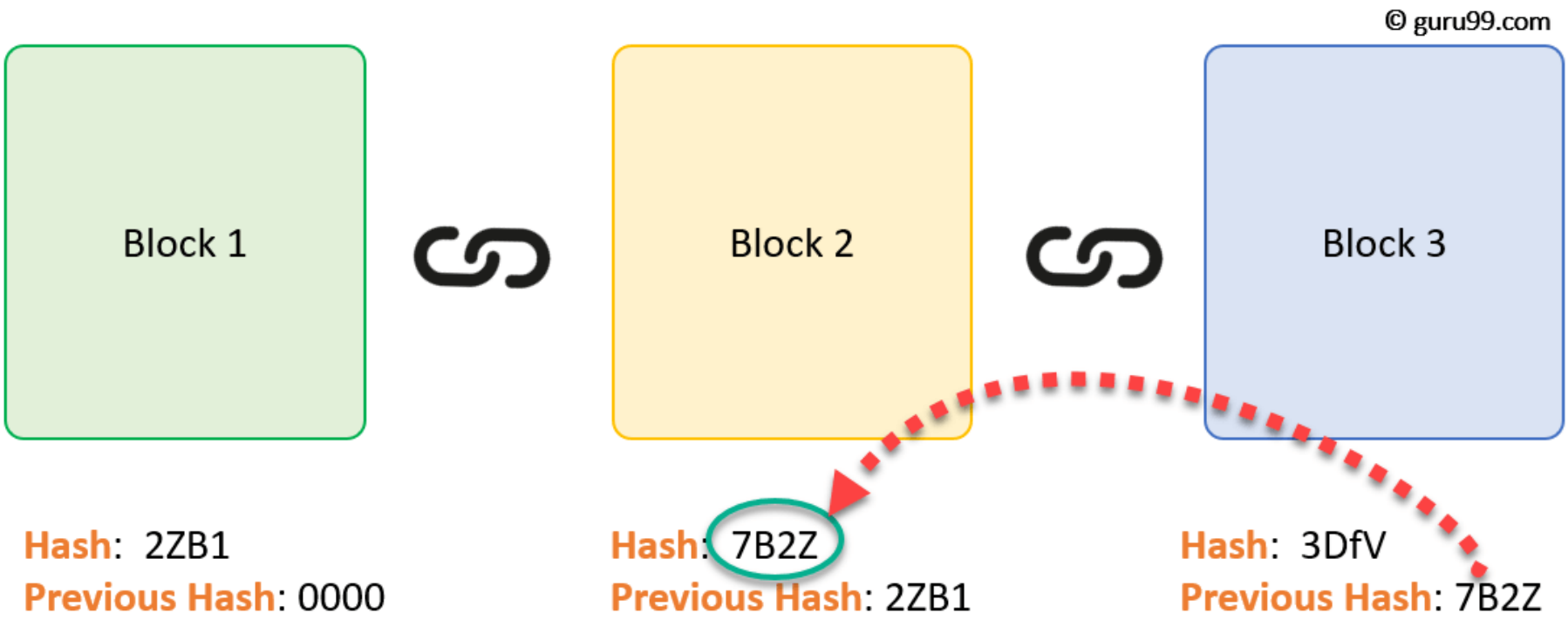
Bitcoin Block Example

Hash SHA256

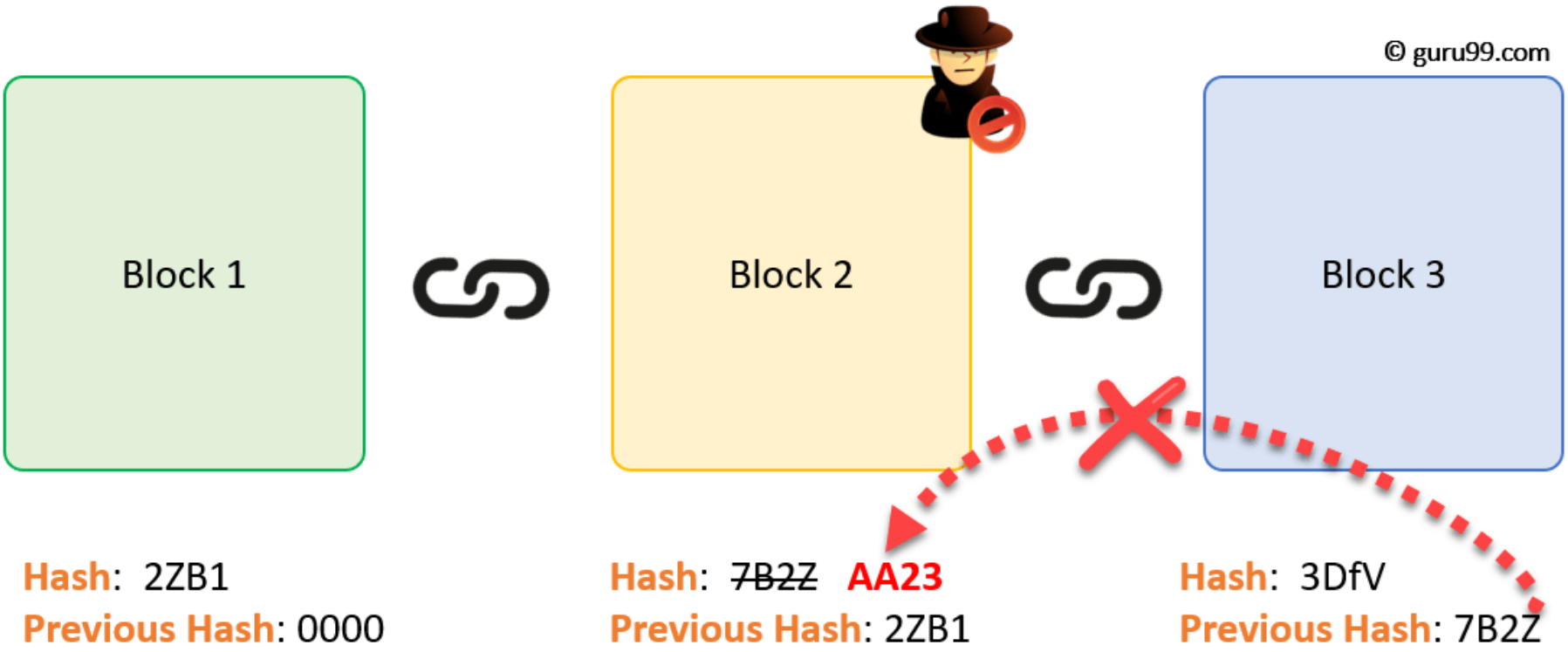
HASH:
7E0CE566ED2900D81508C7
768A05A4A50CCBC3632E72
EE8D32DE69636B663362

Hash acts as a Unique Fingerprint of the Block

Cadena de bloques

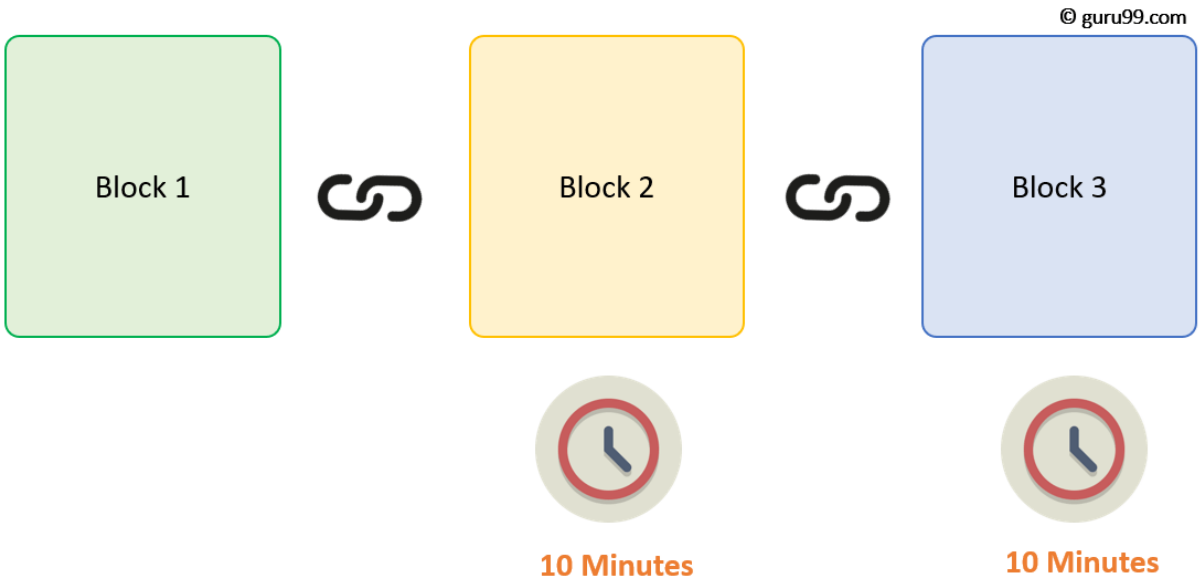


Resistencia a ataques



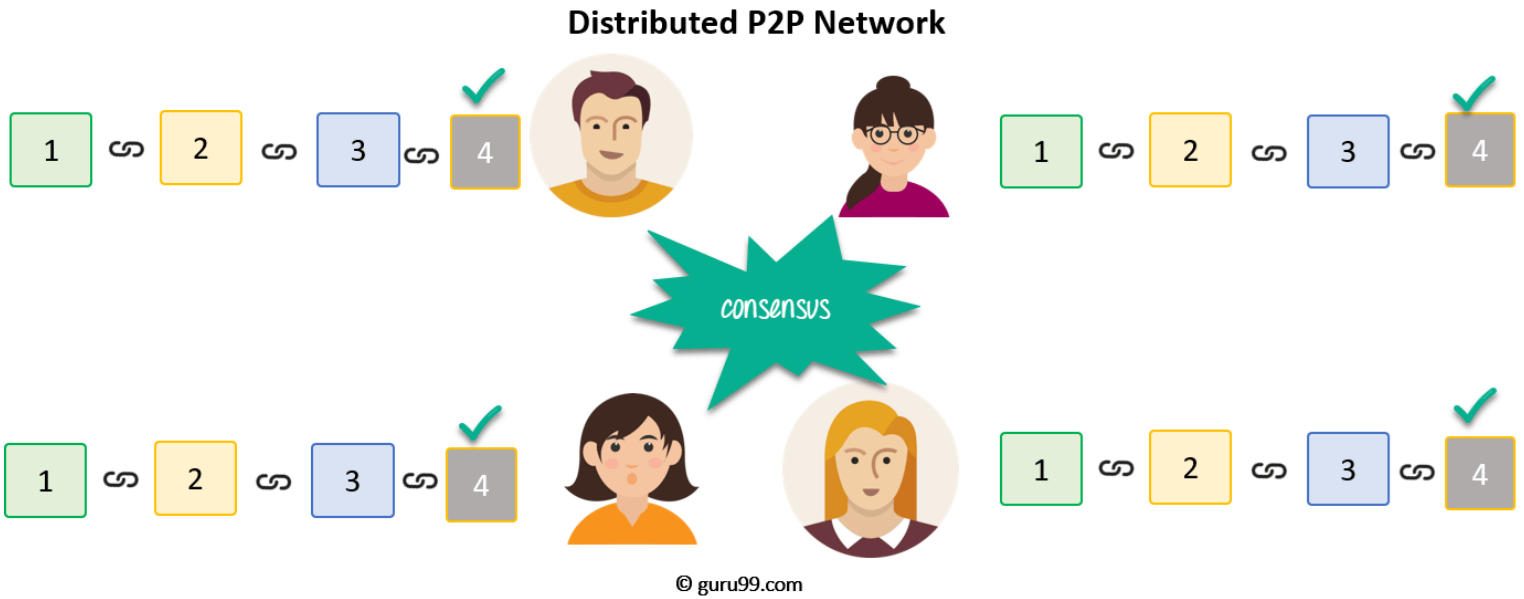
Prueba de trabajo

- Actualmente hay suficiente velocidad computacional para recalcular todos los bloques.
- Prueba de trabajo: mecanismo que relentiza la creación de nuevos bloques
- Es un problema computacional que requiere mucho tiempo para resolver, pero poco tiempo para verificar su resultado.
- En el caso de Bitcoin se tardan 10 minutos en añadir un nuevo bloque a la cadena



Red P2P Distribuida

- Cualquiera puede unirse a una red P2P.
- Cuando alguien se une, recibe una copia del blockchain. Cada ordenador se denomina nodo.
- Cuando un usuario crea un nuevo bloque se envía a todos los usuarios de la red.
- Cada usuario comprueba que no ha sido alterado y lo añade a la red.
- Los nodos crean un consenso



Sección 2 | Transacciones Blockchain

¿Cómo funcionan las transacciones en blockchain?

1. Una persona solicita una transacción (para criptomonedas, contratos, registros u otra información).
2. La transacción solicitada se transmite a una red P2P con la ayuda de nodos.
3. La red de nodos valida la transacción y el estado del usuario con la ayuda de algoritmos conocidos por todos.
4. Una vez completada la transacción, el nuevo bloque se añade al bloque existente. De forma permanente e inalterable.

¿Por qué usar blockchain?

- Resilencia: Blockchain suele basarse en arquitectura replicada. La cadena sigue siendo utilizada por la mayoría de los nodos en caso de un ataque masivo contra el sistema.
- Reducción de tiempos: En la industria financiera, puede desempeñar un papel vital al permitir la liquidación más rápida de las operaciones, ya que no necesita un largo proceso de verificación, liquidación y compensación, ya que existe una única versión de los datos acordados.
- Fiabilidad: Blockchain certifica y verifica la identidad de las partes interesadas. Esto elimina los registros dobles, reduciendo las tasas y acelerando las transacciones.

¿Por qué usar blockchain? (2)

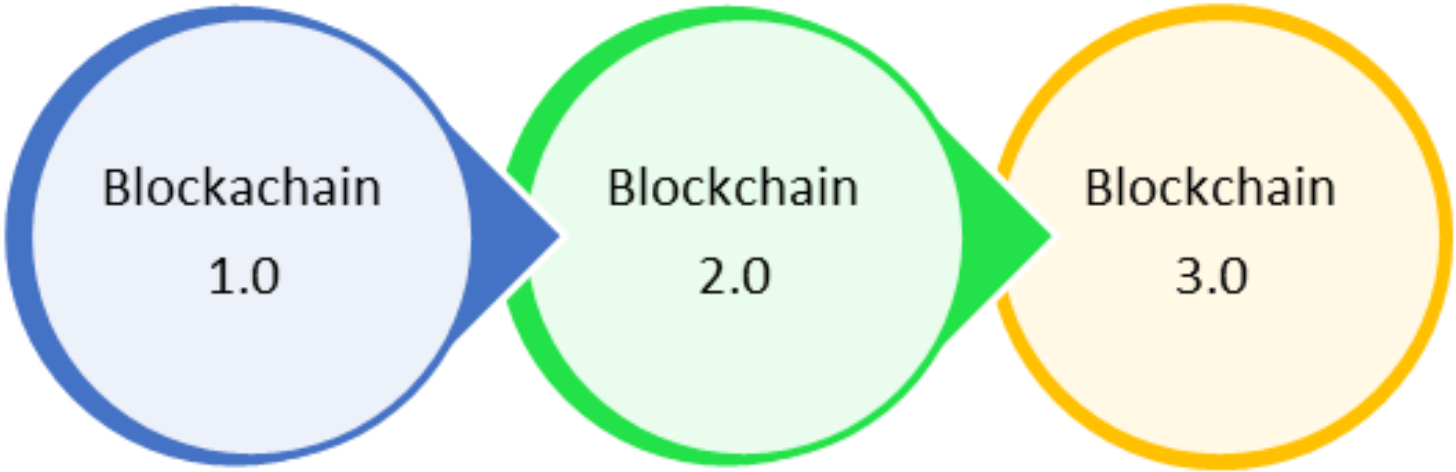
- Transacciones inalterables: Al registrar las transacciones en orden cronológico, Blockchain certifica la inalterabilidad de todas las operaciones, lo que significa que cuando se añade un nuevo bloque a la cadena de libros de cuentas (*ledgers*), no se puede eliminar ni modificar.
- Prevención de fraudes: Los conceptos de información compartida y consenso previenen posibles pérdidas por fraude o malversación. En las industrias basadas en la logística, blockchain se puede usar como mecanismo de monitorización para reducir los costes.
- Seguridad: Atacar una base de datos tradicional consiste en derribar un objetivo específico. Con blockchain, cada parte tiene una copia de la cadena original, por lo que el sistema permanece operativo, incluso cuando un gran número de otros nodos caen.

¿Por qué usar Blockchain? (3)

- Transparencia: Los cambios en blockchains públicas son visibles públicamente para todo el mundo. Esto ofrece una mayor transparencia y todas las transacciones son inmutables.
- Colaboración: Permite a las partes realizar transacciones directamente entre ellas sin necesidad de mediar con terceros.
- Descentralización: Hay reglas de estándares sobre cómo cada nodo intercambia la información en el blockchain. Este método asegura que todas las transacciones sean validadas y que todas las transacciones válidas se añadan una por una.

Sección 3 | Versiones y Variantes de Blockchain

Versiones



Blockchain 1.0: Moneda

La implementación de DLT (tecnología de *ledger* distribuido) llevó a su primera y obvia aplicación: las criptomonedas. Permite transacciones financieras basadas en la tecnología de bloques. Se utiliza en moneda y pagos. Bitcoin es el ejemplo más destacado en este segmento.

Blockchain 2.0: Contratos inteligentes

Los nuevos conceptos clave son los contratos inteligentes, pequeños programas informáticos que "viven" en el blockchain. Son programas informáticos libres que se ejecutan automáticamente y chequean condiciones definidas anteriormente como la facilitación, verificación o el cumplimiento. Se utiliza como sustituto de los contratos tradicionales.

Blockchain 3.0: DApps

DApps es una abreviatura de aplicación descentralizada. Tiene su código backend ejecutándose en una red descentralizada peer-to-peer. Un DApp puede tener código de frontend e interfaces de usuario escritos en cualquier lenguaje que pueda hacer una llamada a su backend, como una aplicación tradicional.

Variantes

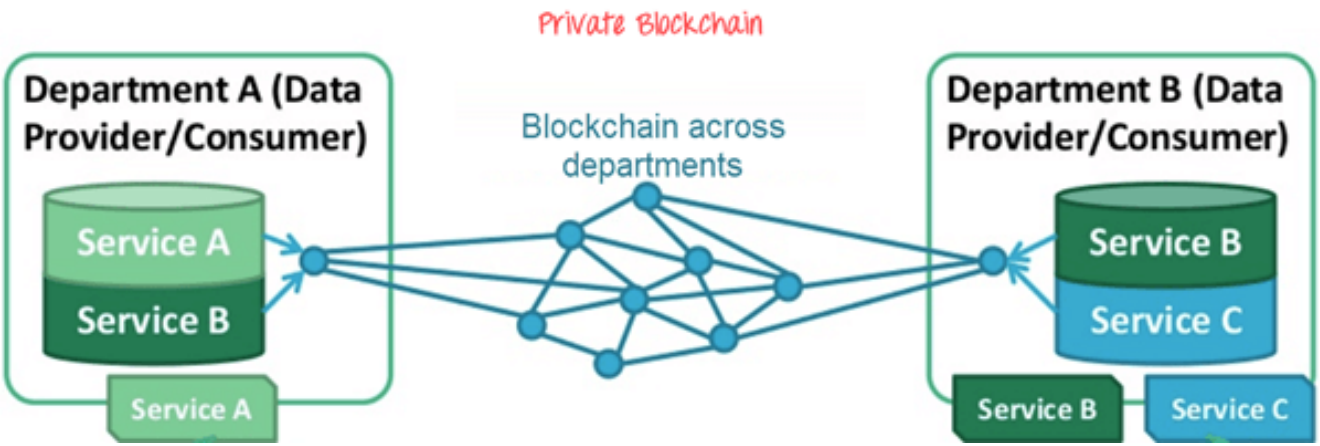
- Públicas
- Privadas
- Consorcio

Públicas

En este tipo de cadenas de bloques, los libros de contabilidad son visibles para todo el mundo en Internet. Permite a cualquiera verificar y añadir un bloque de transacciones a la cadena de bloques. Las redes públicas tienen incentivos para que las personas se unan y sean gratuitas para su uso. Cualquiera puede usar una red pública de bloques.

Privadas

La cadena privada de bloques está dentro de una sola organización. Permite que sólo personas específicas de la organización verifiquen y añadan bloques de transacciones. Sin embargo, a todo el mundo en Internet se le permite generalmente ver.



Consorcio

En esta variante de sólo un grupo de organizaciones puede verificar y añadir transacciones. Aquí, el *ledger* puede estar abierto o restringido a grupos seleccionados. La cadena de bloques del consorcio se utiliza en todas las organizaciones. Sólo está controlado por nodos preautorizados.

Sección 4 | Casos de uso

Mercados

1. Facturación, supervisión y transferencia de datos
2. Gestión de cuotas en la red de la cadena de suministro

Gobiernos

1. Servicios transnacionales de gobernanza personalizada
2. Votación, propuestas de bonos P2P
3. Digitalización de documentos/contratos y comprobantes de propiedad para transferencias
4. Registro e identificación
5. Servicio de tele-abogado
6. Registro e intercambio de propiedad intelectual
7. Comprobantes fiscales Servicio de notaría y registro de documentos

IOT

1. Redes de sensores agrícolas y de drones
2. Redes domésticas inteligentes
3. Smartcity integrada.
4. Sensores inteligentes para el hogar
5. Autoconducción
6. Robots personalizados, componentes robóticos
7. Drones personalizados
8. Asistentes digitales

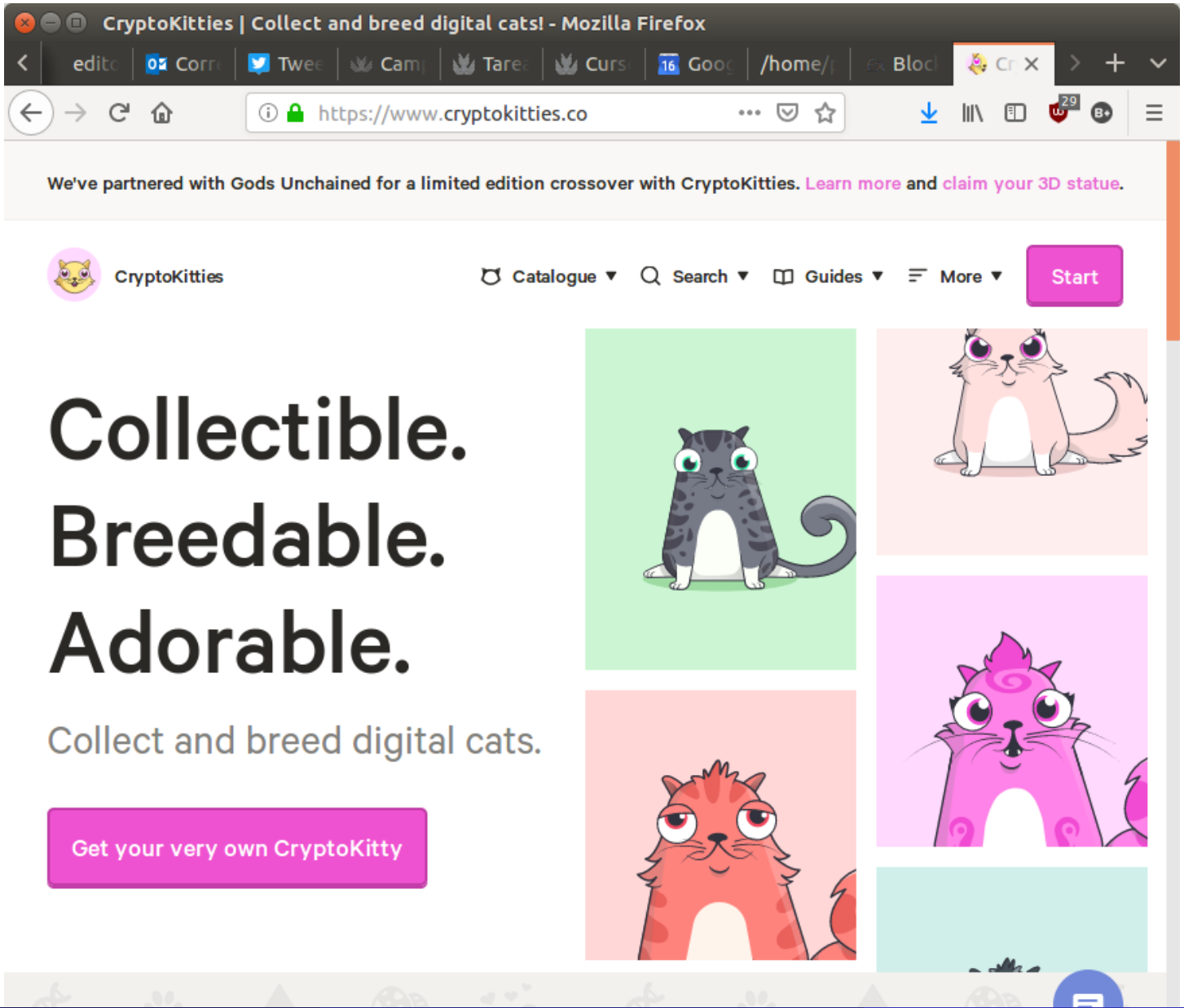
Salud

1. Gestión de datos
2. Bancos de datos médicos universales sobre salud
3. QS (Quantified Self) Data Commons
4. Grandes análisis de flujo de datos de salud
5. Cartera de salud digital inteligente
6. Ficha de salud
7. Contratos de desarrollo personal

Arte y Ciencia

1. Supercomputación
2. Análisis de multitudes
3. Recursos P2P

Cripto-Kitties



Transacción Cripto-Kitties

https://etherscan.io/tx/0x42f49d70ecae112343f5a7b1000287641a826455e9d00e5e6ac4d41db89affbb

The Ethereum Block Explorer

HOME | BLOCKCHAIN | TOKENS | RESOURCES | MORE

Transaction 0x42f49d70ecae112343f5a7b1000287641a826455e9d00e5e6ac4d41db89affbb

Home / Transactions / Tx

Etherscan - Sponsored slots available. **Book your slot here!**

Overview | Internal Transactions | Event Logs (2) | Comments | Loa

Transaction Information

Tools & Utilities

TxHash:	0x42f49d70ecae112343f5a7b1000287641a826455e9d00e5e6ac4d41db89affbb
TxReceipt Status:	Success
Block Height:	7075885 (1 Block Confirmation)
TimeStamp:	31 secs ago (Jan-16-2019 12:24:24 PM +UTC)
From:	0xfe5be95a00b0ff19573090002666edf604a7916b
To:	Contract 0xb1690c08e213a35ed9bab7b318de14420fb57d8c (CryptoKitties_SalesAuction) TRANSFER 0.003914523456695333 Ether From 0xb1690c08e213a35ed9... To 0xcfee1c9c3a4e8e709e2f... TRANSFER 0.000001363936136 29 Ether From 0xb1690c08e213a35ed9... To 0xfe5be95a00b0ff195730...
Tokens Transfered:	From 0xb1690c08e213a35...To 0xfe5be95a00b0ff19... For ERC-721 TokenID [1312254] CK
Value:	0.004068401293741 83 Ether ($0.52)
Gas Limit:	158820
Gas Used By Transaction:	60508 (38.1%)

Finanzas

1. Pago en moneda digital
2. Pagos y Remesas
3. Mercados de capital desvinculados
4. Contabilidad interdivisional
5. Compensación y Negociación y Derivados
6. Contabilidad

Sección 5 | Bitcoin

¿Qué es una criptomoneda?

Una criptomoneda es un medio de intercambio como las monedas tradicionales como el EUR, pero está diseñada para intercambiar la información digital a través de un proceso hecho posible por ciertos principios de criptografía. Una criptocurrencia es una moneda digital y se clasifica como un subconjunto de monedas alternativas y monedas virtuales. Una criptomoneda es un instrumento portador basado en criptografía digital. En este tipo de criptomoneda, el titular tiene de la moneda tiene la propiedad. No se lleva ningún otro registro de la identidad del propietario. Cualquiera puede usar bitcoin sin pagar ninguna cuota de proceso. Si se trata de Bitcoin, el remitente y el destinatario realizan la transacción directamente sin necesidad de recurrir a un tercero.

¿Qué es Bitcoin?

En el año 1998, Wei Dai publicó "B-Money", un sistema anónimo de dinero electrónico distribuido.
Bitcoin fue lanzado en 2009 por un desconocido llamado Satoshi Nakamoto.
Bitcoin es una tecnología P2P que no está gobernada por ninguna autoridad central ni bancos. Actualmente, la emisión de Bitcoins y la gestión de las transacciones se llevan a cabo de forma colectiva en la red. Actualmente es la criptomoneda dominante en el mundo.
Es de código abierto y está diseñado para el público en general, lo que significa que nadie posee el control de Bitcoin. De hecho, sólo se han emitido 21 millones de Bitcoins. Actualmente, Bitcoin tiene una capitalización de mercado de 12.000 millones de dólares.

Blockchain y Bitcoin

La cadena de bloques es la tecnología detrás de Bitcoin. Bitcoin es el token digital, y blockchain es el libro de cuentas (*ledger*) que lleva la cuenta de quién es el propietario de los tokens digitales. No se puede tener Bitcoin sin blockchain, pero se puede tener blockchain sin Bitcoin.
Otras criptomonedas destacadas:

- Ethereum
- Bitcoin Cash
- Ripple
- Litecoin
- Dogecoin

Mitos sobre Blockchain

Mito	Realidad
Resuelve todos los problemas	No, es sólo una base de datos
Tecnología sin confianza	Puede cambiar la confianza y también difundirla
Privada	Se centra en la integridad y no en la confidencialidad
Inmutable	Sólo ofrece inmutabilidad probabilística

Limitaciones de Blockchain

- Riesgo de error: Siempre existe el riesgo de error, siempre y cuando esté involucrado el factor humano. En caso de que una cadena de bloques sirva como base de datos, todos los datos entrantes deben ser de alta calidad.
- Desperdiciable: Cada nodo que ejecuta la cadena de bloques tiene que mantener el consenso a través de la cadena de bloques. Esto ofrece un tiempo de inactividad muy bajo y hace que los datos almacenados en la cadena de bloques sean inalterables para siempre. Sin embargo, todo esto es un desperdicio, porque cada nodo repite una tarea para llegar a un consenso.

Conclusiones

- Blockchain es una cadena de bloques que contienen información
- La cadena de bloques no es Bitcoin, pero es la tecnología que hay detrás de Bitcoin.
- Cada bloque contiene su hash.
- Cada bloque tiene un hash del bloque anterior.
- La cadena de bloques requiere una prueba de trabajo antes de añadir un nuevo bloque.
- La base de datos de la cadena de bloques se distribuye entre múltiples pares y no está centralizada.
- La tecnología de la cadena de bloques ofrece Resiliencia, Descentralización, Reducción de tiempo, confiable y ofrece transiciones inalterables.

Referencias

- https://medium.com/@mvmurthy/full-stack-hello-world-voting-ethereum-dapp-tutorial-part-
- https://www.guru99.com/blockchain-tutorial.html