

# Seminario Blockchain

## Clase Práctica N°1

Profesor:

- Esp. Ing. Fernando Boiero

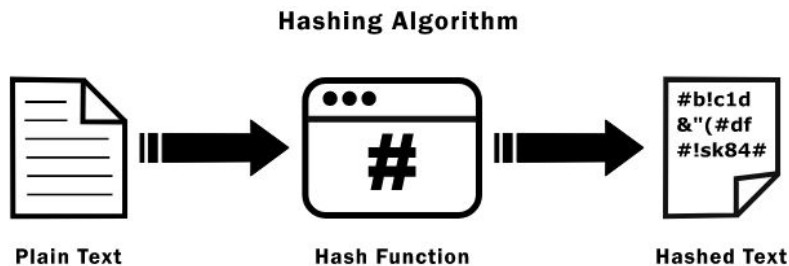
# Blockchain Demo: Parte 1

- Demostración de Blockchain Visual, fácil de entender para que nos pongamos en tema.
- Iremos viendo las partes claves de una Blockchain.



# SHA 256 - Secure Hash Algorithm

- Son un montón de números random. Es la huella digital de cualquier tipo de dato o información.
- Veamos ahora un ejemplo de esto en la [Blockchain de ejemplo...](#) Escribiremos palabras y veremos cómo va cambiando el hash. Siempre que pongamos la misma información... el hash va a ser el mismo... ya si modificamos algo el hash va a cambiar.




- Extendamos un poco más la idea de un Hash y vemos la siguiente idea...

# Características del algoritmo SHA-256

Un algoritmo hash **funciona en una sola dirección**: esto quiere decir que de cualquier contenido podemos generar su hash (su “huella digital”) pero de un hash no hay forma de generar el contenido asociado a él, salvo probando random hasta dar con el contenido.

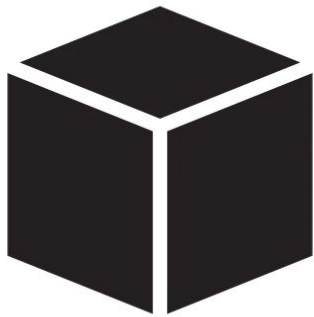
Entre las diferentes formas de crear hashes, el algoritmo usado por SHA-256 es uno de los más usados por su **equilibrio entre seguridad y costo computacional de procesamiento para la generación** del mismo.

Otra de las particularidades del algoritmo de hash SHA-256 es que la **longitud del hash resultante es siempre igual**, no importa lo largo que sea el contenido que uses para generar el hash: ya sea de una letra o todas las palabras de un Libro entero, el resultado siempre es una cadena de 64 letras y números (con una codificación de 256 bits, 32 bytes).



# Bloque

- En un Bloque observamos los campos “Data” y “Hash”... agregando también el “Número del Bloque” y el “Nonce”.
- Hash empieza con 4 ceros... ¿Qué significa eso?



¡Que el Bloque está firmado!



- Ahora, agregaremos información en "Data"... Se pondrá rojo y lo mismo significa que no está firmado. Por lo que se asume que no es válido en la Blockchain.
- **Nonce:** Número que se busca obtener para que haya 4 ceros al comienzo del Hash. (1,2,3...10000)
- **Botón de Minado:** Cuando lo apretamos, con el texto que tenga el bloque o que hayamos puesto... Se va a buscar el Nonce que haga que el Hash tenga 4 ceros al comienzo del mismo, obteniendo la firma del Bloque (En este caso la dificultad de minado para el bloque es de 4 ceros antes... eso depende de la dificultad que se establezca a la minería en determinado momento).



**¿Qué es una Blockchain para ustedes?**

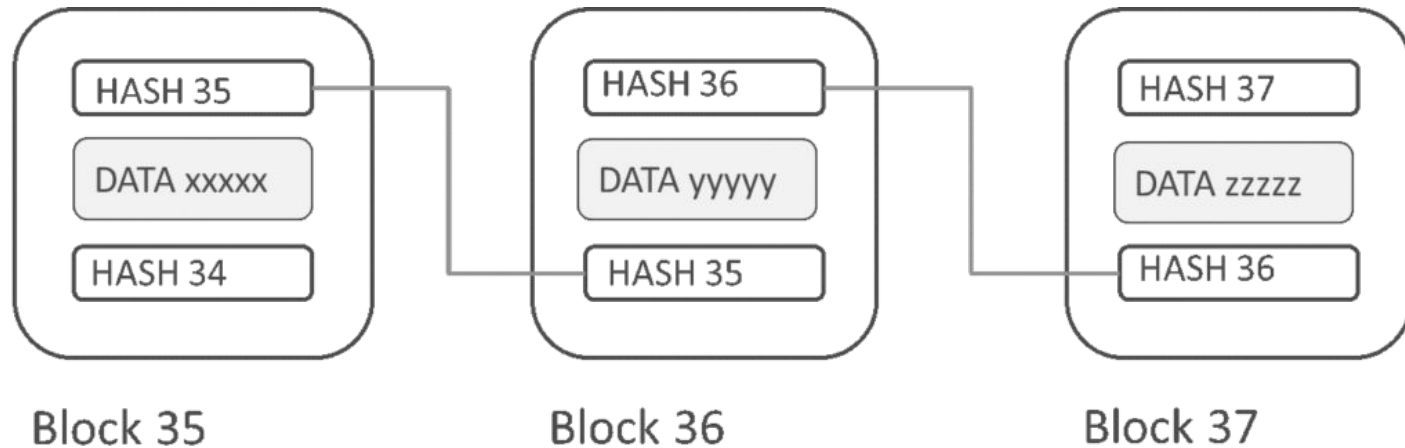


The background of the image features a repeating pattern of stylized, light blue cubes connected by thin lines, creating a three-dimensional, isometric effect that represents a blockchain structure.

**Blockchain**



Una blockchain, originalmente **cadena de bloques**, es una lista creciente de registros, llamados bloques, que están vinculados mediante criptografía. Cada bloque contiene un hash criptográfico del bloque anterior, una marca de tiempo y datos de transacciones.



# Blockchain

- Conjunto de “Bloques”. Uno seguido al otro con un orden específico.
- Cada “Bloque” apunta al anterior. En “Prev” del bloque que estoy parado va el Hash del Bloque Previo.
- El Bloque #1 no tiene previo... Se denomina Bloque GÉNESIS y lleva muchos ceros en Prev.



- Veamos qué pasa si modificamos un Bloque, sea el último de la cadena o alguno en el medio... observamos que la Blockchain se rompe!

¡Tenemos que re-minar la cadena!

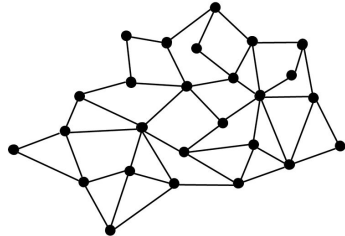
- Cuanto más para atrás se altere la Blockchain más difícil va a ser generar un cambio.
- Ahí podemos ver la resistencia de una Blockchain a mutaciones o cambios.

¿Cómo vemos que nuestra Blockchain fue Re-Minada? ¿Cómo detectamos eso?



# Blockchain Distribuida

- Se ve como la anterior... Pero hay **Peer A,B,C...** En fin hay muchos que son **contenedores de una réplica de la Blockchain**, todos distribuidos mediante internet. Cada uno tiene una copia completa de la cadena.
- Veamos que el último Hash por ejemplo de Peer A,B,C... es idéntico. Si cambiamos alguno de los Bloques del peer A, veremos que se altera la cadena en ese Peer... pero los demás siguen intactos. Si la minamos...por más que se ponga verde, el Hash del último bloque no va a ser el mismo. La red de Peers, al ver que A es diferente a B y C, no la va a aprobar, gana B y C.
- Las Blockchains tienen muchísimos bloques... por lo que siempre se guían en base a los números Hash para ver que todo esté en orden.



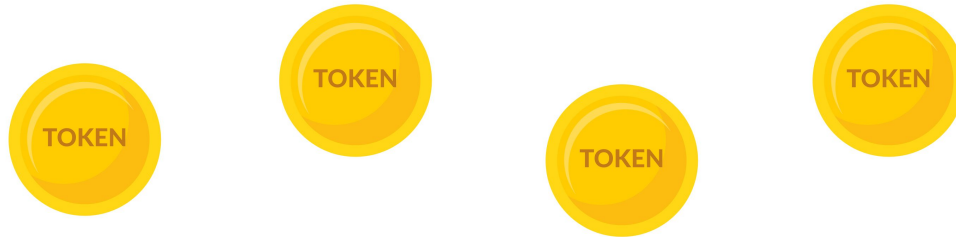
Eso es una Blockchain en sí, pero con esto no hacemos mucho que digamos. Veamos un poquito más...

Veamos un poco más y estudiemos ¿qué es un "Token"?



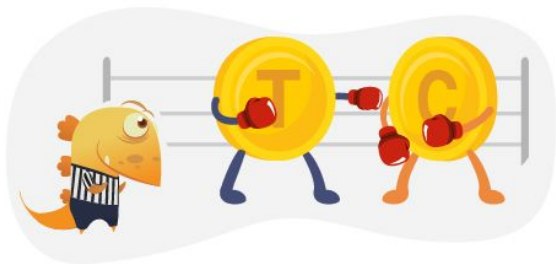
# Tokens

- Tx. (Transactions) en este caso son en dólares. De diferentes personas y montos cada una.
- Veamos que en cada Bloque hay varias transacciones... y las mismas están replicadas en las demás Blockchains de los otros Peers!
- Si alguien altera algún valor en el pasado de alguna transacción de dinero por ejemplo entre 2 personas, lo vamos a detectar y nos notificaremos a simple vista. Es muy importante que con la plata no se pierda el registro y ese es el punto fundamental para usar una blockchain en este caso! Se resiste a cualquier tipo de modificación de cosas que hayan pasado en el pasado.
- En este caso vemos que solo se registran transacciones entre personas, pero no se tiene en cuenta cuánta plata tiene cada uno... el balance. Vemos lo siguiente ya que algo no estaría del todo bien...



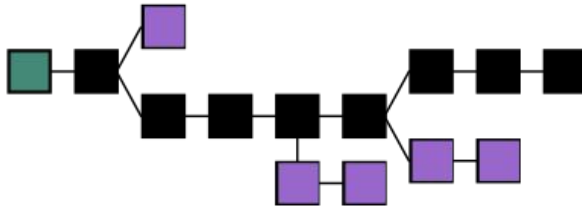
# Diferencia entre Token y Criptomoneda

- Ahora bien, en este punto seguro estarás confundido entre lo que es un token y una criptomoneda. Y la respuesta corta para terminar esta confusión es que **un token y una criptomoneda son cosas distintas**. Muy distintas en realidad.
- Por un lado, una criptomoneda es creada desde el principio con la firme intención de ser un medio de intercambio. Uno que cuenta con su propia blockchain y que no depende de otro sistema para su funcionamiento. En definitiva, una criptomoneda es un sistema de intercambio de valor autosostenible.
- Un token por el contrario no es ninguna de estas cosas. En primer lugar, un token es creado para representar cualquier cosa. Puede ser una casa, una acción de una empresa, un coleccionable, o las partes que conforman el todo de una línea de producción de aviones, incluyendo los aviones mismos. Si se pueden usar como un medio de pago o de intercambio, pero su objetivo es ser un medio para representar cosas del mundo real.
- Lo segundo, es que un token depende de otro sistema para funcionar, es decir, no son autosostenibles. Por ejemplo, los tokens de Ethereum no serían nada si la blockchain de Ethereum y su criptomoneda el Ether no existieran.



# Coinbase Transactions

- Le vamos a agregar una Coinbase Tx a nuestros bloques y le vamos a asignar un monto inicial a una Persona.
- Luego en los siguientes Bloques vamos a distribuir esa plata entre diferentes personas. Teniendo en cuenta que el monto total para operar es el capital inicial. No es que se pueda inventar plata.
- Esto se podría realizar para múltiples monedas en una misma blockchain y demás funciones que ya iremos viendo más adelante.
- Los nodos tienen una copia de la blockchain y son los que van a decidir o mejor dicho validar que los bloques estén de manera correcta y no haya alteraciones.





Eso sería una Blockchain simplificada, ya adentraremos más en temas específicos pero espero que haya quedado todo claro. Cualquier duda la respondemos!

### **Consigna:**

Levantar el proyecto en Localhost e interactuar con el mismo:

<https://github.com/anders94/blockchain-demo>



# Herramientas:



- Git:

<https://www.hostinger.com.ar/tutoriales/instalar-git-en-distintos-sistemas-operativos>

- node.js: <https://nodejs.org/en/download/>

- npm: <https://www.npmjs.com/>

- Docker (docker-compose up -d)

<https://docs.docker.com/compose/reference/up/>



## What is a Peer to Peer Network?

# P2P Networks



Blockchain - YAP  
Island...

