

GUÍA DEL ASESOR BLOCKCHAIN

LÍNEA BLOCKCHAIN		
II. NÚCLEO ESPECÍFICO		b. Fundamentos de blockchain
Sesión 5	Clasificación de los diferentes protocolos	Tiempo: 3 hora

Con antelación verificar si se cuenta con:

Aula virtual	X	Accesos	X	Presentación	X	Recursos		Cámara y micrófono	X
--------------	---	---------	---	--------------	---	----------	--	--------------------	---

- Explorador de internet. - Office

Objetivos

- Entender el concepto general de los métodos de consenso en una Blockchain para tomar decisiones de grupo.
- Conocer las características particulares de los métodos de consenso.
- Conceptualizar el problema de la tolerancia a fallas Bizantinas.
- Identificar los métodos de consenso utilizados en las diferentes cadenas de bloques.
- Establecer el método de consenso idóneo para el caso de estudio de la empresa

Introducción al tema

En esta sesión revisaremos la clasificación de los diferentes métodos de consenso utilizados en las cadenas de bloques y su importancia para el funcionamiento de estas, son el núcleo de esta tecnología porque a través de dichos métodos se establecen las reglas necesarias para asegurar que el bloque de transacciones que se añadirá a la cadena, sea el que contiene la única versión verificada y aprobada por todos los nodos.

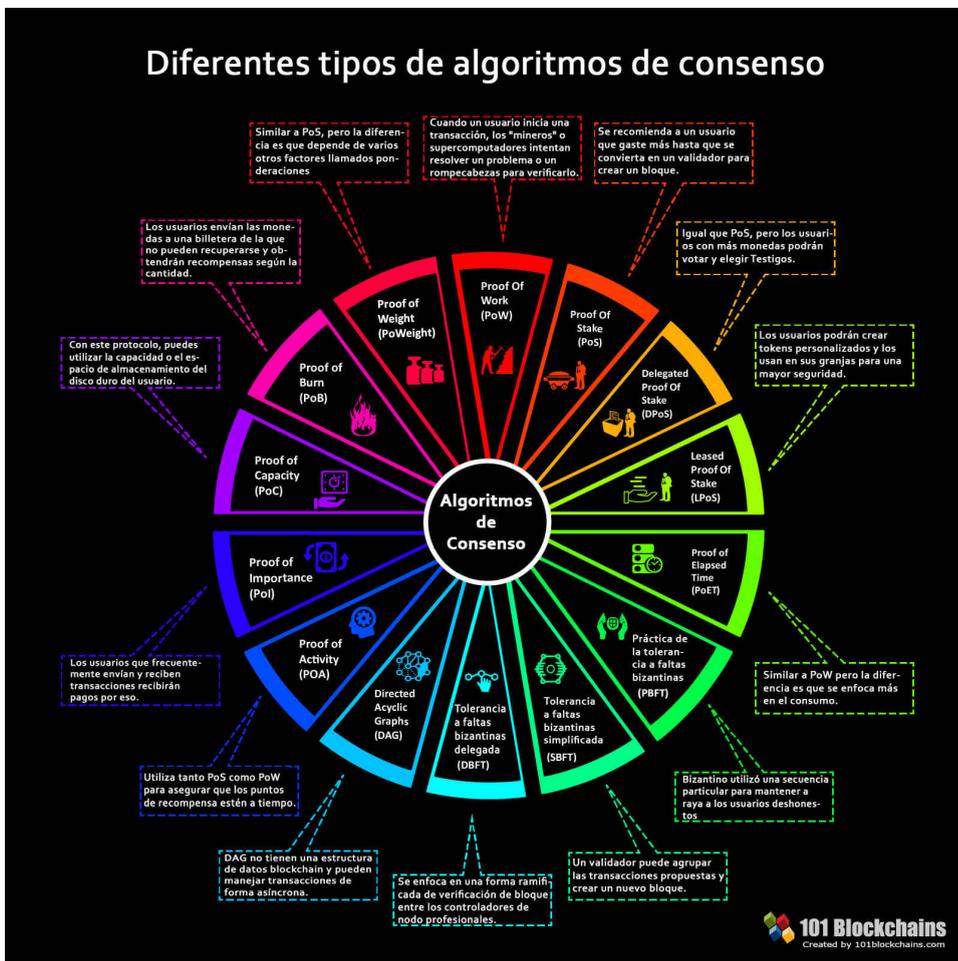
Los métodos de consenso son la pieza clave para lograr la descentralización de manera segura, su objetivo principal es que todos los nodos participantes de la red hablen el mismo idioma, están diseñados para tomar decisiones por la mayoría de participantes que beneficien la red sin importar que algunos de ellos no estén de acuerdo o actúen de manera corrupta. Un método de consenso permite que se logre identificar una transacción fraudulenta y sea rechazada por no cumplir las reglas establecidas por la red, proporcionando una capa de seguridad programada y descentralizada que no se tenía en sistemas anteriores, reduciendo la posibilidad de ataques del 51% casi a cero.

También conoceremos la evolución de estos métodos en los sistemas blockchain desde el Bitcoin e identificaremos ventajas y desventajas de los mismos

Finalmente, en esta sesión se hará énfasis en la elección del método idóneo para el caso de estudio de cada empresa.

Objetivos específicos de los métodos de consenso:

- **Llegar a un acuerdo:** El mecanismo reúne todos los acuerdos del grupo tanto como puede.
- **Colaboración:** Cada uno en el grupo apunta a un mejor acuerdo que resulte en los intereses colectivos del grupo.
- **Cooperación:** Cada miembro trabaja en equipo y dejá de lado sus propios intereses.
- **Igualdad de derechos:** Cada uno de los participantes tiene el mismo valor en la votación. Esto significa que el voto de cada persona es importante.
- **Participación:** Todos los que están dentro de la red deben de participar en la votación. Nadie se queda fuera o nadie puede quedarse fuera de la votación.
- **Actividad:** Cada miembro del grupo es igualmente activo. No hay miembros con más responsabilidades que otros en el grupo.



https://101blockchains.com/wp-content/uploads/2018/09/Algoritmos_de_consenso.jpg

- Prueba de trabajo (PoW)
- Prueba de participación (PoS)
- Prueba de participación delegada (DPoS)

- Prueba de participación arrendada (LPoS)
- Prueba de tiempo transcurrido (PoET)
- Práctica de tolerancia a faltas bizantina
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn

Método: Propuesta pedagógica

La sesión se realizará de forma sincrónica a distancia a través de la plataforma TEAMS.

- Primera parte: charla magistral de un invitado especial para todos los participantes de la línea blockchain, se realizará con apoyo audiovisual y una ronda de preguntas para resolver las dudas de los participantes presentes.
Duración: 1 hora.
- Segunda parte: los participantes se dirigen a sus respectivos grupos con su asesor asignado. El asesor contextualizará y profundizará el tema de la sesión, y responderá a las preguntas de los participantes que tengan relación con la conferencia. Se realizarán las actividades previstas con acompañamiento del asesor blockchain, utilizando demos para reforzar conocimientos a través de la práctica.
Duración: 2 horas.

Habilidades y competencias desarrolladas

- Entendimiento general del concepto de los métodos de consenso
- Conocimiento de las características principales del consenso
- Identificar los diferentes métodos de consenso y sus características

Recursos

- Explorador de Internet
- <https://www.youtube.com/watch?v=ltr1a6VLpHM&t=10s>
- <https://coinmarketcap.com/>
- Office instalado

Instrucciones

Actividad 1

Identificar algoritmos de consenso de protocolos disponibles en Coinmarketcap

Elegir un token o criptomoneda disponible en Coinmarketcap e identificar su método de consenso

Actividad 2

Juego de Bloques

OBJETIVO:

Explicar los métodos de consenso con el uso de definiciones simples mediante el uso de fichas que serán representadas como bloques de transacciones.

Overview:

Buscamos que los participantes encuentren el Hash correspondiente a cada bloque en secuencia correcta, con información encriptada en la metadata del bloque en la cual se encuentra la definición de uno de los métodos de consenso utilizados en las cadenas de bloques.

Fichas:

Las fichas estarán en un archivo powerpoint en el cual se desarrollará la actividad y un archivo excel donde encontrarán la tabla de encriptación.

Juego:

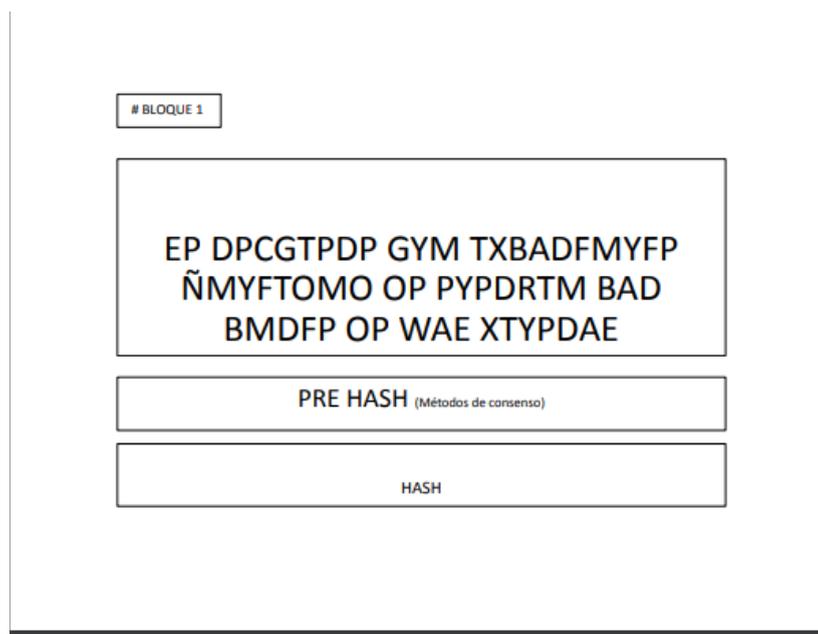
Cada jugador tendrá disponibles 6 fichas en archivo PPT, en la cual la primera de ellas tendrá la información del hash del bloque anterior.



Componentes:

- Número de Bloque:** Corresponde a la secuencia que debe llevar la cadena de bloques
- Metadata:** Contiene la definición del método de consenso del bloque actual de manera encriptada.
- Pre Hash:** Método de consenso del bloque anterior.
- Hash:** Método de consenso del bloque actual.

De esta manera tenemos que la primera ficha contiene el mensaje encriptado y el hash previo así:



En la tabla de encriptación encontrarán los datos para encontrar el mensaje o la definición en la metadata, con una encriptación muy sencilla en la que el único

parámetro es que el abecedario no empieza por la A sino por otra letra que deben encontrar.

El objetivo final, es descifrar 6 métodos de consenso escondidos en el juego y armar una Blockchain de 6 Bloques

ACTIVIDAD 2: IDEA DE PROYECTO

Mediante el cuestionario desarrollado por el BID, las empresas deberán responder si ¿es recomendable utilizar blockchain para resolver el problema identificado?

[Cuestionario 1](#)

BALANCE DEL DÍA

- Los participantes tendrán claro que no existe un solo algoritmo de consenso para sincronizar e incentivar los nodos de la red.
- Que hay alternativas al a prueba de trabajo más ecológicas en cuanto a consumo de energía
- Que dependiendo del tipo de red y de la confianza que se tenga en los nodos, se pueden utilizar diferentes algoritmos de consenso.
- No todos los algoritmos de consenso recompensan a los nodos.