

2022



`</codecrypto.academy>`

MÓDULO 2

Minería y Protocolos

¿Cómo nos ponemos de acuerdo en una red?

Copyright © codecrypto.academy



Tabla de contenidos

▼ 01

Section A

Minería y protocolos de consenso

▼ 02

Section B

Proof of Work

▼ 03

Section C

Proof of Stake

▼ 04

Section D

Delegated Proof of Stake

▼ 04

Section E

BFT, PBFT y dBFT: los protocolos bizantinos tolerantes a fallos

▼ 06

Section F

RAFT

▼ 07

Section G

Directed acyclic graph, Tangle y Hashgraph

▼ 08

Section H

Solo



Section A

Minería y protocolos de consenso



Protocolos de Consenso ¿Qué son?

- Es la base del funcionamiento de toda red DLT. Consiste en entender, **cómo la red se pone de acuerdo respetando unas normas preestablecidas para validar transacciones.**
- Por citar algunos de los más importantes, Proof of Work, Proof of Stake o Tangle.
- Es importante introducir en este punto, el por qué de la existencia de tantos protocolos. Es debido al **trilema** que plantean las redes DLT (lo analizaremos más adelante)

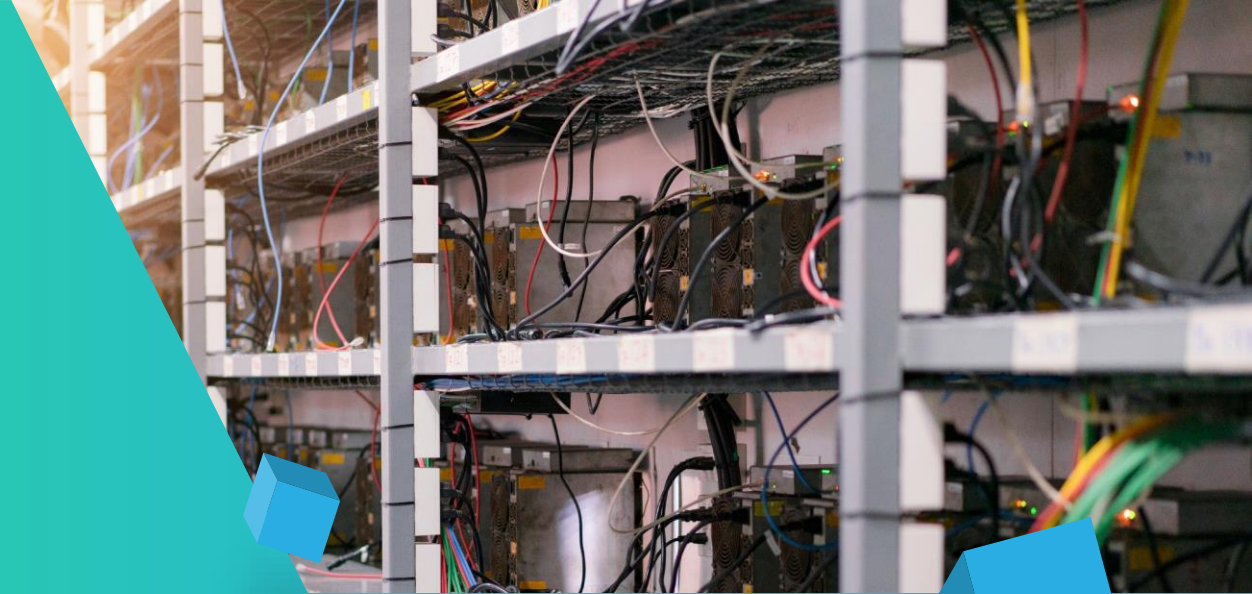




Minería – Explicación breve

- Como resumen inicial, la minería en redes descentralizadas como Bitcoin o Ethereum, no consiste en más que, potencia de computación intentando resolver un problema matemático propuesto por la red.
- Me explico: básicamente, para lo que sirven estas dos redes es para realizar intercambios (pagos) de manera descentralizada. Por lo que, en vez de que un banco diga si tienes fondos o no para pagar, lo decide la red (los ordenadores con su potencia de computación)

(Lo explicaremos con mucho más detalle a continuación)





Minería – ¿Por qué es necesario entenderla?

- Es la base del funcionamiento de una gran parte de redes DLT (ya que no todas se basan en minería).
- Consiste en cómo la red es recompensada al trabajar respetando el protocolo de consenso acordado dentro de esa red para validar transacciones.





Section B

Proof of Work



Proof of Work – ¿Qué es?

Es el protocolo de consenso que usa la red de Bitcoin.

- PoW se basa en que un participante de la red debe realizar un trabajo dentro de ella, consistente en la creación de un nuevo bloque **(minería)**. Por ese trabajo, cada participante que es capaz de crear (minar) un nuevo bloque, recibe una recompensa, que se paga en Bitcoin.
- Por esto, al proceso de creación de nuevos bloques se le llama minería, aunque lo que se están creando realmente son nuevos bloques, y por consecuencia Bitcoins para realizar las recompensas.

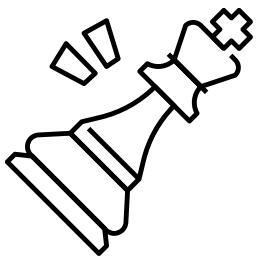




Jugadores



Reglas



Consecuencias



Recompensa

Recordatorio Teoría de Juegos

- **La Teoría de Juegos**, es la parte de las matemáticas que hace que todo sistema DLT tenga sentido.
- La idea principal, es que todas las partes implicadas sacan su beneficio si cumplen las reglas; de manera que a todas las partes les interesa seguir jugando.
- Pregunta: ¿Por qué en la red de Bitcoin nadie miente?



Proof of Work en Bitcoin

Características y Funcionamiento

- ✓ Existe un límite de creación de 21 millones de BTC
- ✓ La red de Bitcoin está diseñada para que cada 10 minutos se cree un bloque
- ✓ Cada bloque que se mina, se compone de 2048 transacciones, y cada transacción ocupa 0.5kB; por lo tanto cada bloque pesa 1MB (1024KB)
- ✓ Halving: Cada 210.000 bloques se reduce a la mitad la cantidad de BTC que se dan de recompensa
- ✓ Actualmente la recompensa por bloque minado son 6.25 BTC

- ✓ A parte de la recompensa, el minero recibe el fee asociado a cada transacción. Hay que tener en cuenta, que si el fee asociado no es lo suficientemente atractivo para los mineros, la transacción no será incluida para ese nuevo bloque, dando prioridad a los que más paguen (ese es el problema que está teniendo Ethereum a día de hoy)

El próximo Halving será en torno al 22 de mayo de 2024

(210.000 bloques X 10 min = 2.100.000 horas = 4 años)

Más info en: www.bitcoinblockhalf.com





Proof of Work en Bitcoin – Dificultad (Hashrate)

- **Cuantos más equipos** de minado añadas a la red, más aumenta tu capacidad de cómputo en ella. Por tanto, tendremos mayores posibilidades de minado.
- ¿Qué ocurre si no se consigue crear un bloque en los 10 minutos previstos, o por el contrario, se consigue antes de tiempo?

La red aumenta o disminuye la dificultad de minado para adecuarlo a 10 minutos.

- Hashrate o Hashpower: es la potencia que consume la red Bitcoin para estar continuamente en funcionamiento.
- Por funcionamiento continuo nos referimos a la cantidad de potencia que requiere la red para generar un bloque cada 10 minutos.





Proof of Work en Bitcoin – Creación de bloques

▼ 01

Imaginemos que quiero realizar un pago de 1 BTC a alguien, para lo cual, se crea una transacción a la cual se le asocia una comisión para el minero.

▼ 02

La transacción llega al pool (que es donde están listas todas las transacciones de todos los usuarios), y los mineros están continuamente seleccionando las mejor pagadas 2048 transacciones del pool, para generar el nuevo bloque.

▼ 03

El nodo (minero) que consigue resolver el problema matemático (basado en árboles de Merkle) propuesto por la red antes que los otros, propone la solución a los demás nodos, que deberán validar que está correctamente resuelto (esto significa, que si hay algún dato corrupto, como pueda ser que alguien quiere pagar sin realmente tener fondos para hacerlo, la red le va a pillar).

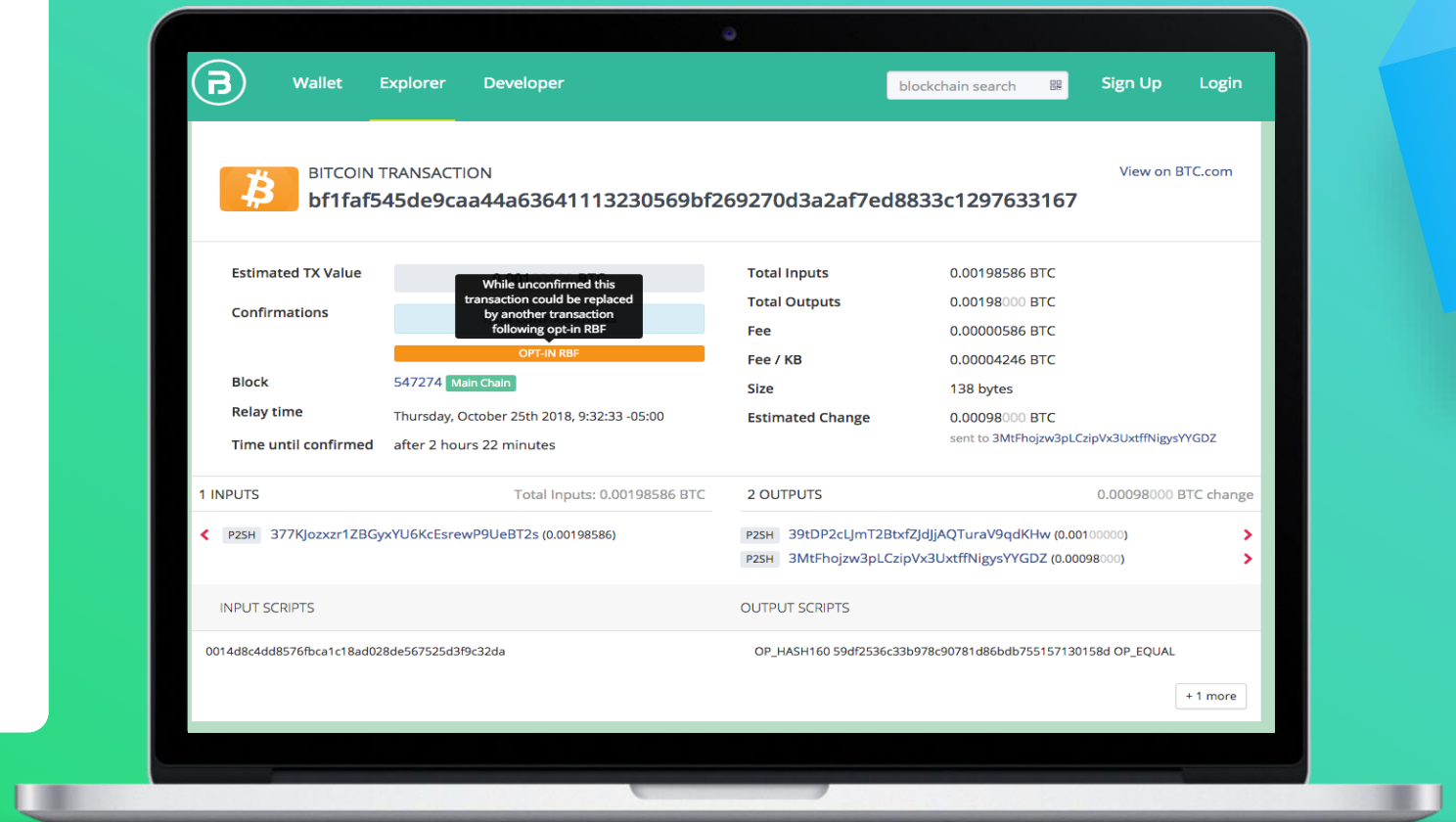
▼ 03

Finalmente, el nuevo bloque (2048 transacciones) se guarda en la red, y el minero recibe la recompensa (6.25 BTC a día de hoy), más los fees de cada transacción.



Proof of Work en Bitcoin – Creación de bloques

- Es un método para aumentar el fee asociado a tu transacción si ningún minero está interesado en incluirla en el bloque.
- Existen algunas instrucciones importantes en este sentido:
 - “-abandontransaction” para abortar la transacción y ejecutarla de nuevo
 - “Opt-in RBF” para actualizar el fee asociado a la transacción sin cancelarla





Proof of Work en Bitcoin – Costes (Feb 2018)

¿Cuánto cuesta minar un bitcoin?

Precio de la extracción de 1 BTC en función del precio de la electricidad en diferentes partes del mundo

Donde es más barato			Donde es más caro		
Venezuela	531 \$	India	3.274 \$	Alemania	14.275 \$
Trinidad y Tobago	1.190 \$	Canadá, Ontario	3.965 \$	Dinamarca	14.275 \$
Uzbekistán	1.788 \$	Rusia	4.675 \$	Tuvalu	14.493 \$
Ucrania	1.852 \$	Estados Unidos	4.758 \$	Tonga	14.671 \$
Kuwait	1.983 \$	Noruega	7.784 \$	Islas Marshall	14.751 \$
Bielorrusia	2.177 \$	Francia	7.930 \$	Islas Cook	15.861 \$
Bangladesh	2.379 \$	Reino Unido	8.402 \$	Islas Salomón	16.209 \$
Kazajistán	2.835 \$	Japón	8.723 \$	Baréin	16.773 \$
Arabia Saudí	3.172 \$	Italia	10.310 \$	Niue	17.566 \$
China	3.172 \$	España	11.103 \$	Corea del Sur	26.170 \$



Section C

Proof of Stake



Proof of Stake

Diferencias PoW vs PoS

- Mayor poder de computación (PoW) vs mayor propiedad de tokens (PoS)
- Entonces, en PoS, en vez de demostrar capacidad de trabajo (minado), lo que el nodo de PoS (**forging**) ofrece, es **COMPROMISO**, al tener este que **depositar una cantidad de capital dentro de la red para ser parte de ella**.
- Al igual que en PoW, si un nodo de PoS (**forging**) intenta manipular la red, tendrá consecuencias, que en este caso podrá desencadenar en la pérdida de su **stake**.

Proof of WORK



v/s

Proof of STAKE





Proof of Stake – Funcionamiento (1)

- El creador de un nuevo bloque se elige de forma pseudoaleatoria mediante los métodos Randomized Block Selection o Coin Age Based Selection; **ambos métodos utilizan como parámetro principal la cantidad de stake bloqueado de cada nodo (forger).**
- Entonces, ¿con este protocolo, la **complejidad** de creación del bloque debe ser alta o baja?
- **Baja, ya que el compromiso con la red se demuestra con la cantidad de stake que deposita el forger.**





Proof of Stake – Funcionamiento (2)

- Importante recalcar, que aunque existe una gran similitud entre la función de los nodos en ambos protocolos, los nodos no se les dice minados, se les dice que están **forged o minted**. A su vez, los nodos son conocidos como **forgers**, y no mineros.
- En la mayoría de los casos de PoS, los tokens se crean en el lanzamiento y por tanto el número está de inicio limitado. Por tanto, en lugar de recibir recompensas por parte de la red, los forgers reciben los fees asociados a cada transacción.





Proof of Stake – Funcionamiento (3)

- En otros casos, se pueden crear nuevas unidades (tokens) para pagar a los forgers (en vez de obtener los fees de cada transacción), **incurriendo de esta forma, en la devaluación del token de la red.**





Proof of Stake – Dilema (1)

- Mayor poder de computación (PoW) vs mayor propiedad de tokens (PoS)
- Entonces, en PoS, en vez de demostrar capacidad de trabajo (minado), lo que el nodo de PoS (**forgers**) ofrece, es **COMPROMISO**, al tener este que **depositar una cantidad de capital dentro de la red para ser parte de ella**.
- Al igual que en PoW, si un nodo de PoS (**forgers**) intenta manipular la red, tendrá consecuencias, que en este caso podrá desencadenar en la pérdida de su **stake**.



- ¿Qué pasaría entonces si diversos forgers se pusieran de acuerdo para validar un conjunto de transacciones (bloque) fraudulento.
Básicamente, este es el concepto de fork (recordemos por ejemplo, Ethereum y Ethereum Classic), ya que lo que está ocurriendo es que hay un conjunto de actores de la red que quiere realizar algo que no está contemplado en las reglas de la red.
- Por tanto, en una Blockchain, no existe realmente ni el bien ni el mal, existe solo lo que es válido y lo que no. Entonces, si un conjunto de nodos quiere realizar una acción que no está recogida en las reglas de la red, lo que está creando ese grupo es una nueva red con reglas diferentes, es decir, un **fork, una nueva Blockchain.**



Section D

Delegated Proof of Stake

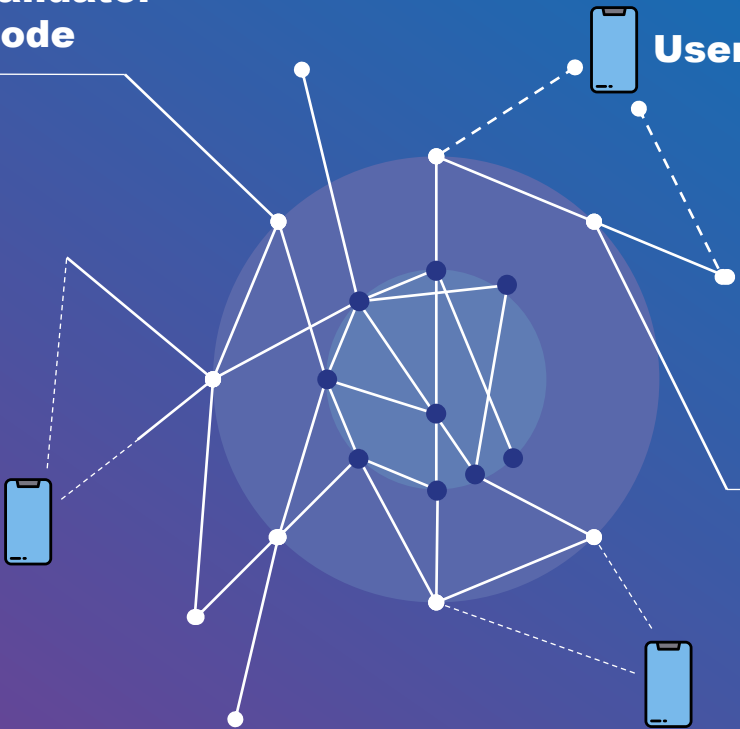


DPoS

Validator
Node

User

Node



Delegated Proof of Stake – ¿Qué es? (1)

- Se trata de un refinamiento del modelo propuesto por el PoS. Esta última invita a una concentración de los activos en la base de proceso de validación. Por lo tanto, la lógica de descentralización puede perder su valor.
- Por eso, en lugar de los actores que posean muchos tokens, los actores que validarán serán elegidos por votación.

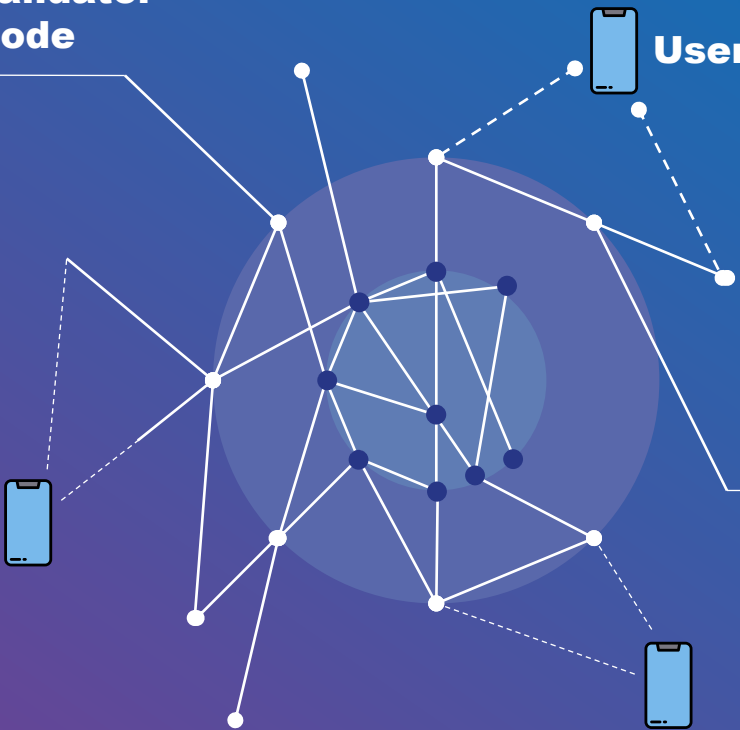


**Validator
Node**

DPoS

User

Node



Delegated Proof of Stake Funcionamiento (1)

- Ejemplo: Imaginemos una red formada por 5 nodos (A-E). A y B son susceptibles de ser validadores, mientras que C posee 100 tokens, D 100 tokens y E 50 tokens.
- C vota A (100 tokens), y, D y E a B (150 tokens).
- El nodo ganador y por tanto el validador hasta las próximas elecciones será el nodo B.
- Pregunta: ¿Qué pensáis de esto?

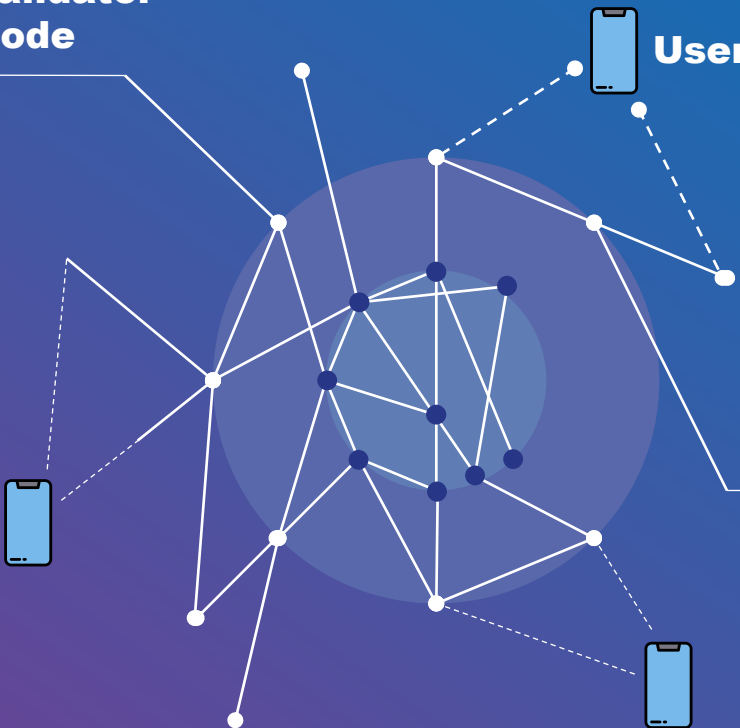


**Validator
Node**

DPoS

User

Node



Delegated Proof of Stake Funcionamiento (2)

- De este modo, los actores más potentes son menos susceptibles de ser atacados, puesto que no validan nada, solo votan. Siendo de esta forma los nodos más eficientes y menos congestionados los que tienden a ser validadores
- El mecanismo de pago puede ser inflacionista (se generan tokens al realizar la validación) o deflacionista (el autor de la transacción paga gastos, habiéndose creado todos los tokens en el lanzamiento de la red)



BLOCKTIVITY

Add My Chain Newbie Roadmap FAQ About

☒ Tx ☒ Record ☐ Protocol ☐ Block Time ☒ MC ☒ Price ☒ X'tivity ☒ Potential ☒ Activity 7d ☒ Chart 7d

#	Symbol	Activity 24h	Tx 24h	Record	MC	Price %	X'tivity	Potential	Activity 7d	Activity 7d
1	WAXP	26,284,224	21,820,680	31,197,964	168	0.2 %	35	85029	-2 %	
2	XLM	9,889,928	..	13,922,989	2792	5 %	13	1925	3 %	
3	TRX	6,574,874	6,574,874	9,142,521	5095	-12 %	9	701	20 %	
4	HIVE	2,301,617	2,277,835	4,567,648	156	-2 %	3	8018	16 %	
5	EOS	1,698,691	757,264	81,594,315	912	1 %	2	1012	-21 %	
6	XRP	1,309,464	1,309,464	2,202,437	15,254	2 %	2	47	0.0 %	
7	WAVES	873,182	873,182	1,481,609	513	2 %	1	925	86 %	
8	FSN	822,190	219	821,031	19	4 %	1	23518	5 %	
9	BTC	759,075	291,948	1,022,091	412,538	-5 %	1	1	11 %	
10	MHC	743,557	743,557	3,680,390	6	2 %	1.6	67351	-21 %	

¿Dudas de la eficacia del protocolo? → blocktivity.info

- Activity: Txs 24h
- Average: Media Txs 7 días
- Record: Pico Txs
- MarketCap: Valoración
- X'tivity: $\text{Ind f}(\text{BTC Cap}, \text{BTC TXs})$

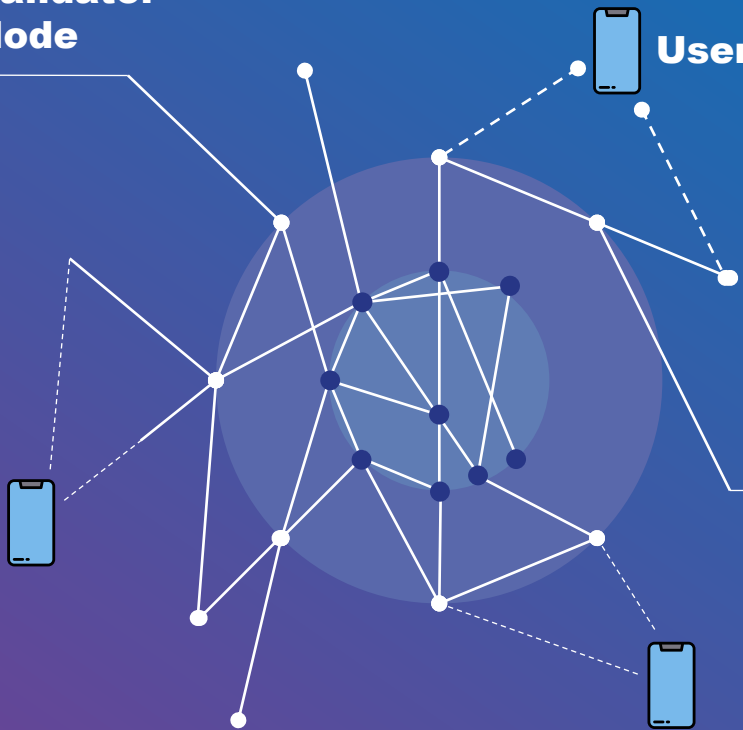


DPoS

Validator
Node

User

Node



Delegated Proof of Stake Problemas

1. Al querer optimizar el proceso de validación, el planteamiento ha permitido reducir la cantidad necesaria de actores para mantener el protocolo. A cambio, es mucho más fácil de atacar y para corromper la red se necesitan menos del 50% del consenso.
2. Los actores que ya son ricos, pueden serlos más. Como poseen el derecho a voto, cuantos más recursos tienen más pueden influir.
3. Los validadores o grandes propietarios pueden formar cárteles de influencia. Esto atenta directamente contra la descentralización.



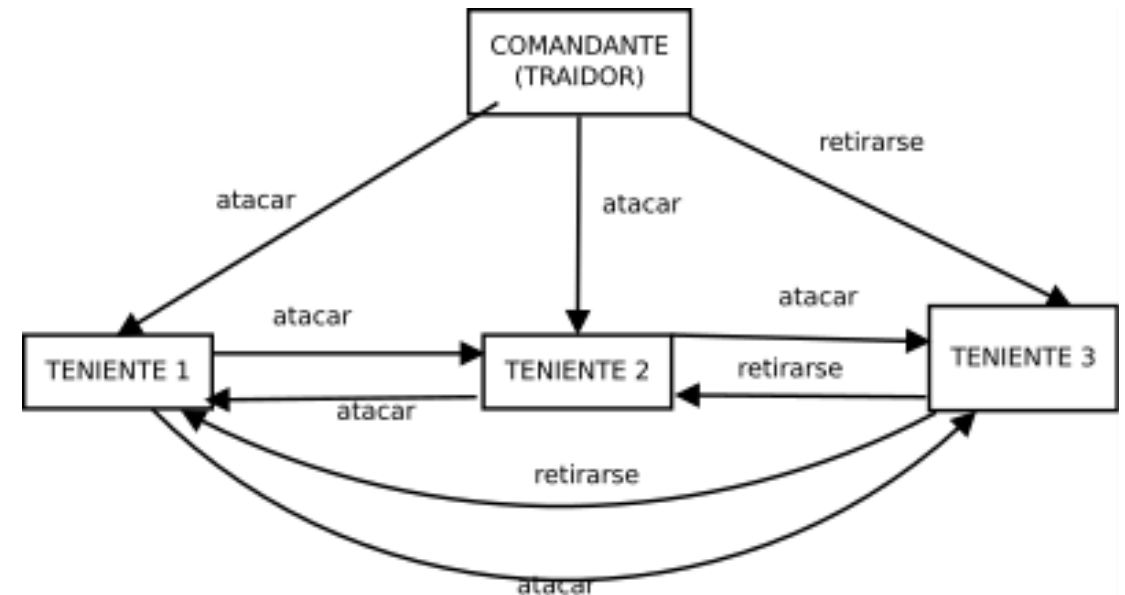
Section E

BFT, PBFT y DBFT: los protocolos bizantinos tolerantes a fallos



Problema de los generales bizantinos (BFT)

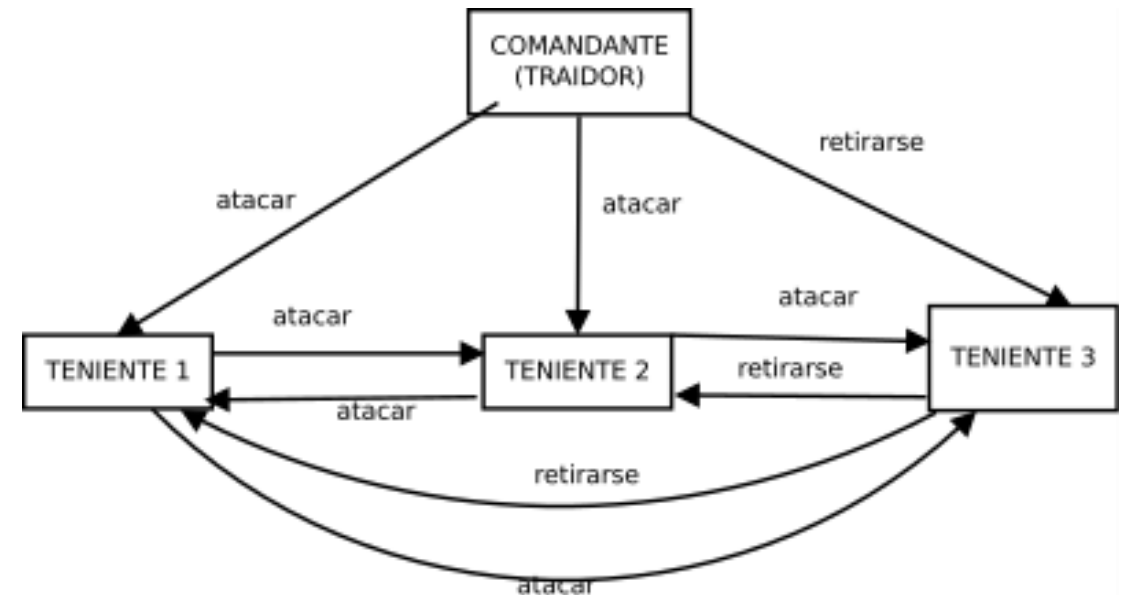
- Para explicar estos protocolos, es necesario presentar el problema de los generales bizantinos. En teoría de la informática, se trata de una metáfora para tratar problemas de fiabilidad de la información y de la integridad de los interlocutores.
- Imagínate que varias armadas alrededor de la ciudad, deben coordinarse para lanzar un ataque. Para ello, los generales deben usar mensajeros para enviarse las comunicaciones de ataque o retirada.





Problema de los generales bizantinos (BFT)

- Aplicado al mundo de la informática, el general es un nodo, y el mensajero representa la comunicación electrónica entre los servidores.
- Vamos a llamar "n" a la cantidad de servidores defectuosos o malintencionados. Matemáticamente, se ha demostrado que sería necesario que al menos un tercio de los mensajes estuvieran corrompidos para cuestionar el mensaje. Esto significa que, para que una red sea fiable, es necesario que haya al menos $3n+1$ nodos operativos.

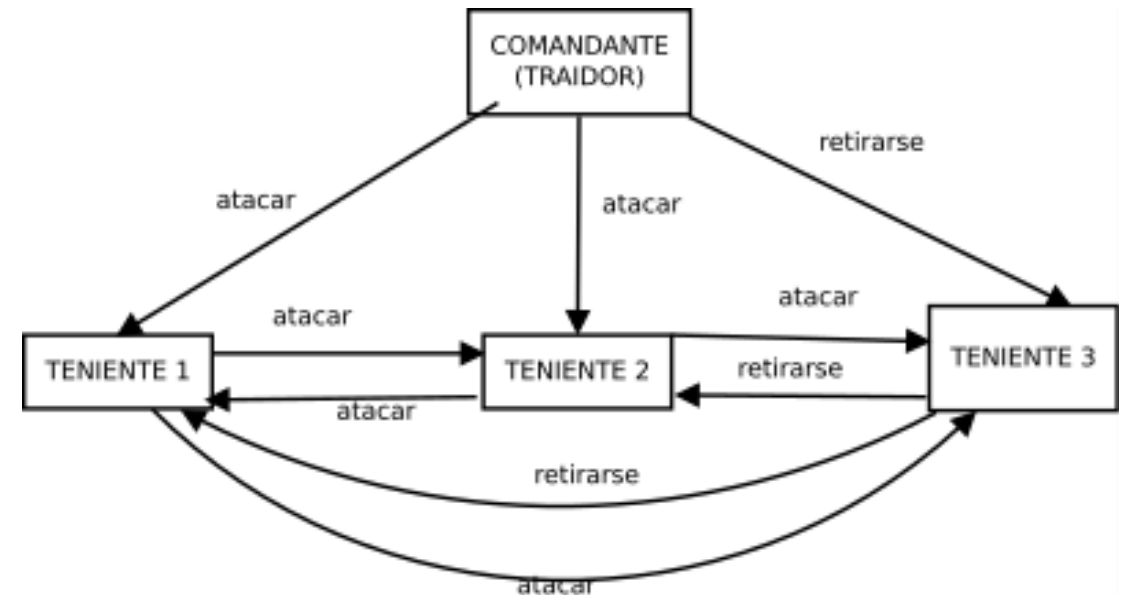




Problema de los generales bizantinos (BFT)

Ejemplo: Pensemos en un sistema en el cual existen 10 nodos.

- Esto querría decir, que un BFT, podría tolerar como máximo 3 nodos malintencionados o defectuosos.
- Si lo queremos pensar a la inversa, necesitaríamos un sistema de 10 nodos como mínimo, para que pudieran fallar como máximo 3, y el sistema seguiría funcionando correctamente.

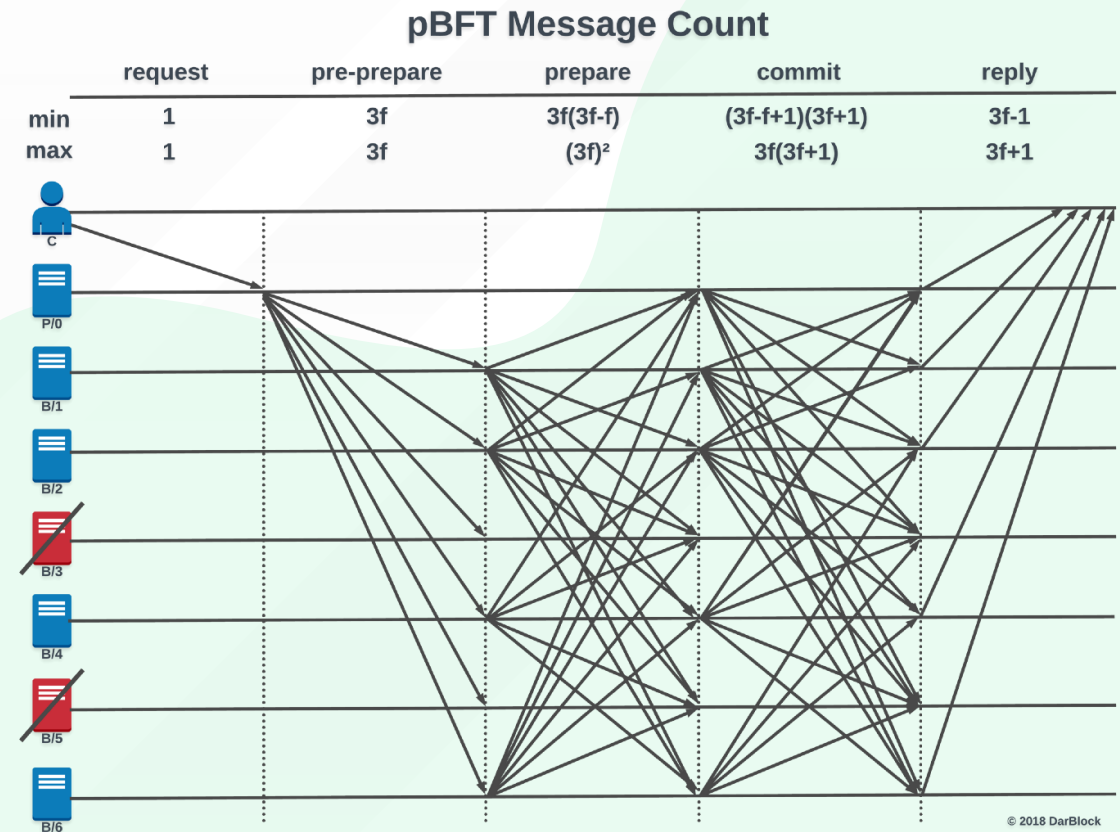




Practical Byzantine Fault Tolerance (PBFT)

El protocolo PBFT se realiza por turnos, descomponiéndose estos en cuatro partes.

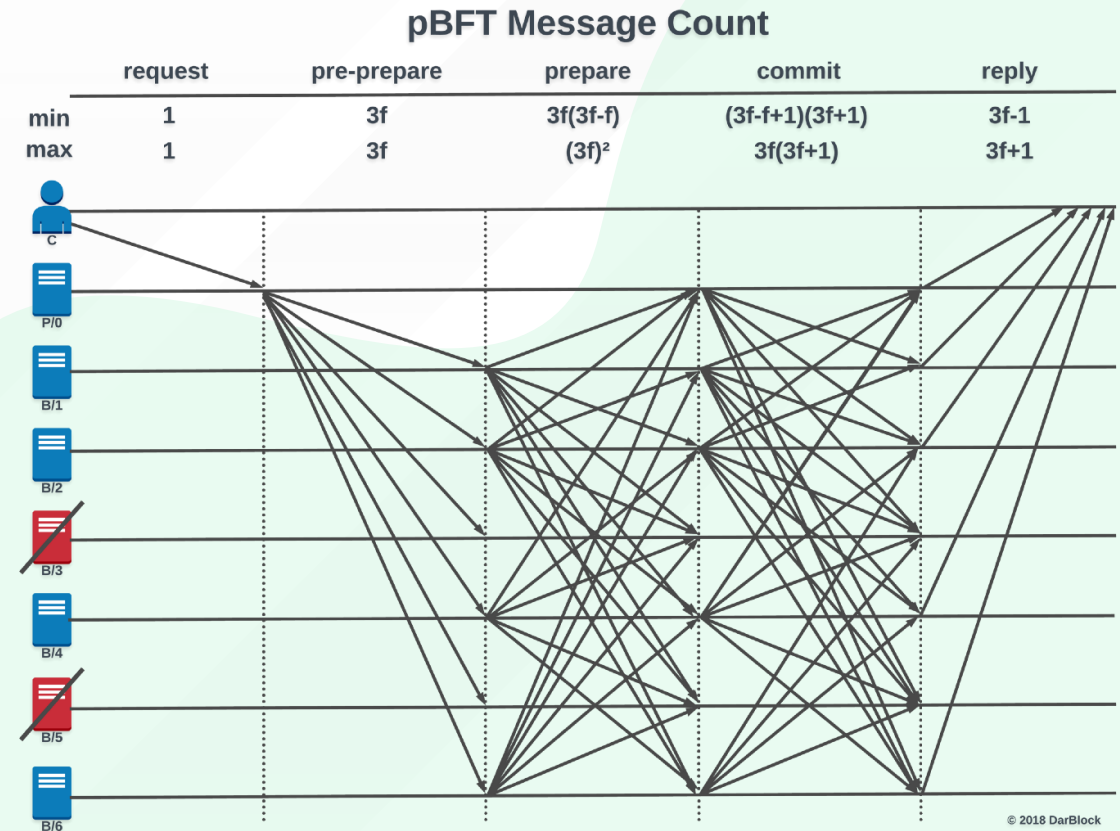
1. El cliente envía una solicitud al nodo principal o líder para invocar un servicio.
2. El nodo líder retransmite la solicitud a los nodos back-up.
3. Estos últimos, ejecutan la solicitud y luego la reenvían al cliente.
4. El cliente espera " $f+1$ " respuestas de los distintos nodos con la misma respuesta, donde " f " representa la cantidad de nodos potencial máxima regenerados o defectuosos.





Practical Byzantine Fault Tolerance (PBFT)

- El nodo líder se puede cambiar en cada turno. También se puede sustituir durante una operación si el envío de los datos a los nodes no tiene lugar durante una ventana de tiempo definida.
- También es posible que una mayoría de nodes determinen si un node libre es defectuoso y lo sustituyen por el líder siguiente en la fila.

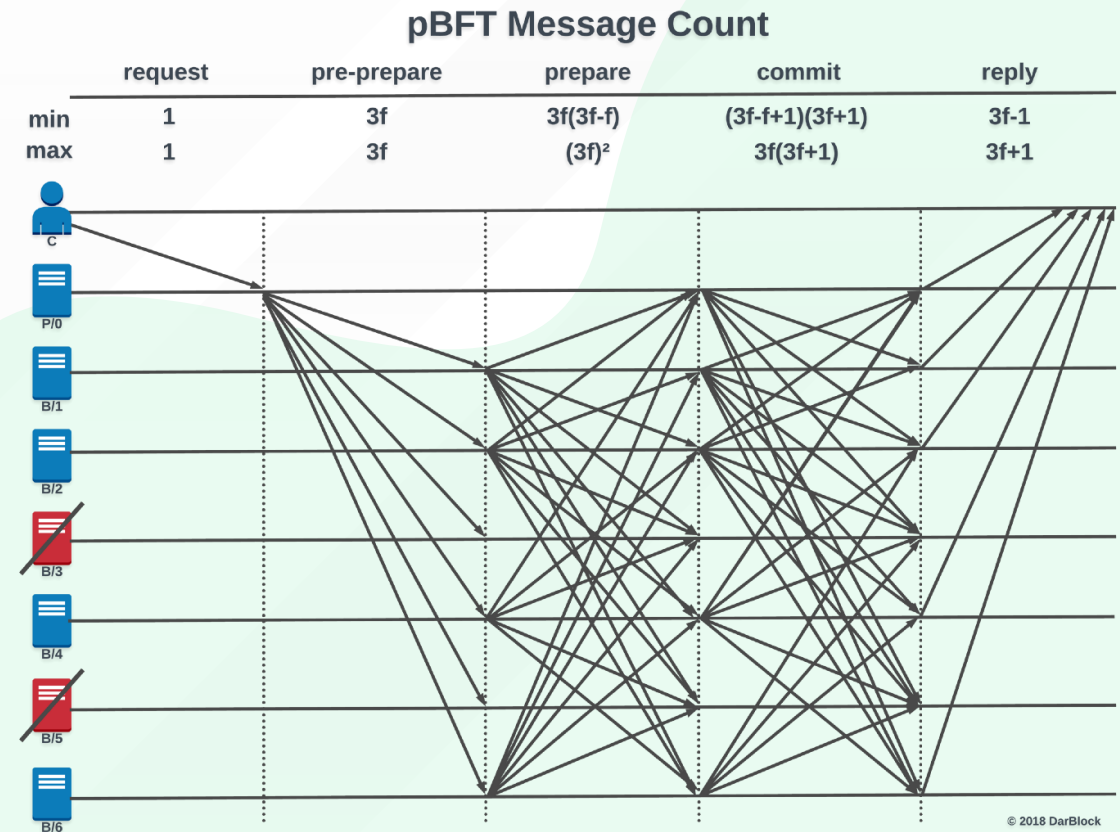




Practical Byzantine Fault Tolerance (PBFT)

Ejemplo: Pensemos en un sistema en el cual existen 10 nodos.

- Si sabemos que existen 3 nodos defectuosos o malintencionados y estamos usando PBFT, básicamente significa que si llegan a la salida 4 o más respuestas iguales, el mensaje será fiable.
- Es decir, es imposible que nos lleguen 4 o más mensajes iguales, y que la info se considere errónea.

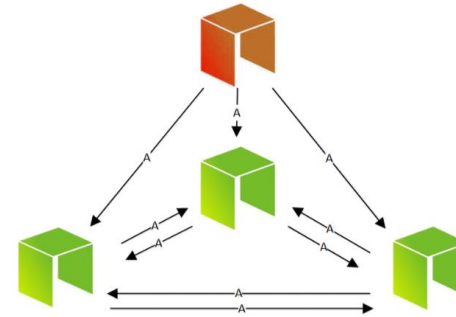


© 2018 DarBlock



Delegated Byzantine Fault Tolerance (DBFT)

- El DBFT es una variante que fusiona el planteamiento PoS & PBFT.
- La idea general es la siguiente: El conjunto de los usuarios elige los nodos, denominados bookkeepers. Su función es añadir bloques nuevos al registro. Cada uno de estos nodos propone un bloque por turno, y este se añade al registro cuando al menos el 66% de los otros bookkeepers lo valida.



NEO
smart economy

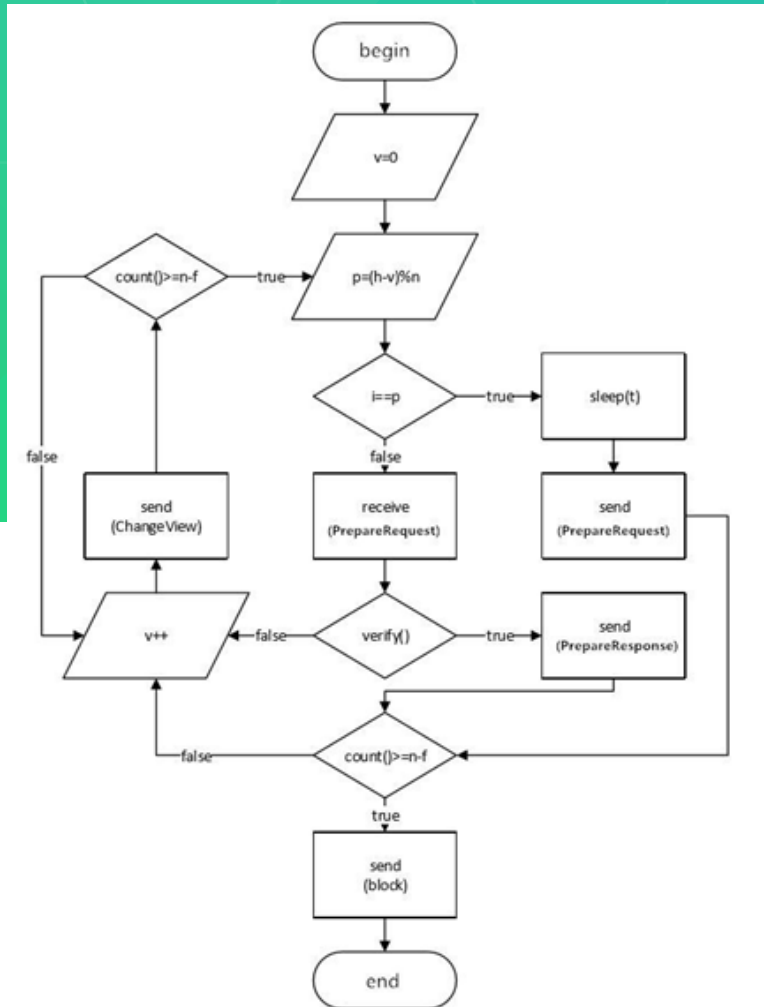
Basic Crypto
Consensus Algorithm



Delegated Byzantine Fault Tolerance (DBFT)

Las etapas que permiten encontrar un consenso mediante DBFT pueden resumirse como se describe a continuación:

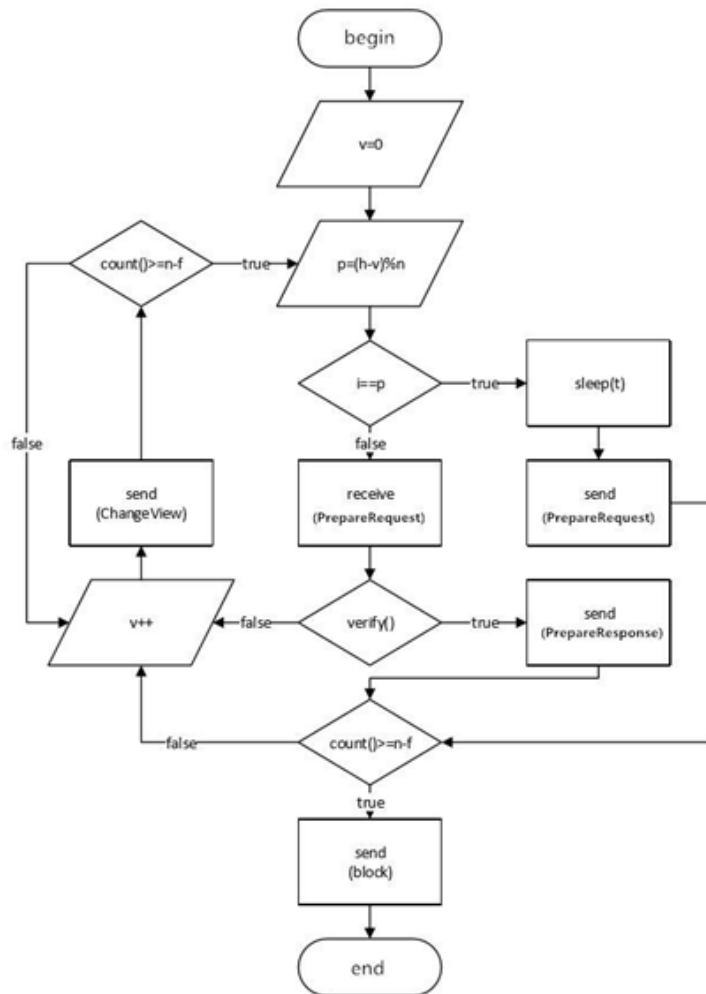
1. Un cliente envía una solicitud a la red blockchain utilizando este protocolo bajo la forma de un mensaje.
2. El conjunto de los usuarios de la blockchain vota para designar nodos (bookkeepers). Este grupo de nodos elegidos se actualiza periódicamente. El voto se pondera según la cantidad de criptomonedas poseída, es decir, cuantas más criptos tiene un usuario más peso tiene su voto (PoS).
3. Uno de los bookkeepers se selecciona aleatoriamente para enviar un bloque. Este nodo se llama speaker. Los bookkeepers se convierten en speakers por turnos al azar
4. El speaker recibe la solicitud enviada por el cliente en la primera etapa. Esta operación está esperando a ser escrita en el registro. El speaker verifica las firmas electrónicas que identifican al emisor de la transacción y su validez, para reunir las todas en un bloque.





Delegated Byzantine Fault Tolerance (DBFT)

5. El speaker envía su bloque a todos los bookkeepers.
6. Los bookkeepers verifican el bloque para evitar que la transacción sea inválida, las firmas electrónicas incorrectas, etc. y por consiguiente la validan.
7. El consenso se alcanza cuando al menos el 66% de los bookkeepers validan el bloque. Entonces se añade a la blockchain.
8. Por último, periódicamente se designa un speaker nuevo de manera aleatoria y el proceso vuelve a empezar la etapa 1.





Delegated Byzantine Fault Tolerance (DBFT)

El objetivo de estos mecanismos es hacer verificaciones cruzadas entre nodos de confianza. Este planteamiento también tiene la ventaja de que solo una comunidad restringida de actores soporta la carga de la validación.

Las blockchains Neo y Tezos usan estos mecanismos

Existen muchas otras variantes, como el federated byzantine agreement usado en Stellar. Sin embargo, se aplican los mismos mecanismos y tienen la misma finalidad: proteger la red, hacer converger las transacciones válidas y realizar estas operaciones con un nivel de servicio elevado



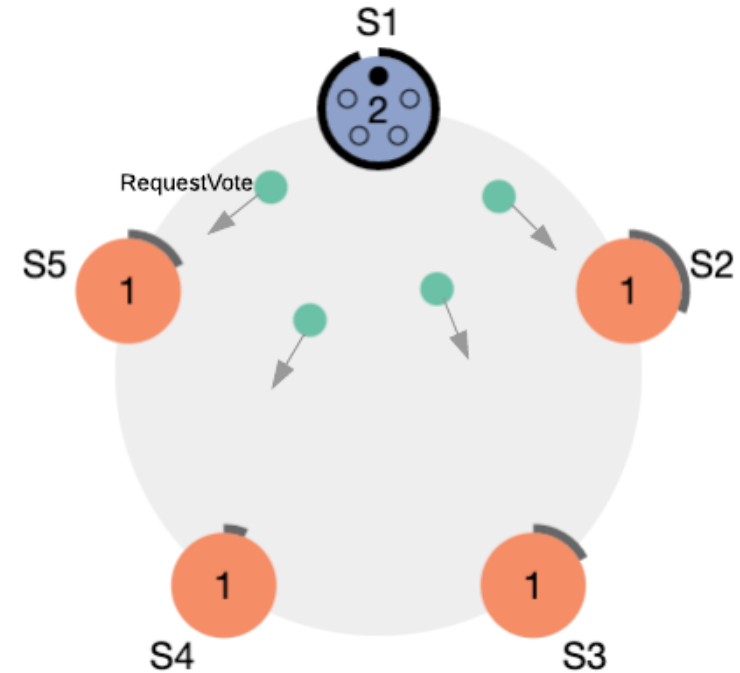
Section F

RAFT



RAFT

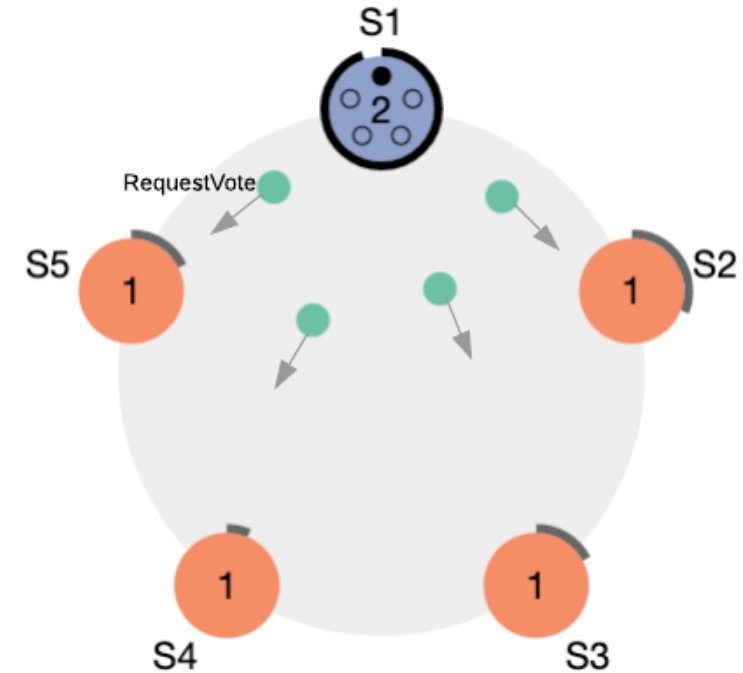
- RAFT es un algoritmo de consenso tolerante a fallos (por ejemplo: caídas de servicio) para contextos distribuidos. Se trata de una variante de la familia PAXOS.
- Garantiza que en caso de fallo, el sistema siempre sea capaz de gestionar las solicitudes que se le envían. Este algoritmo parte del principio de que las informaciones que circulan en la red son fiables y los interlocutores íntegros.
- Por lo tanto, no es posible aplicarlo en un contexto de blockchain pública, si no solo en blockchains permitidas (privadas)





RAFT

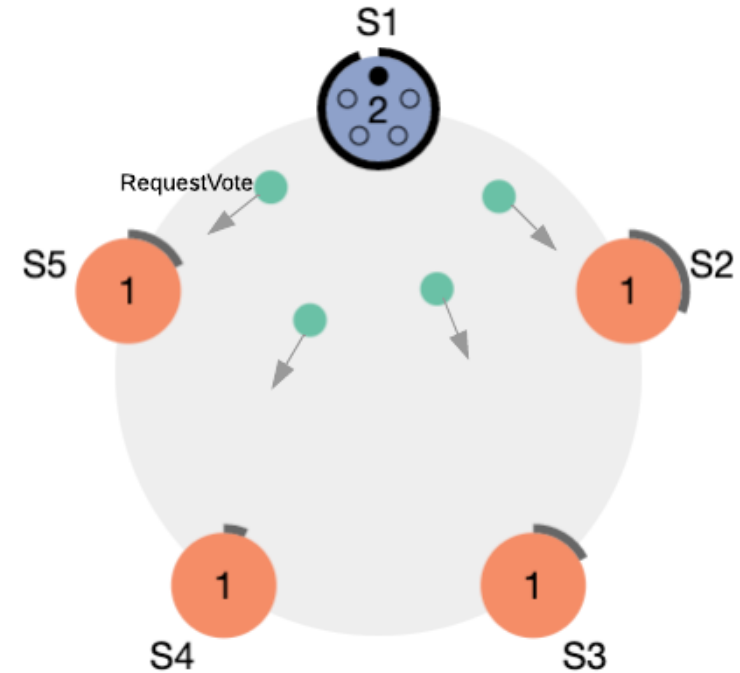
- Hyperledger Fabric y Quorum utilizan este algoritmo. Parten del principio de que para acceder a la red, ya se han hecho previamente una determinada cantidad de controles con una gestión estricta de seguridad anticipada.
- Los certificados digitales se ocupan de la seguridad funcional, mientras que RAFT de la seguridad técnica como las caídas de sistemas, pérdidas de conexión, retrasos de envío, etc.





RAFT

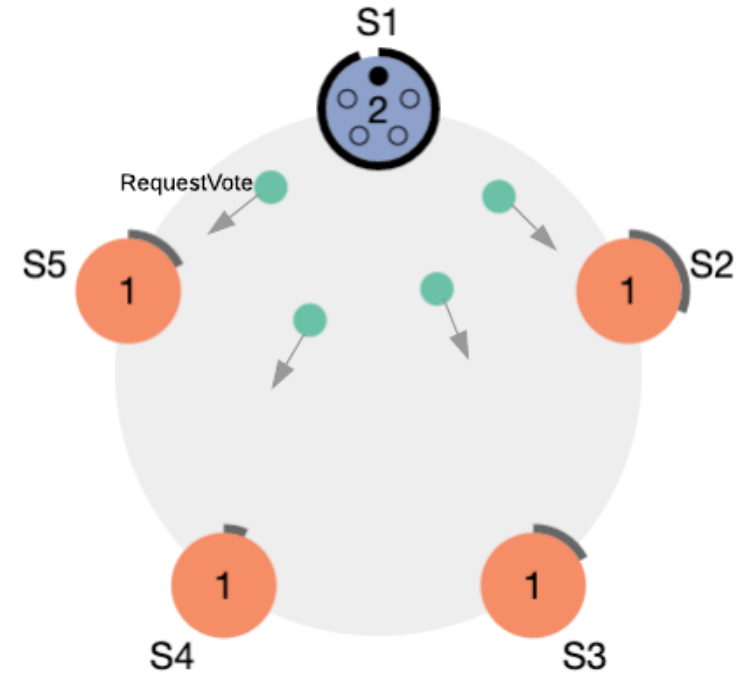
- En la práctica, este mecanismo de consenso es mucho más accesible que PoW o PoS. Al principio, los nodos de la red, llamados candidatos, van a elegir a un líder.
- El proceso de emisión de voto es parametrizable, y puede consistir por ejemplo, en cómo actúa un nodo para tratar una información. Una vez elegido el líder, todos los candidatos se convierten en seguidores (followers).





RAFT

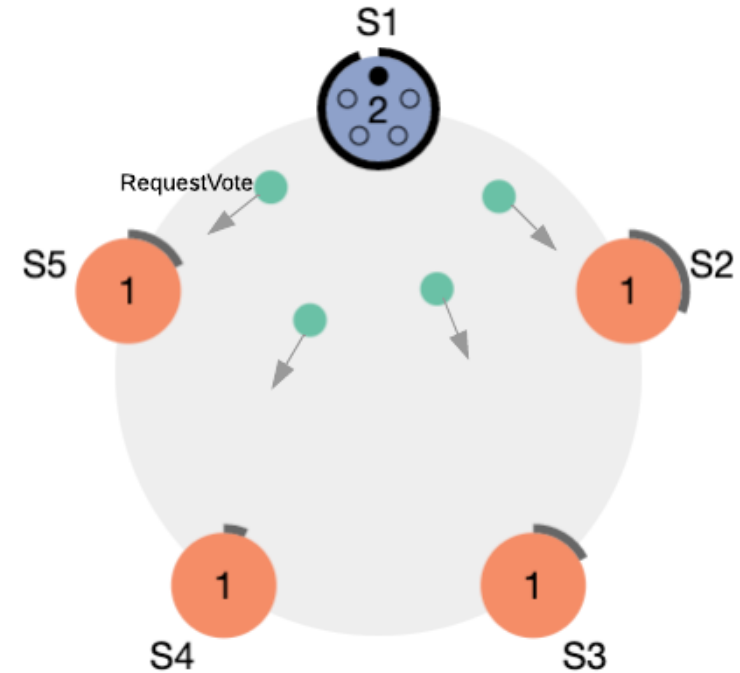
- Cada vez que un usuario del sistema emite una solicitud a la red, se redirige sistemáticamente hacia el líder, el cual procede a la solicitud. Esto significa que directamente valida y se dispone a escribir cualquier cosa que le llegue en base de datos. Esta información la transmite a todos los seguidores de la red.
- Estos últimos reenvían una respuesta al líder para decir que han recibido el mensaje correctamente. Entonces y solo entonces se escribe la transacción en la base de datos finalmente.





RAFT

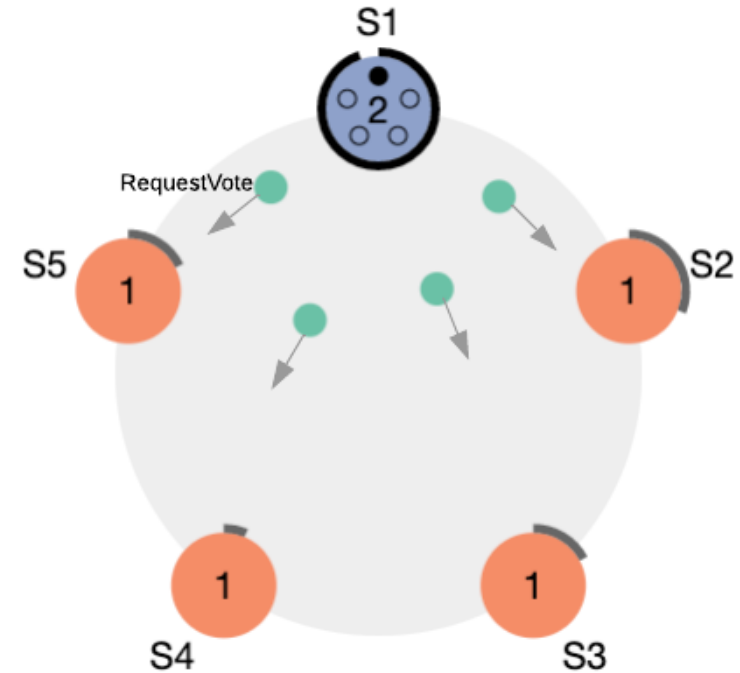
- En el caso de Hyperledger Fabric, el proceso de voto se desarrolla en un componente conceptual denominado OSN (Ordering Service Node). Este componente tomará todas las transacciones y las pondrá en orden. Este orden es no es por fecha u hora, si no que cada transacción tiene dedicado un lugar en el registro.
- (Al revés que en Bitcoin o Ethereum donde los bloques se guardan sucesivamente en el tiempo, este planteamiento es determinista y corresponde al ámbito de las probabilidades)





RAFT

- Por lo tanto, este protocolo es muy distinto de los anteriores, ya que no valida realmente las transacciones. En cambio, se asegura de que la información se haya comunicado correctamente a los distintos miembros de la red, y de que el emisor del mensaje se haya identificado correctamente mediante el intercambio de firmas criptográficas. En un contexto empresarial, con esta seguridad es más que suficiente.

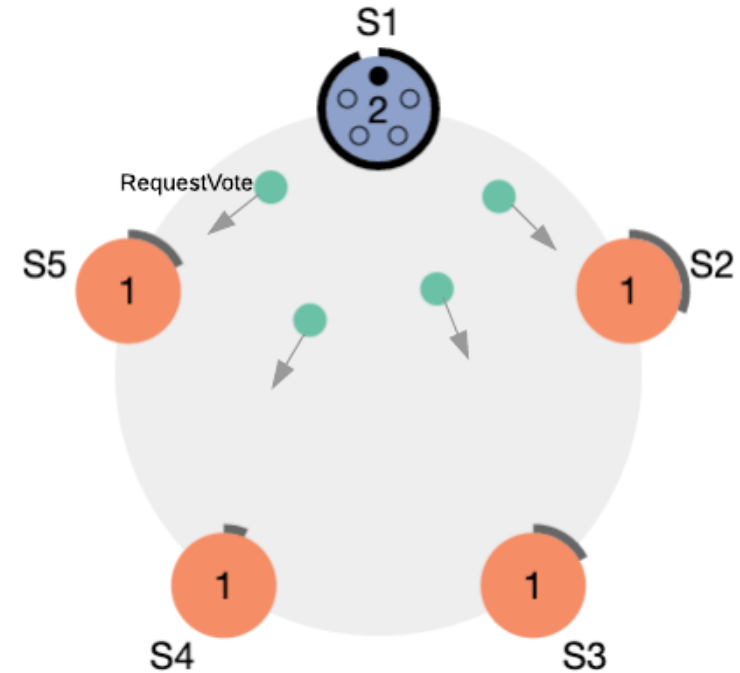




RAFT

- La existencia de este tipo de protocolo es fundamental, ya que ofrece una resistencia que no ofrece una base de datos centralizada compartida entre actores.
- Ventajas: Es muy eficiente energéticamente (no hay minado), el proceso de validación no es probabilístico y no es necesario garantizar la fiabilidad del emisor de la información.
- Ventaja adicional: En comparación con los bizantinos, RAFT solo necesita " $2n+1$ " nodos para que funcione, por lo tanto, se necesitan menos componentes para su mínima implementación técnica.

Pregunta: ¿Podríamos comparar este protocolo entonces a un sistema centralizado?

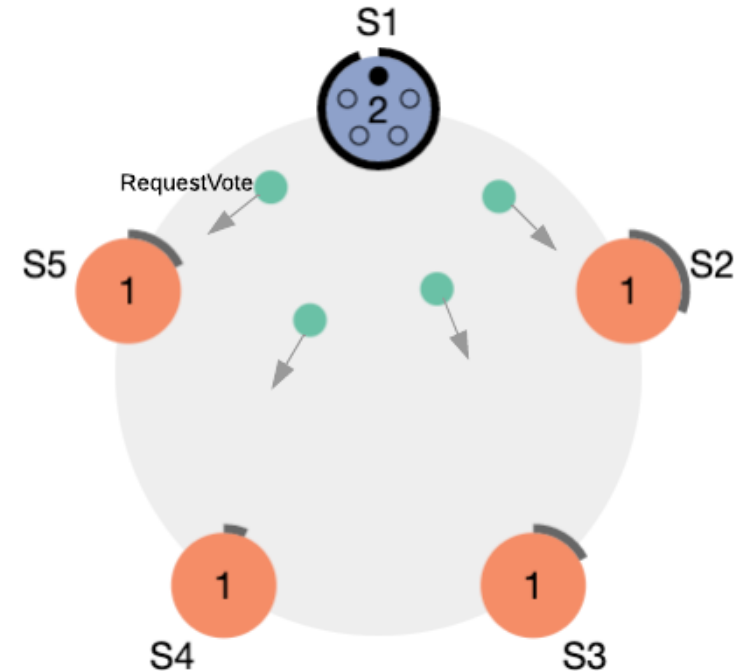




RAFT

- La existencia de este tipo de protocolo es fundamental, ya que ofrece una resistencia que no ofrece una base de datos centralizada compartida entre actores.
- Ventajas: Es muy eficiente energéticamente (no hay minado), el proceso de validación no es probabilístico y no es necesario garantizar la fiabilidad del emisor de la información.
- Ventaja adicional: En comparación con los bizantinos, RAFT solo necesita " $2n+1$ " nodos para que funcione, por lo tanto, se necesitan menos componentes para su mínima implementación técnica.

Pregunta: ¿Podríamos comparar este protocolo entonces a un sistema centralizado?

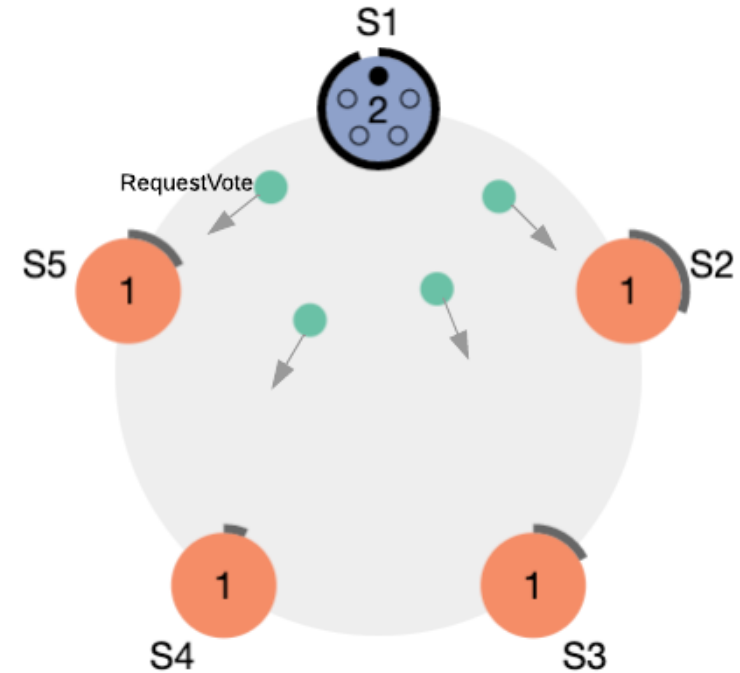




RAFT

Desventajas:

1. No se puede aplicar a blockchain públicas.
2. Es posible que la info enviada proceda de una fuente dudosa (si se salta el protocolo de certificados).
3. El proceso de voto se puede alterar (igualmente por los certificados).
4. Un actor podría aumentar su peso en la red de manera artificial, y validar transacciones que no deberían validarse.



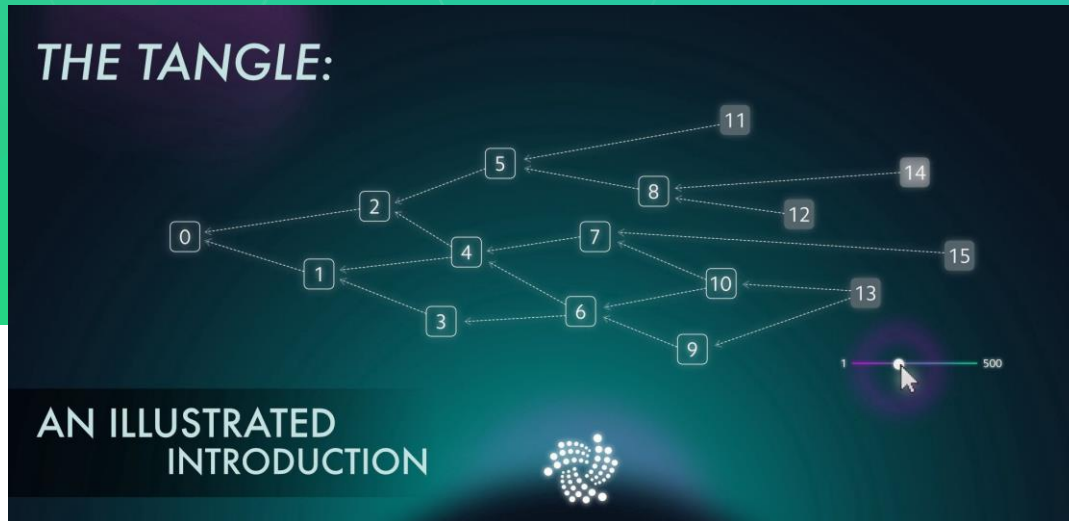


Section G

Directed acyclic graph, Tangle y Hashgraph



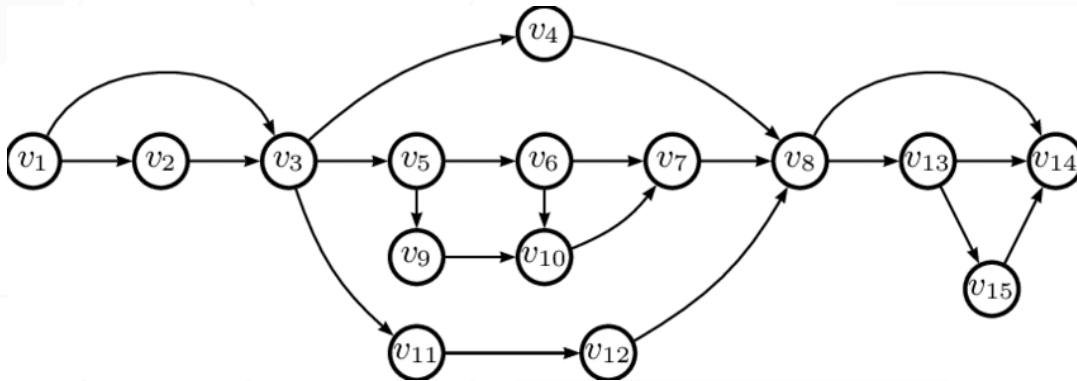
Directed Acyclic Graph (Tangle)



- En Tangle, el proceso general y de modo resumido para el procesamiento y validación de cada una de las transacciones es el siguiente:
- Si nos fijamos en el bloque número 10, para que sea candidato al proceso de validación, se debe crear un lote con las transacciones de los bloques 6 y 7. Una vez realizado el cálculo matemático, éstas dos transacciones se validarán.
- En ese momento, el bloque 13 podrá validar la transacción del bloque 10 (junto con la del bloque 9, siempre que el bloque 9 también haya validado dos transacciones previamente).



Directed Acyclic Graph (Tangle)

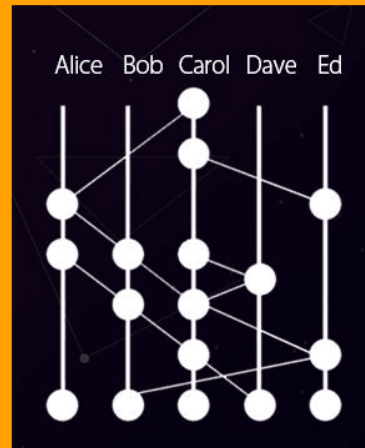


- El objetivo fundamental de Tangle es hacer posible un intercambio de información seguro en el ámbito del IoT con gastos de transacción inexistentes.
- Su segundo objetivo es que ningún nodo en particular sea el encargado de hacer el proceso de validación, sino que lo hagan entre todos.
- Tangle se basa en la teoría de grafos, y más en concreto en los DAG (Directed Acyclic Graph), los cuales no son más que caminos (grafos) que nos permiten ir de un extremo a otro de una red sin poder volver atrás.



Directed Acyclic Graph (Hashgraph)

HASHGRAPH

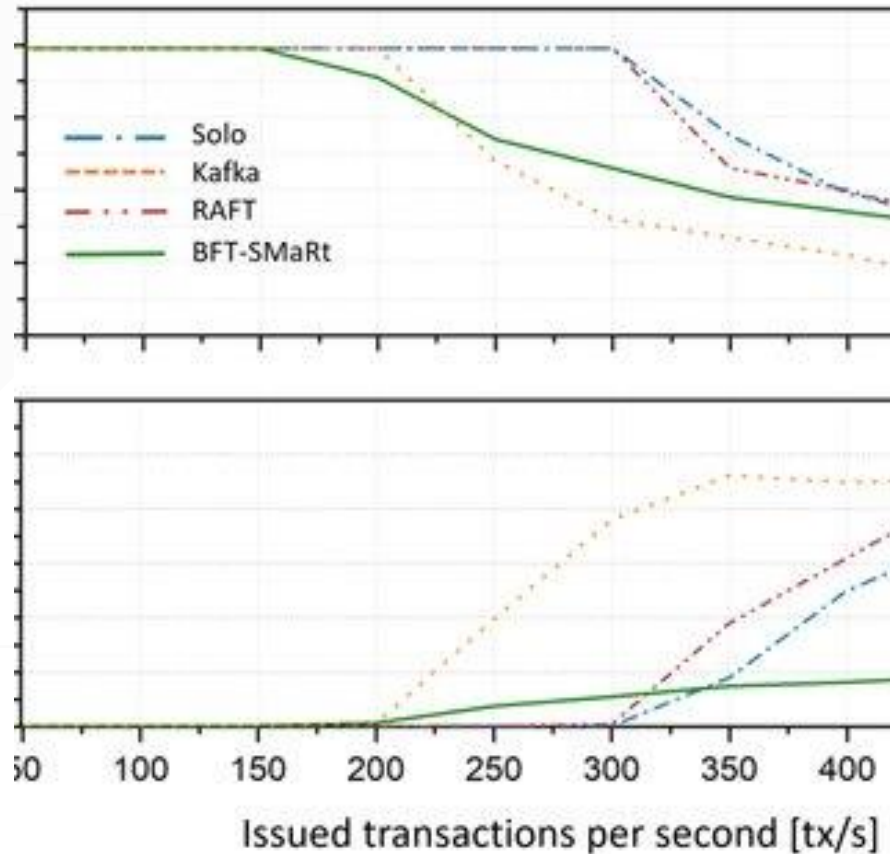


- Aquí, el proceso de selección de las transacciones se sustituye por un protocolo denominado gossip-to-gossip (chismoso a chismoso). Un dato se intercambia entre muchos nodos. Cuanto más se intercambia, más probable es.
- El proceso de validación se realiza mediante nodos que calculan un algoritmo que les da derecho a validar una transacción. El funcionamiento de este algoritmo es muy similar al del PBFT.
- Muy recientemente, el protocolo ha sido propuesto como Open Source después de las muchas presiones realizadas por parte de su propia comunidad.



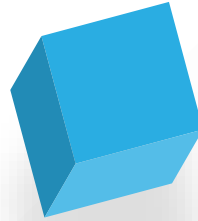
Section H

SOLO



SOLO

- Es el mecanismo de consenso más sencillo que se haya visto en un sistema descentralizado. Podemos encontrarlo en el sistema Hyperledger Fabric y no está adaptado para blockchain públicas. Publica las transacciones a los nodos a los que está conectado. Este mecanismo no busca alcanzar un consenso. Tampoco resiste a los fallos de los sistemas como podría hacerlo RAFT.
- Localizado en el OSN, envía datos, pero no realiza ningún control de la calidad de los nodos. No se puede mejorar. Como recordatorio, el OSN es el órgano de control que puede ordenar las transacciones de la red y garantizar la coherencia del registro.



FIN

¡Muchas Gracias!

