

Hashgraph

<https://youtu.be/nfVWMhKHj7I>

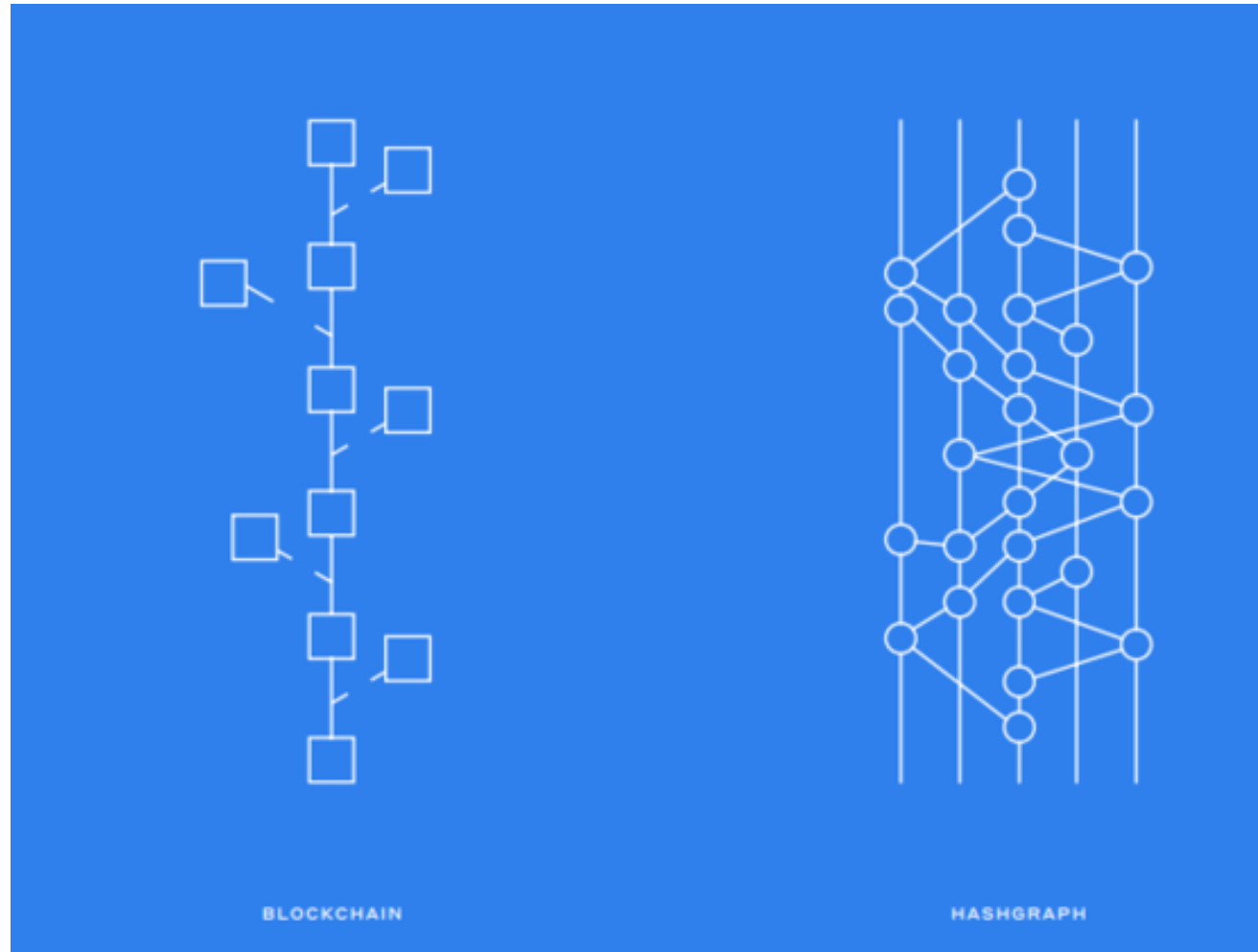
Hashgraph

- 하나의 노드가 다른 불특정 노드에 **가십을 전달하는 방식**으로 작동하는 알고리즘
- 1초에 수십만 건 이상의 **빠른 속도**로 트랜잭션을 처리 가능



Hedera Hashgraph

Blockchain과 Hashgraph 차이점



Blockchain과 Hashgraph 차이점

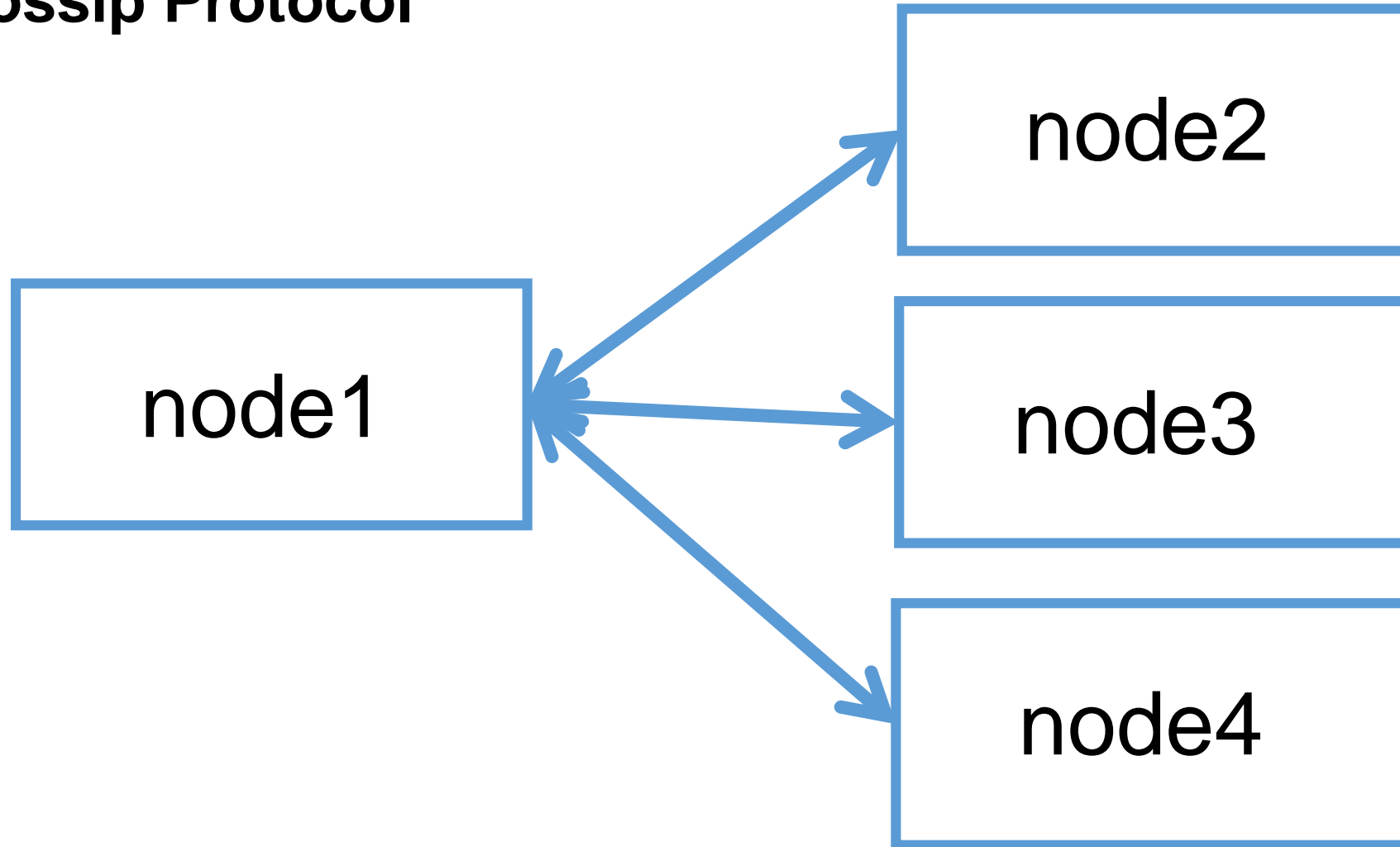
	Blockchain	Hashgraph
빠르게 성장하는 구조의 경우	새로운 블록이 예상보다 빠르게 도착 -> 실패	빠르게 성장하는 구조에 영향 x
가지치기	필요	필요없음
PoW 작업	o	x

네트워크 작동방식

1. 네트워크의 현재 상태나 과거 이력에 대한 정보 조각
> **보고서 형태** 제작 -
2. 무작위로 이웃 노드를 선택하여 전파
3. 새로운 정보가 발생하면 이전에 전파한 보고서에 내용 추가
4. 다시 무작위로 노드를 선택하여 계속 전파
5. 이 과정을 지속적으로 반복 = **gossiping**

합의 알고리즘

1. Gossip Protocol



합의 알고리즘

1. Gossip Protocol_ Gossip about Gossip

- 해시 그래프의 노드들은 정보를 보고서 형태로 만듦
- 이 보고서에는 해시값 포함
- 모두가 언제 무엇을 알았는지 초단위로 전달

* 해시그래프는 가십의 경로를 시간 순서대로 나열한 것이라고 생각

합의 알고리즘

2. 가상 투표 : 투표없는 투표 프로토콜

모든 메시지



마지막으로 보낸 메시지 이름(해시)

나에게 마지막으로 메시지를 보낸 사람(해시)

합의 알고리즘

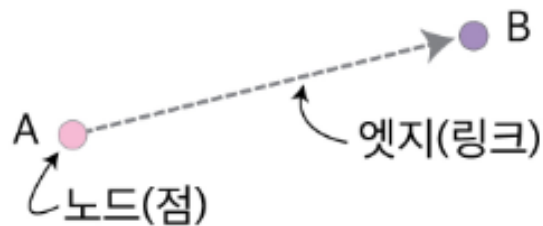
결론

- 블록체인 네트워크에서 상대적으로 높은 합의 권한을 가진 노드가 **악의적**으로 데이터를 지연시켜 변조 시킬 가능성 막을 수 있음.
- 단순히 **해시값만 검사**함으로써,
특정 노드는 네트워크에 유용한 정보에 대해 **반대표를 던지지 않을 것이라는 신념**에 기초하여 가상투표 수행한다고 가정
→ 자연스럽게 합의가 도출 됨.

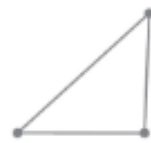
DAG(Directed Acyclic Graph)

- 연속으로 이어지는 방향성을 가진 네트워크 연결 방법
- 순간순간 발생하는 참여자들(노드)에 의해 상황에 따라 데이터 기록
- 반복되거나 동일한 패턴에 의해 다른 곳과 연결 x
- 불특정 다수에게 계속 연결

* 그래프의 구성 요소



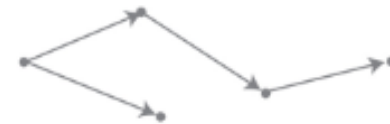
인포그래픽 강민승



순환그래프
(cyclic graph)



비순환그래프
(acyclic graph)



방향성 비순환 그래프
(directed acyclic graph)

DAG(Directed Acyclic Graph)

- 비동기식 비잔틴 장애 허용 합의 알고리즘을 이용
- 모든 노드들이 해당 블록을 **동시에 검증할 필요X**
- 수많은 노드들이 분산되어 각자 검증을 동시에 진행
→ 차례대로 검증하는 **기존 블록체인의 틀을 깬 것**이라 할 수 있음.
- **완결성을 확정**하기 까지 필요한 시간은 **약 3초**라고 알려짐.

해시 그래프의 한계점

- **오픈소스X** → 탈중앙화와 거리가 멀다는 비판
- **트랜잭션 수에 대한 확장성만 높은 프로토콜**이라는 평가
- 프라이빗 세팅 안에서는 빠르고 공정하고 안전
→ 퍼블릭 세팅에서 사용 시,
다른 퍼블릭 블록체인과 동일한 문제점 발생 예측
- 실제 제품이나 서비스가 실현되지 전까지 **확신할 수 없는 한계**

Q & A

