SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

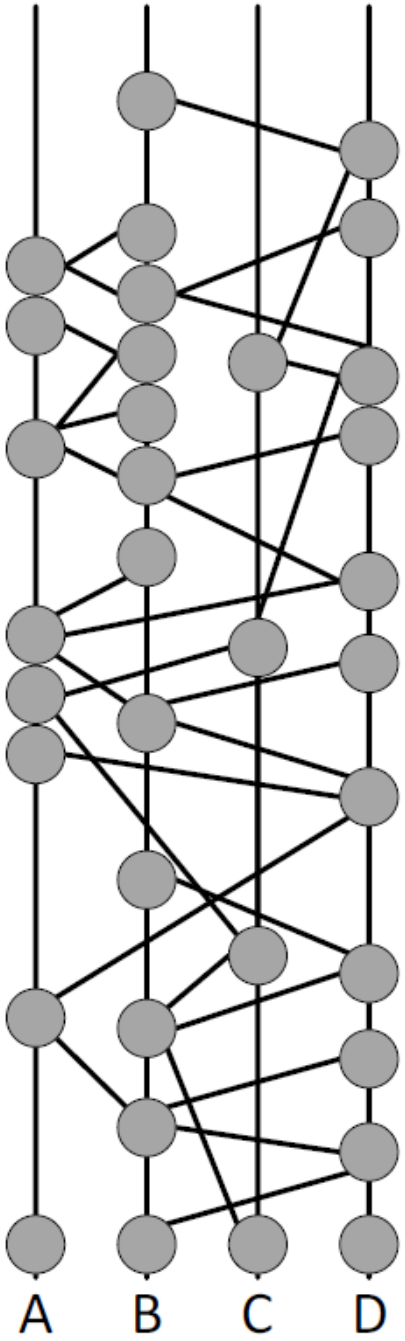
Session 11:

DAG-based DLTs – Part 2

Module 2 – Hashgraph

Hashgraph

- Dr. Leemon Baird is the inventor of the hashgraph distributed consensus algorithm.
- Hashgraph is based on gossips about gossips (with cryptography) and virtual voting.
- It is efficient because people don’t actually send any votes over the Internet.
- Hashgraph is a DAG at its core, but is very different from IOTA.
- It’s permission-based.



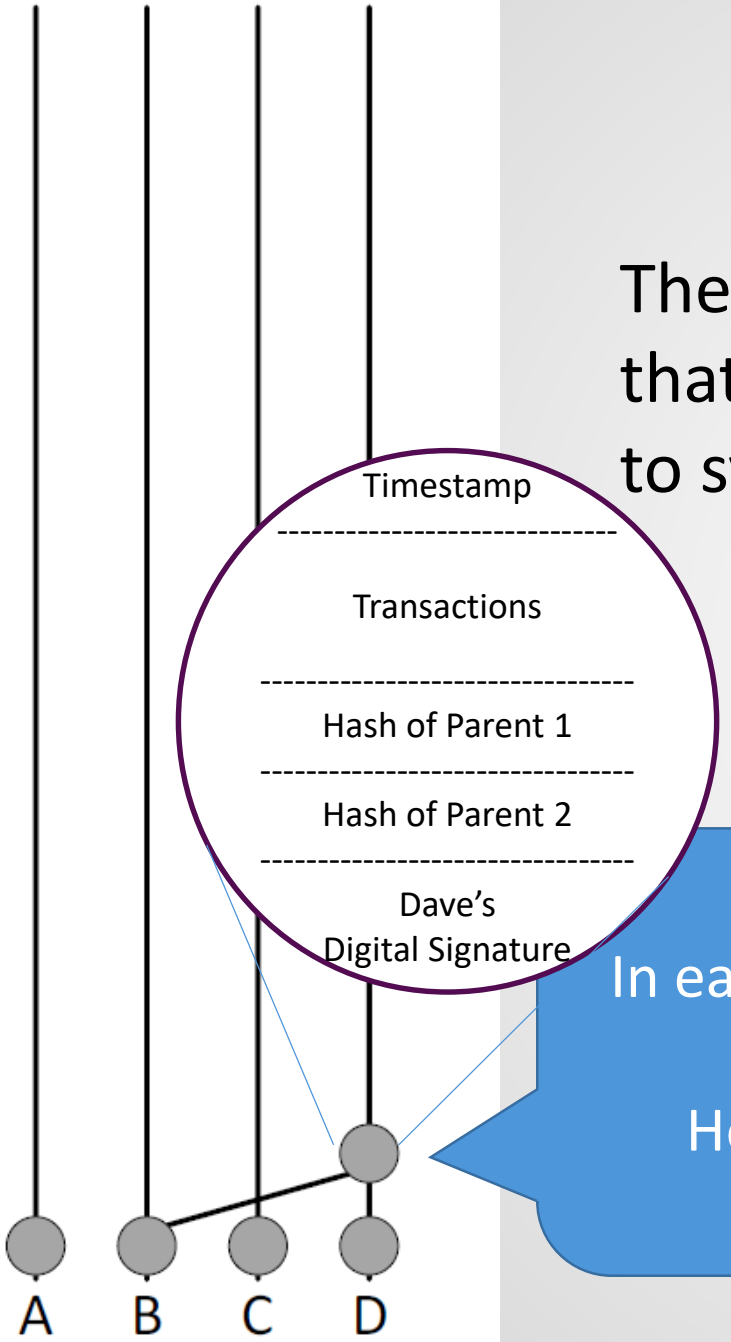
Hashgraph Introduction

A hashgraph is a graph of events which contain transactions.

The goal of the hashgraph consensus algorithm is for the members of the community to come to a *consensus* (agreement) on the *order* of the events (and thus the order of transactions inside the events), and to agree on a *timestamp* for each event (and so for each transaction).

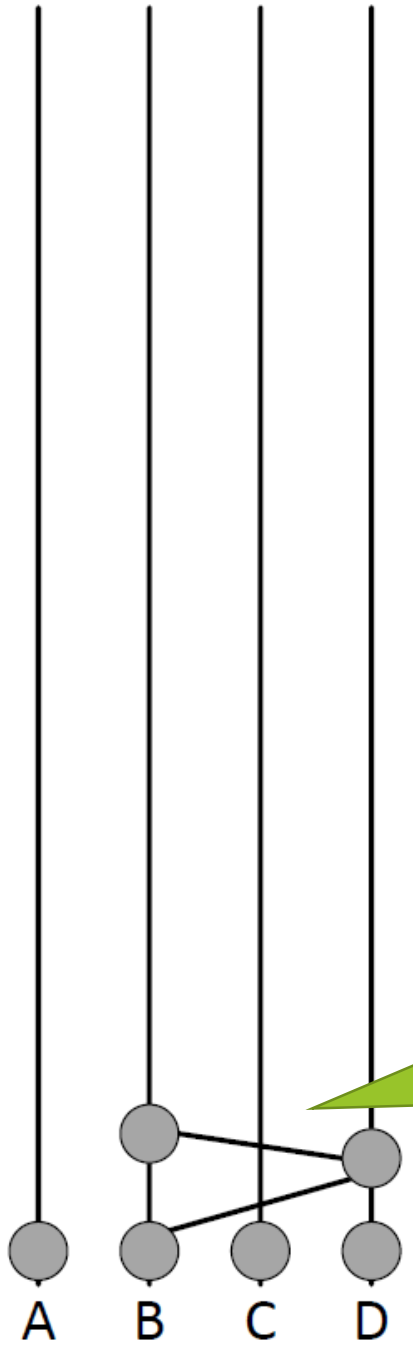
Hashgraph Introduction

The community runs a *gossip protocol*, which means that each member repeatedly calls others at random to sync with them.



In each random contact, a member tells another member all the events he knows (and the other one doesn't).
Here, Dave only didn't know one event that Bob knew.

Hashgraph Introduction

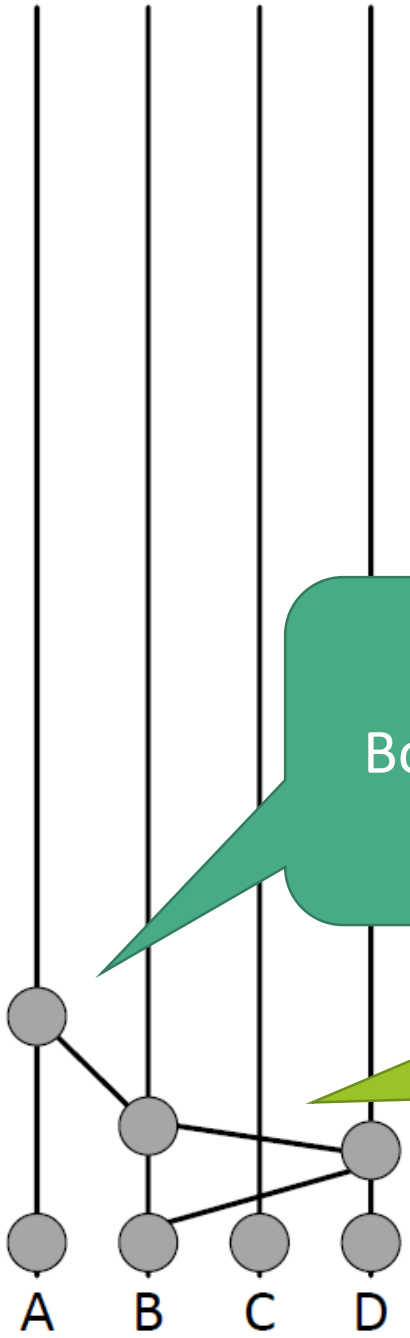


The community runs a *gossip protocol*, which means that each member repeatedly calls others at random to sync with them.

Let's say Dave chooses Bob randomly and sends him all his events (including the new one he just created). Bob records this as an event.

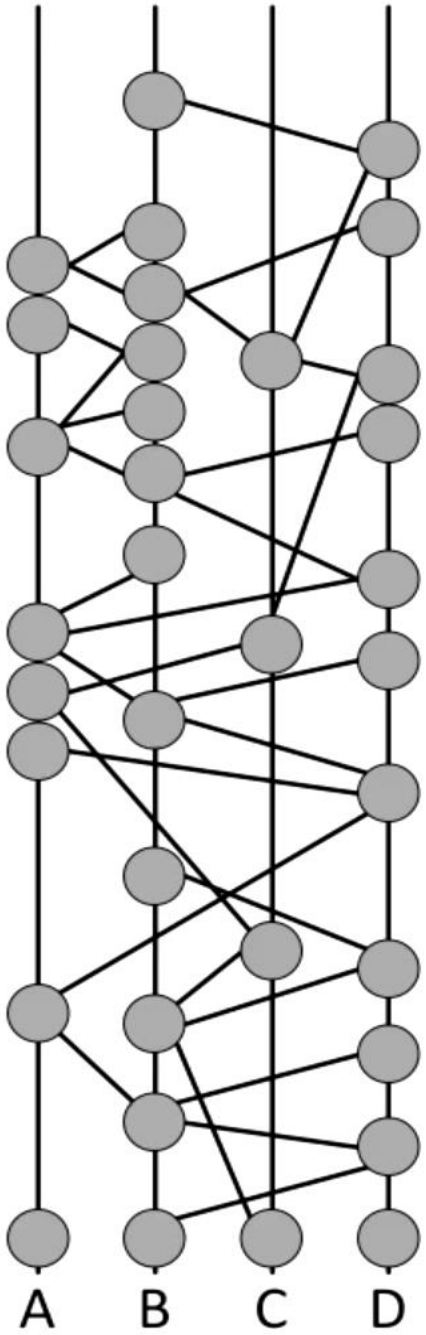
Hashgraph Introduction

The community runs a *gossip protocol*, which means that each member repeatedly calls others at random to sync with them.



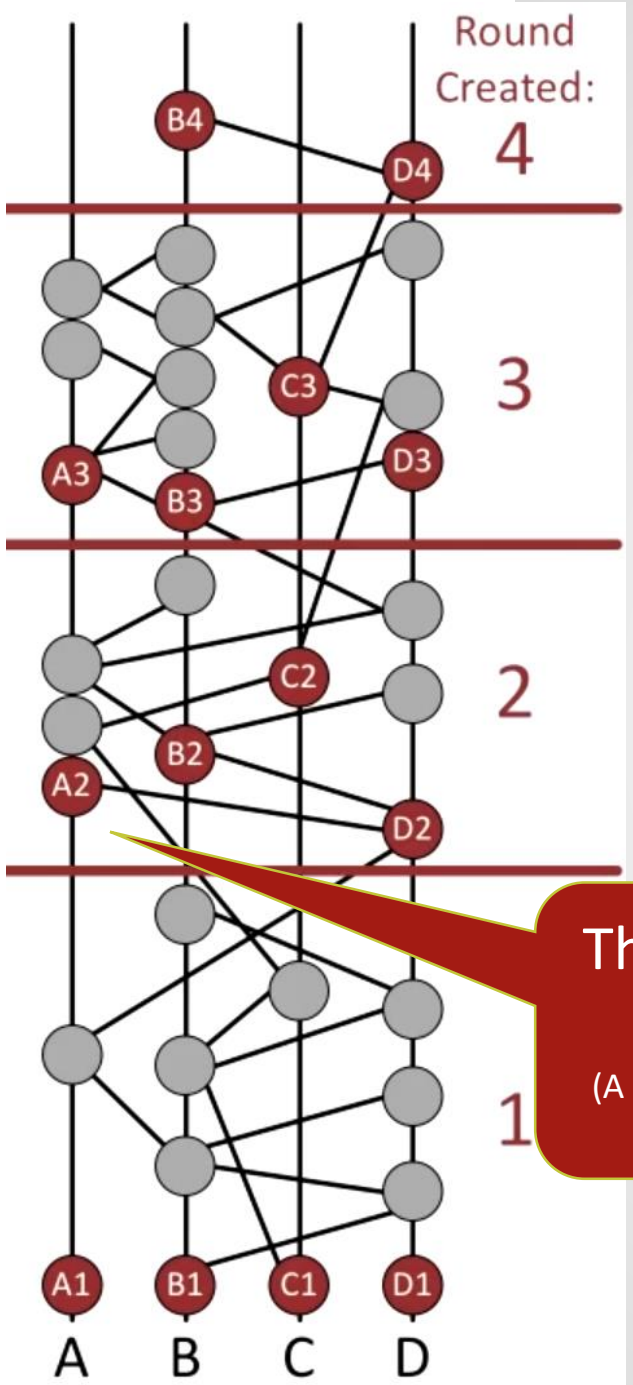
Bob chooses Alice to send the gossip to.

Let’s say Dave chooses Bob randomly and sends him all his events (including the new one he just created). Bob records this as an event.



Hashgraph Introduction

- This continues forever, growing a directed acyclic graph (DAG).
- This is a graph connected by cryptographic hashes, so it is called a hashgraph.
- Each event contains the hashes of the events below it and is digitally signed by its creator.

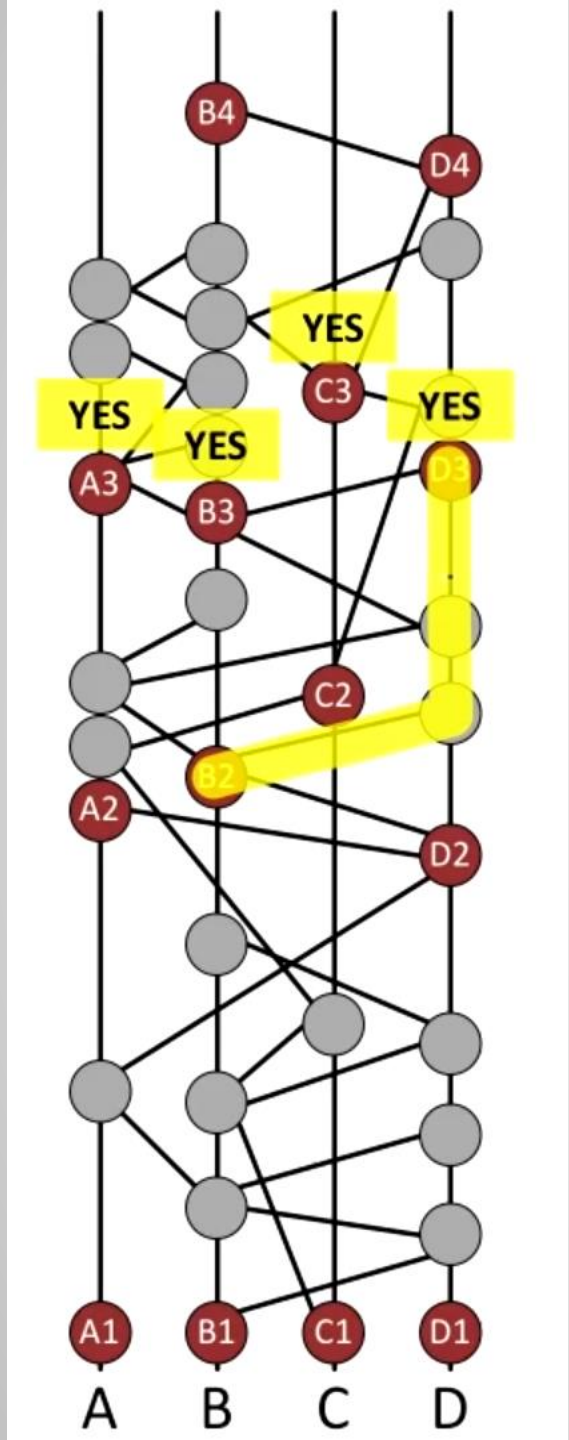


Hashgraph Introduction

- The events are grouped in rounds.
- As soon as you receive an event in a sync, you can immediately find its round. And anyone else receiving it will calculate the same number.

The first event that a member creates in each round is called a witness. Alice's witnesses are labeled A1, A2, … .

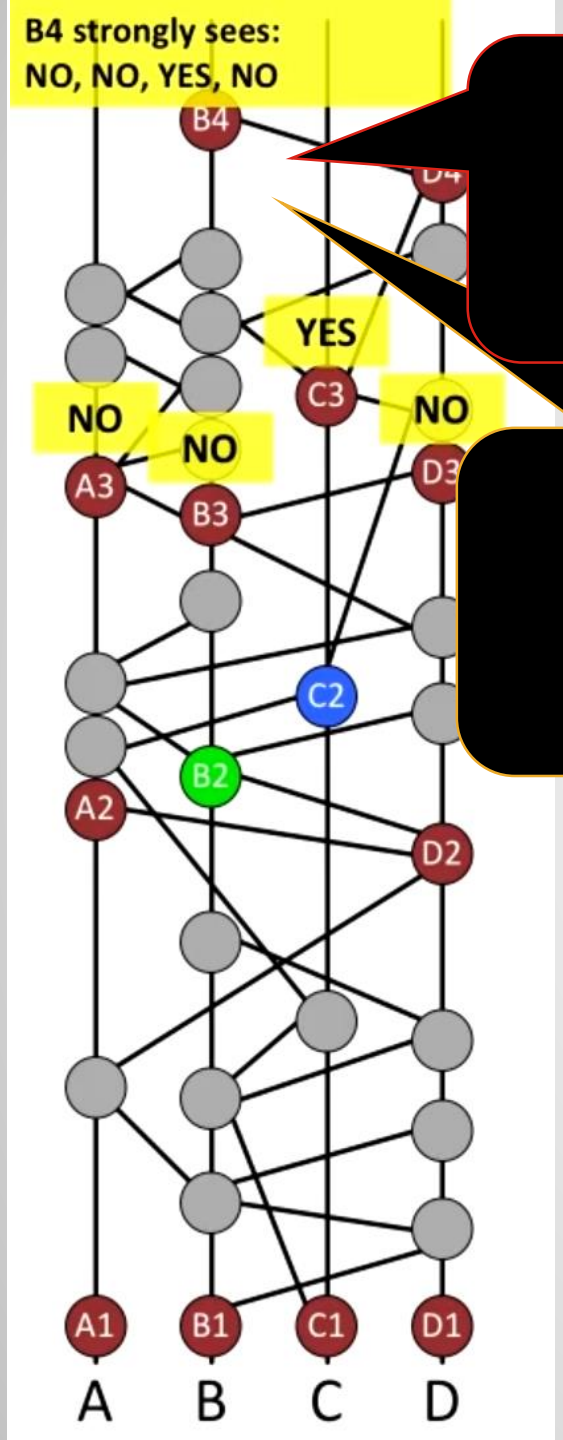
(A new round is created each time one event is able to connect to more than 2/3 of the first events of the current round through the paths that involve at least 2/3 of the nodes in the network)



Hashgraph Introduction

- For each witness, we need to determine if it is a famous witness.
- This is done by the witnesses of the next round.
- **Example:** B2 is considered famous if it is seen by the majority of the witnesses in the next round.
  - Here, B2 is famous, with 4 YES votes.
  - The votes are counted (virtually) by the witnesses of the next round, e.g. B4.

h Introduction



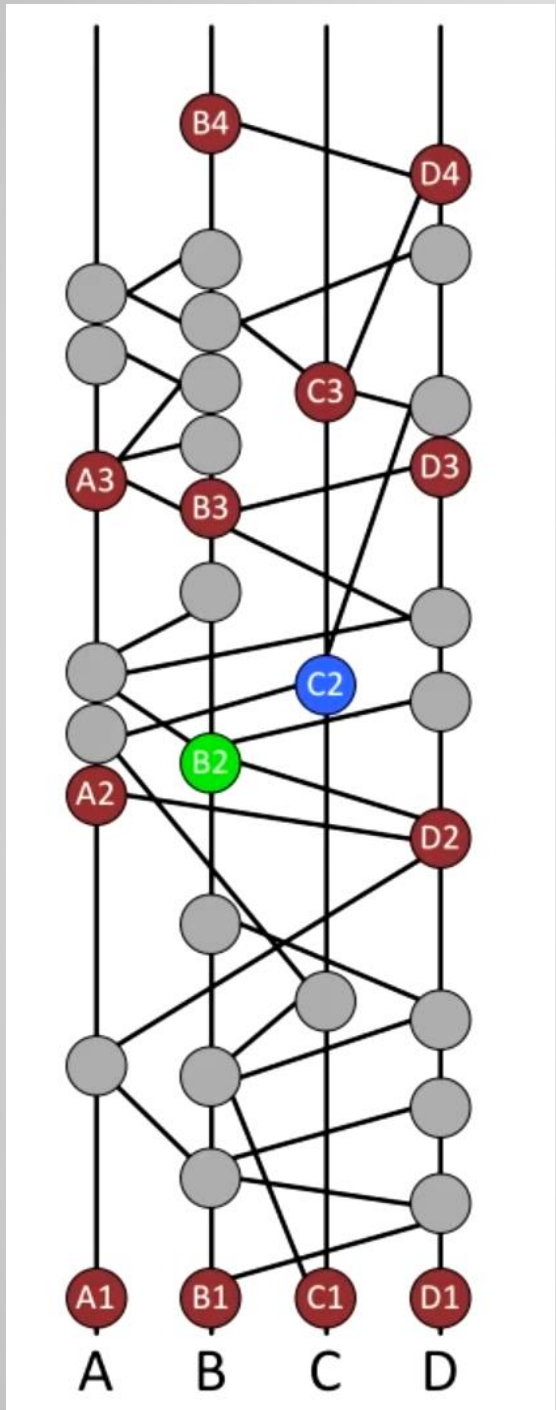
B4 decides that the election result is YES for B2, and colors it green.

B4 decides NO for C2, and colors it blue.

e votes (and registers them in its
om every round-3 witness that it

- To strongly see a witness, there must be enough different paths to it so that they go through a supermajority (2/3) of the population.

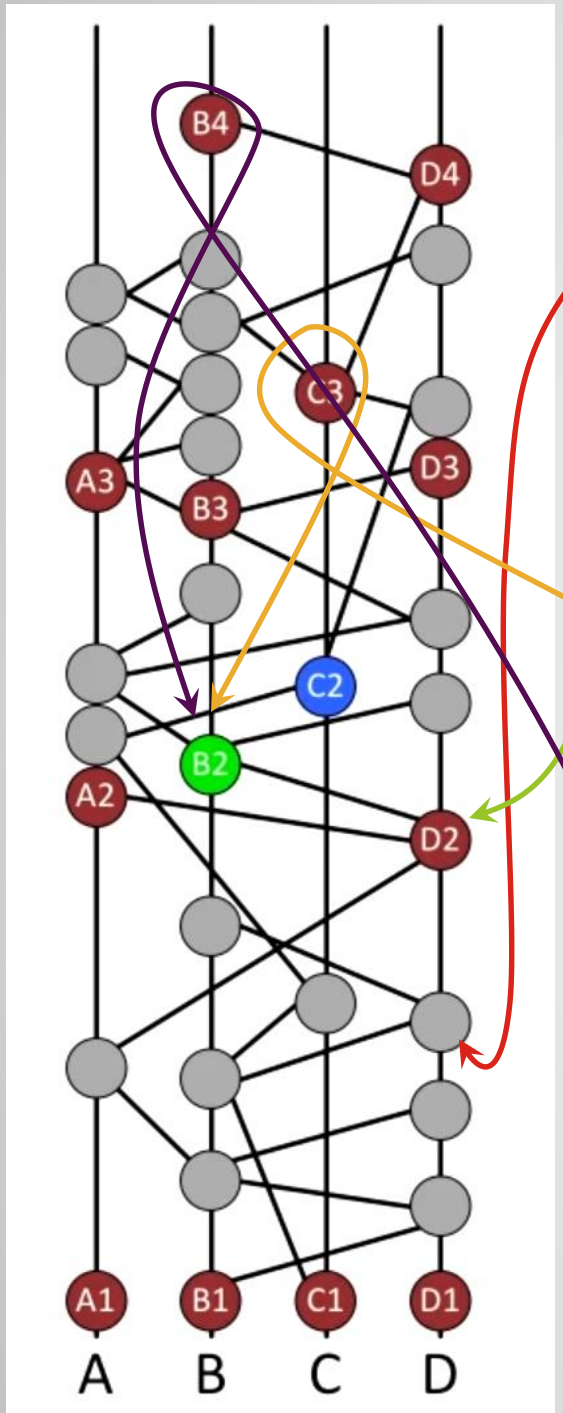
These are the virtual elections, you just saw two.



Hashgraph Introduction

- If B4 cannot decide, it will simply vote based on the majority of what it sees from witnesses of round 3.
  - e.g. 2xYES + 2xNO → vote YES, but not decide.
  - The decision is left to the witnesses of the next round.

- If none of the round-4 witnesses can decide, then each of them will vote.
  - It will be up to the round-5+ witnesses to collect votes from the round-4 witnesses and decide.
  - If cannot, we go to up to the 10th round/coin round (not explained here).



Summary of the Consensus Algorithm

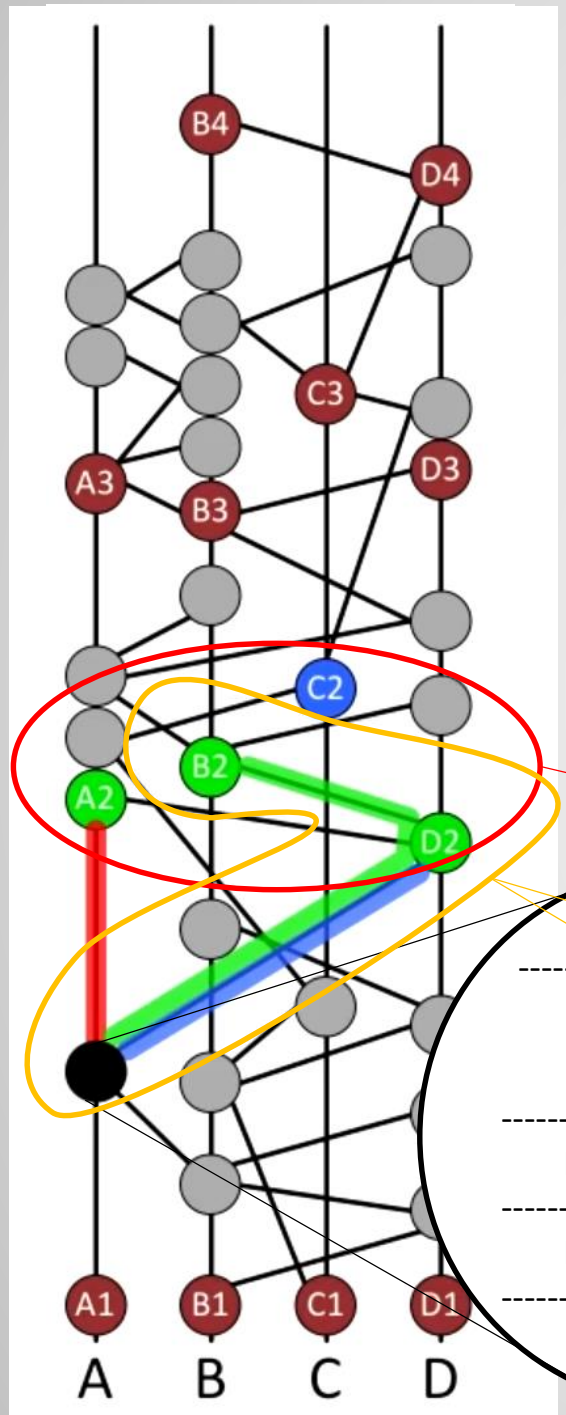
When you get an event, you put it into a round.

The first event in each round is a witness.

The witnesses of the next round judge whether the previous round witnesses are famous or not (election).

The witnesses of the round after, collect the votes and decide YES or NO about the fame of each of the witnesses two rounds before.

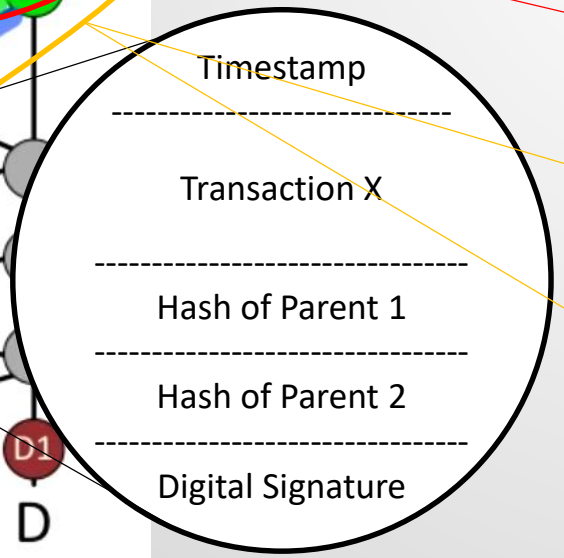
- **Theorem:** We will always decide, eventually, whether a given witness is famous or not, and this decision is gonna be the same for everybody, even if an attacker disrupts part of the communications.



Why did we go through all this?!

Blockchains were invented **"to store transactions distributively and create a consensus on their order. "**

Imagine we want to know when Transaction X has happened?



1. Find the first round in which all the famous witnesses have seen (received) the event.
2. Find the earliest event time for each user that has seen that event.
3. Find the median of those events times

So…, what is the benefit?

Transactions per second (tps) :

Bitcoin (PoW): ~7 tps

Ethereum (PoW ver.): ~15 tps

Hashgraph: ~250000 tps (theoretically)

Hashgraph is only limited by the bandwidth of the internet.

- IOTA claims the same, but has reached 1000tps.

So…, what is the benefit?

Fairness : In Bitcoin, a miner gets to decide whether or not to add a transaction in a block, and thus the order in which it wants the transactions to be put. This can be perceived as unfair by the end-users and prevents building applications such as stock exchange on a blockchain. In Hashgraph the timestamp protocol is (claimed to be) fair for all the users.

So…, what is the benefit?

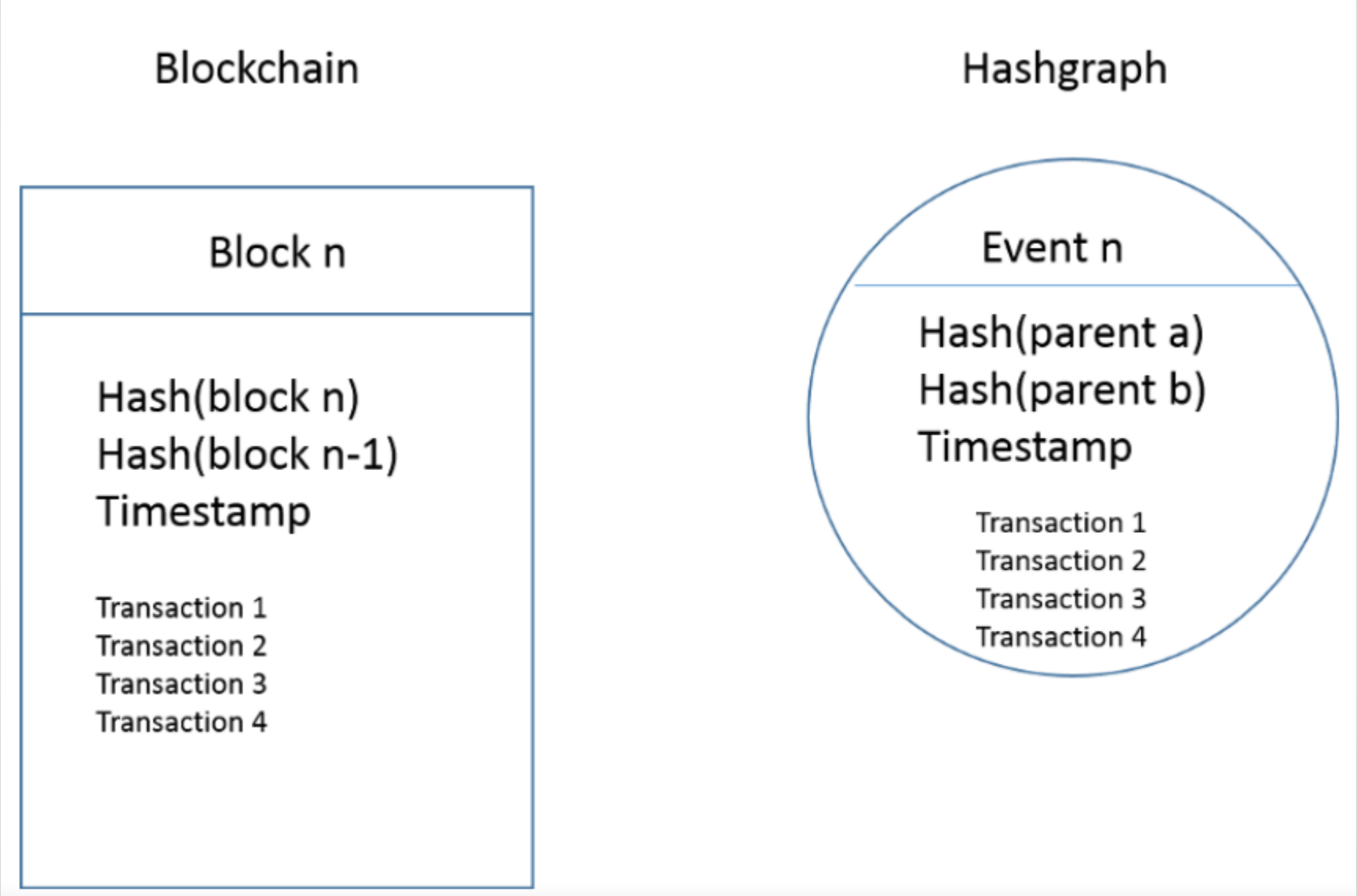
Security : Hashgraph is a distributed consensus technology which is A-BFT (Asynchronous Byzantine Fault Tolerant).

- With less than 1/3 malicious nodes, the protocol reaches a consensus. The attackers can take control of the whole Internet, and do DDoS as well. But the protocol works if every now and then one message gets through.
- No forking is possible, by design.

What's "Asynchronous" Byzantine Agreement?

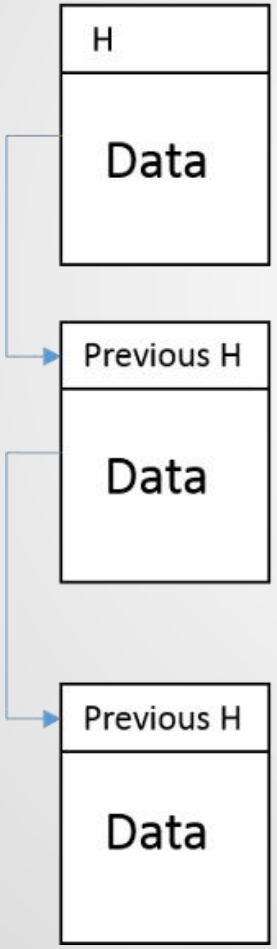
https://www.youtube.com/watch?v=mm40Kkgzw-A

Data Structure Differences

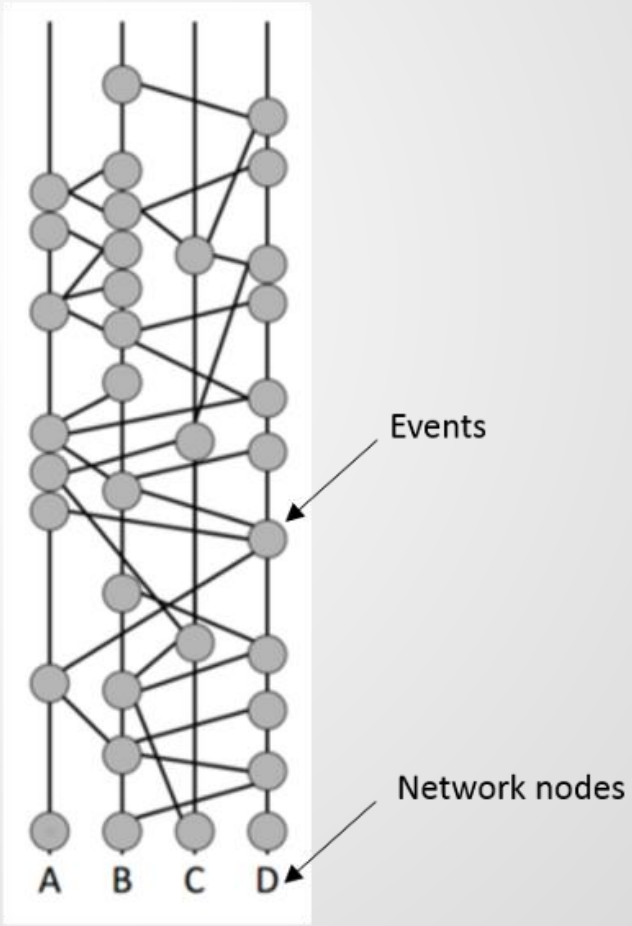


Event Registration Differences

Blockchain



Hashgraph



Wrap up

- We learned about another DAG-based DLT, namely hashgraph.
- It’s a permission-based DLT that works based on gossiping and cryptography and claims to be able to reach high TPSs.
- We finalize the topic of DAG-based DLTs here and talk about the economics of blockchains next.

See you in the next session …