kybern

Hashgraph

Alberto Ballesteros

Kybern

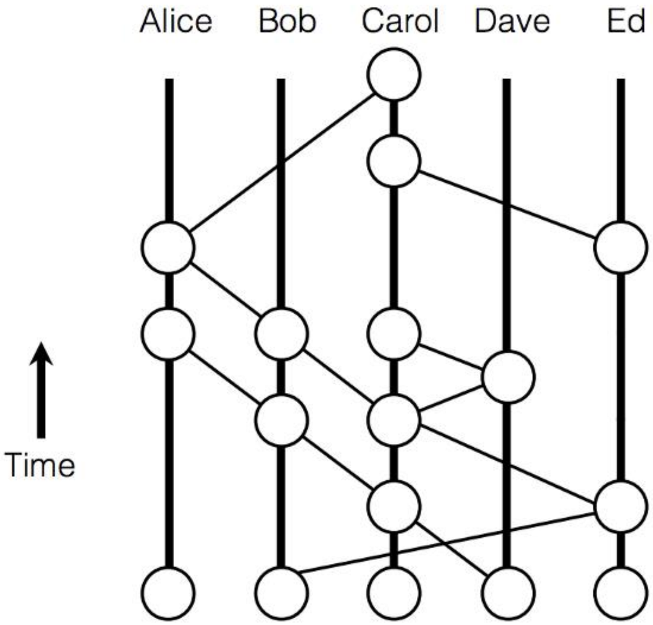
Contents

- Definition
- Concepts
- How it works?
- Use Cases
- Hashgraph vs Blockchain
- References

Definition

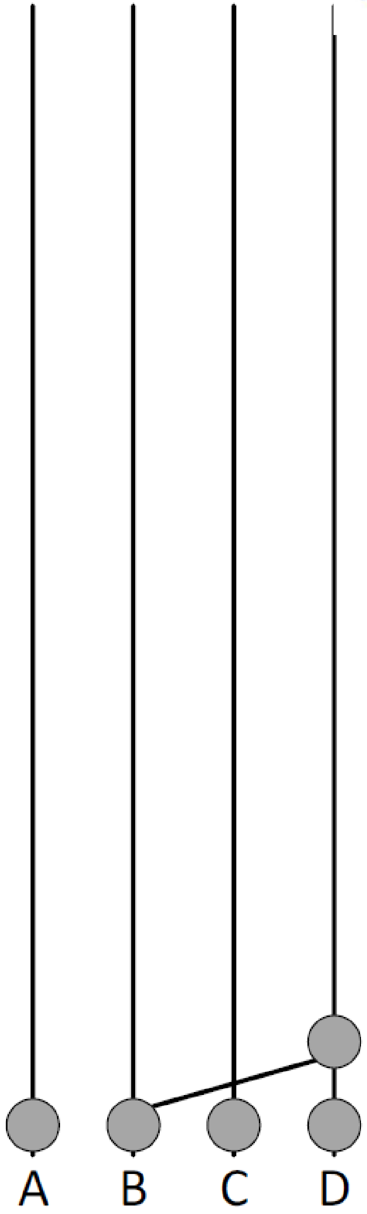
- Data structure that records who gossiped to whom, and in what order.

- Consensus algorithm:
  - Fast, Secure, Fair
  - Techniques:
    - Gossip about Gossip
    - Virtual Voting



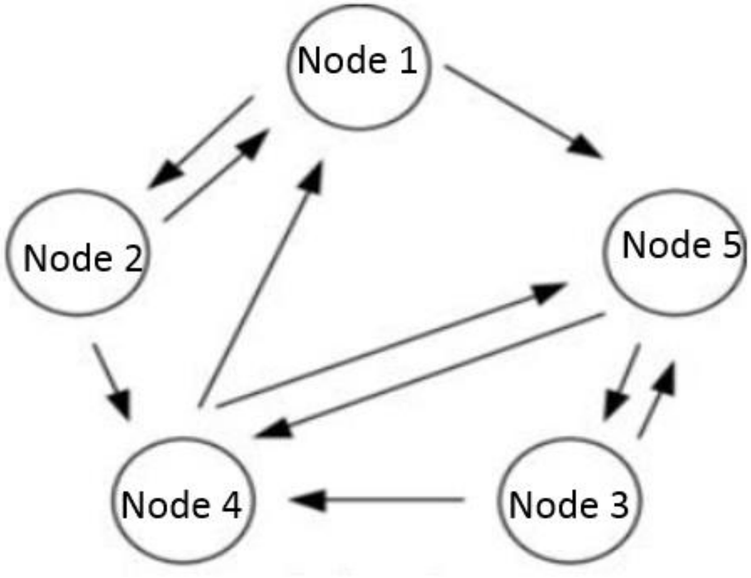
Concepts

- Members: Full nodes (A, B, C, D)
- Events: Data structure (Circles)
- Gossip: Information
  - *Gossip protocol* (Communication)
- Consensus on the order of the events and transactions



Gossip protocol

- Information exchanged via gossip between peers.
- Each member calls others randomly to sync with them.

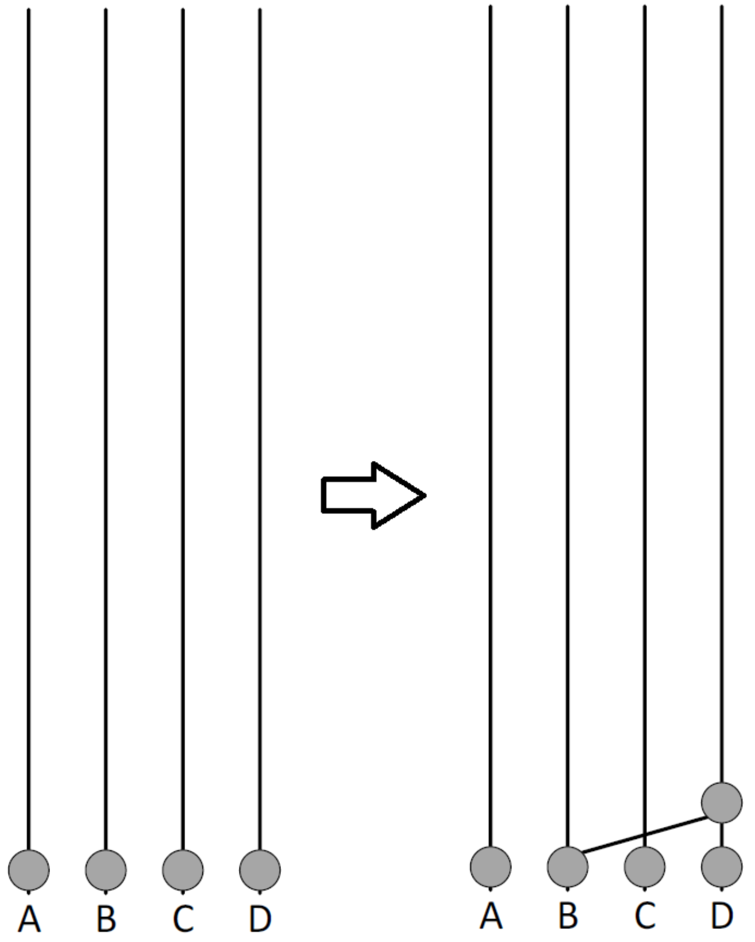


How it works?

- Each member create an event.

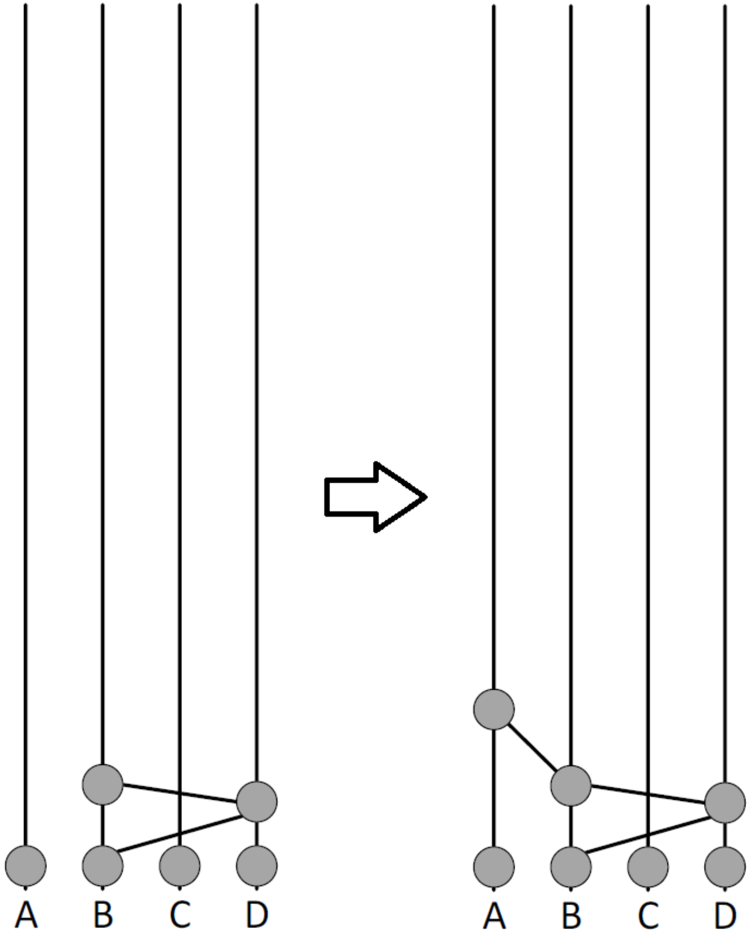
- Each event can contain zero or more transactions

- Gossip protocol:
  - B call D randomly
  - Sent just ONE event



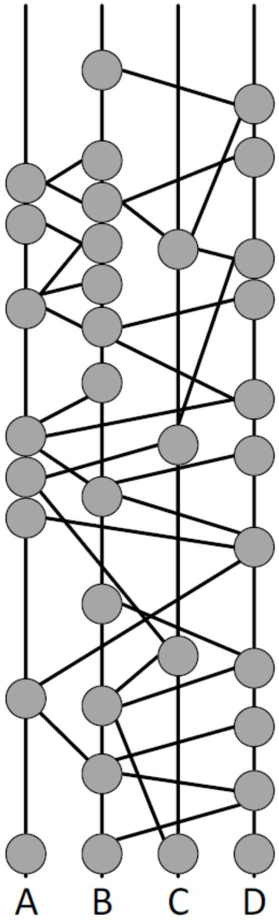
How it works?

- Typically D call B (can all A or C)
- B randomly call A and send 4 events.
- How many events know A?
- A create sync event
- A call B?



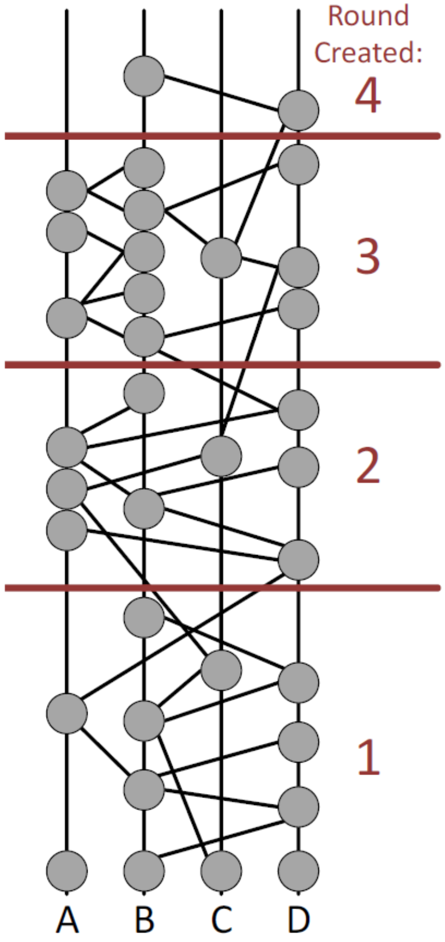
How it works?

- A called D (not B)
- Graph connected by hashes → hashgraph
- All events are signed by its creator
- Older parts inmutable



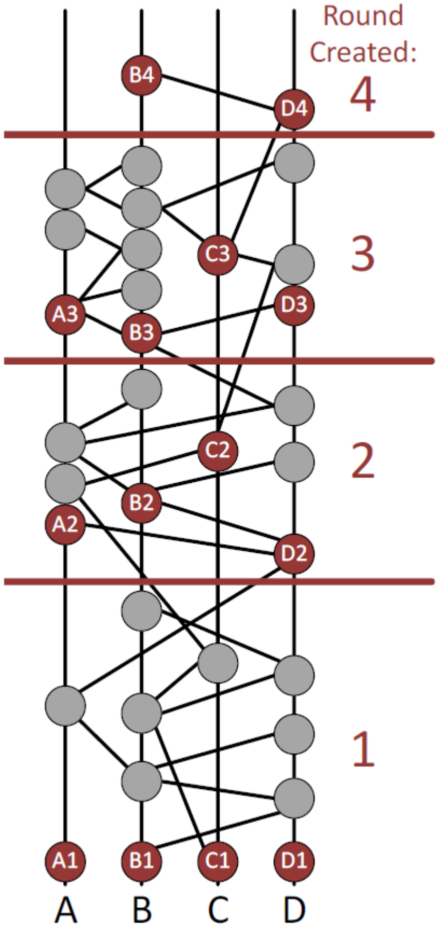
Virtual voting

- Place all the events in order (everybody same order)
- First: Hashgraph divided in rounds
- Round calculated for each event inmediately



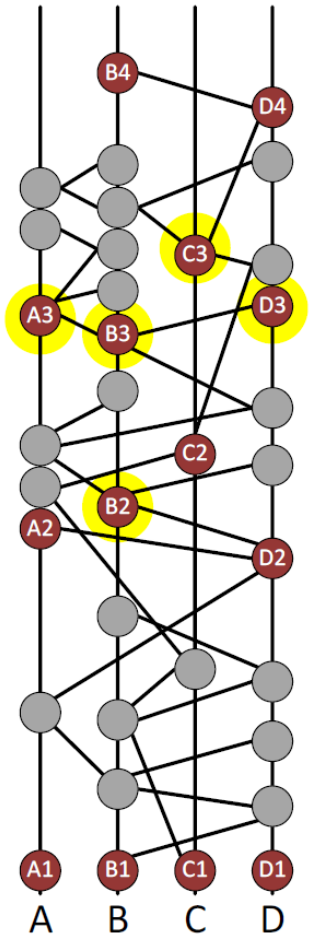
Witness

- Witness: first event in a round for a given member
- 40% are witnesses (4 nodes)
  - ↑ nodes, ↓ % witnesses
- Responsible of calculations
- *It is possible for a member to have no witnesses in a given round. (Round 4)



Famous witness

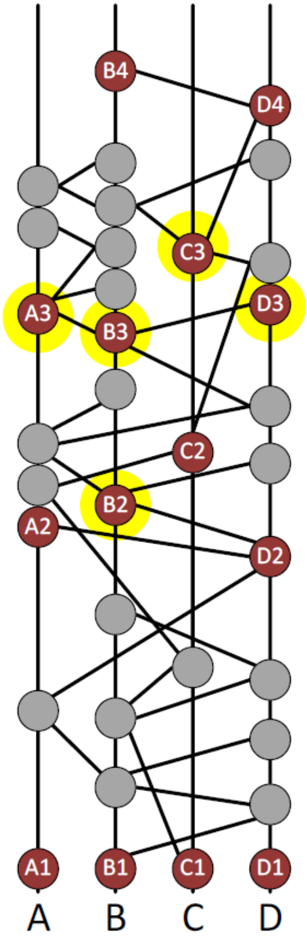
- Famous witness: a witness seen by many witnesses in the next round
- For each witness, we need to determine if it is a famous witness
- Election: Witnesses vote



Famous witness

- X2 are famous?
  - Who vote?
    - X3 witnesses
  - Who count the votes?
    - X4 witnesses

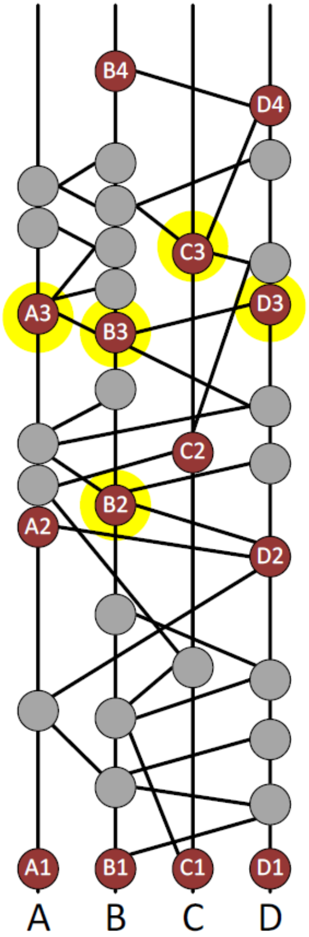
- X2 = {A2, B2, C2, D2}
- X3 = {A3, B3, C3, D3}
- X4 = {B4, D4}



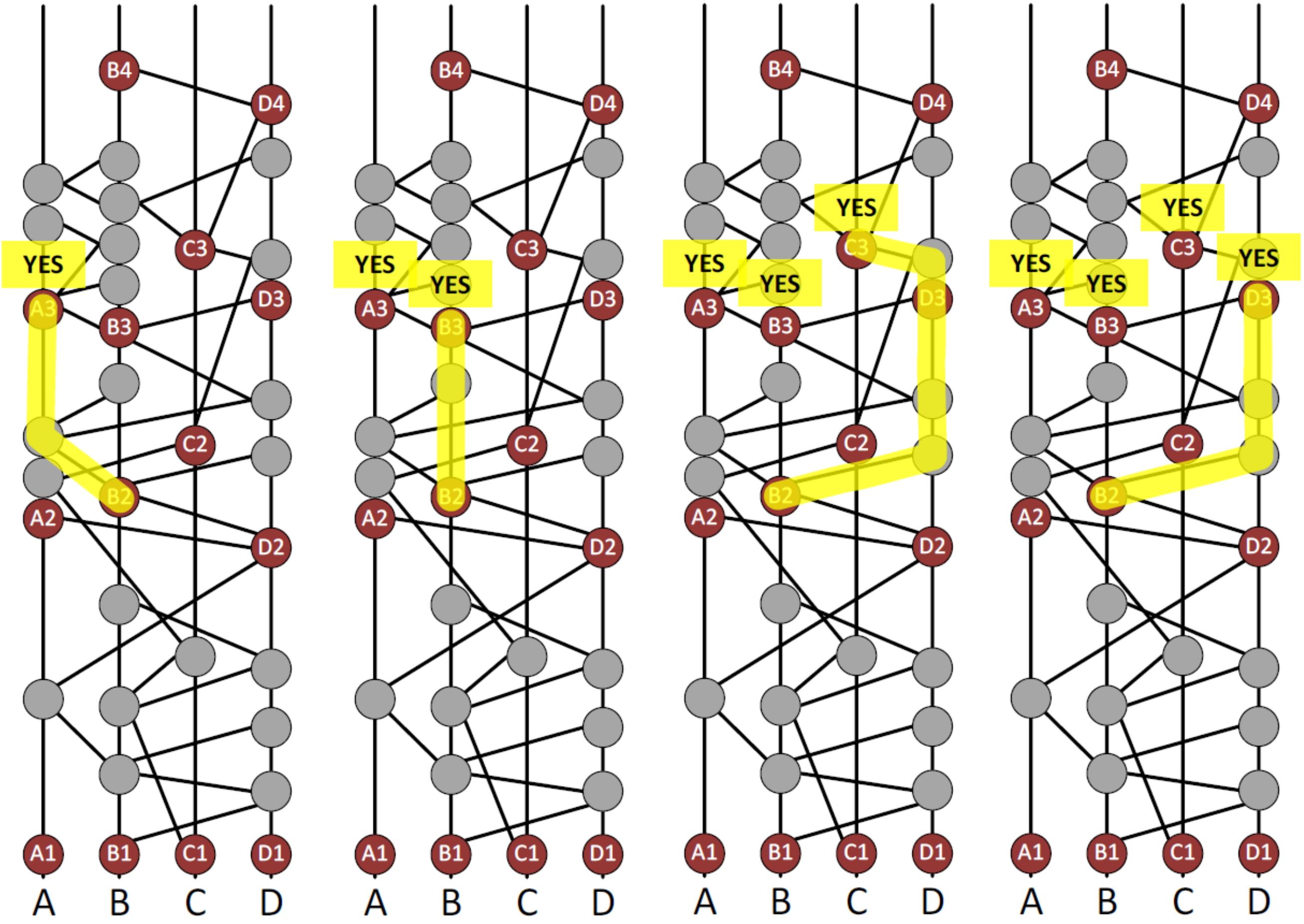
Election

- Vote YES if there is an entirely-downward path from X3 to X2

- A3 can see B2?
- B3 can see B2?
- C3 can see B2?
- D3 can see B2?



Is B2 famous?



B4
D4
C3
D3
B3
C2
B2
A2
D2
A3
A1
B1
C1
D1
A
B
C
D
YES
YES
YES
YES
YES
YES
YES
YES
YES
YES

Is B2 famous?

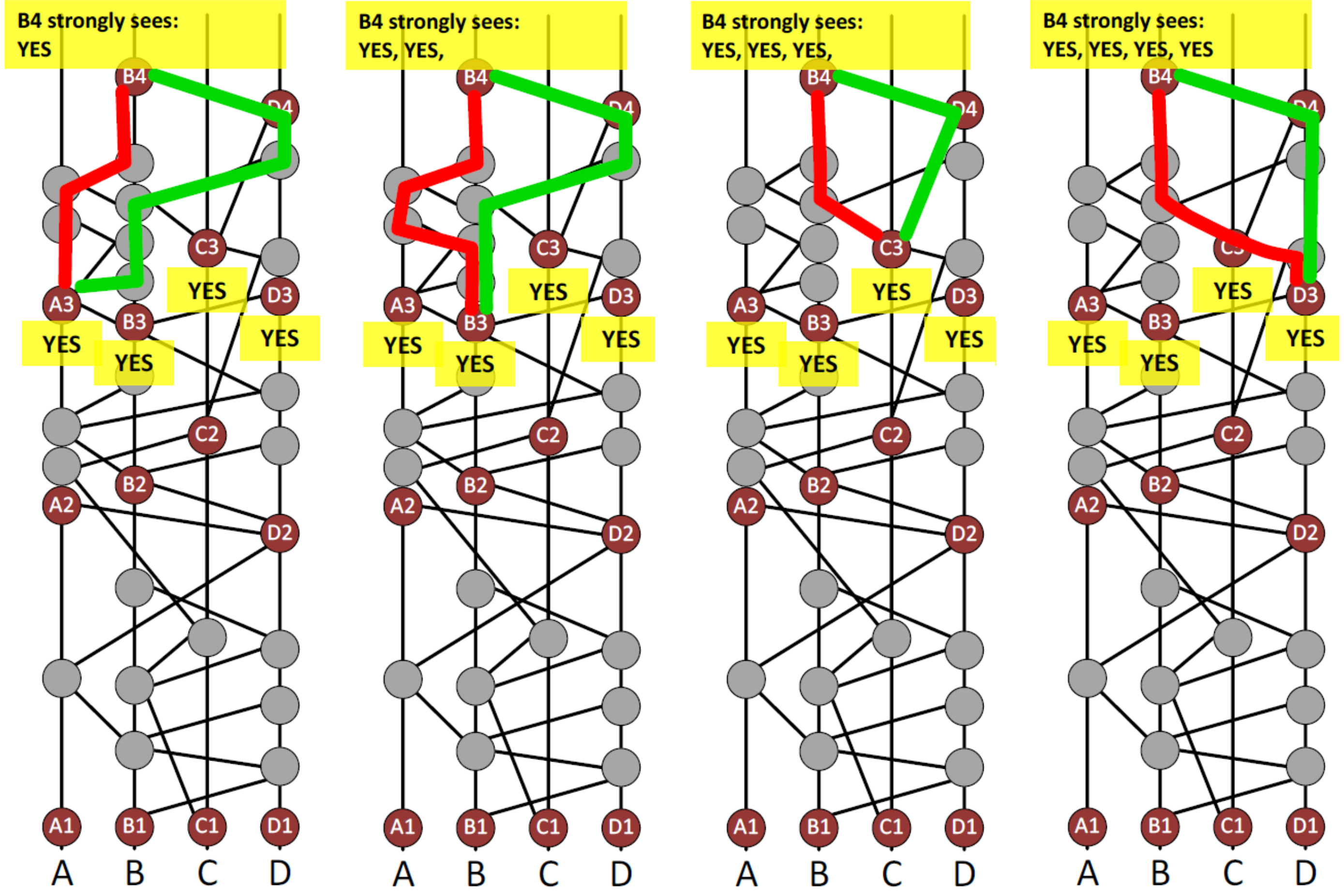
- All X3 witnesses voted YES

- Votes will be counted by X4 witnesses: {B4,D4}
  - Only if X4 strongly see a witness

  - Strongly see: To strongly see a witness there must be enough different paths to it so that together, the paths go through a supermajority of the population

  - Supermajority: $t > \frac{2n}{3}/t, n \in \mathbb{N}$

Is able B4 to strongly see X3?



B4 strongly sees: YES

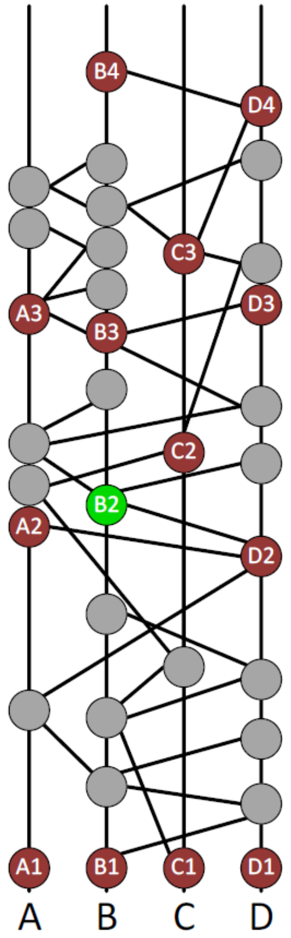
B4 strongly sees: YES, YES,

B4 strongly sees: YES, YES, YES,

B4 strongly sees: YES, YES, YES, YES

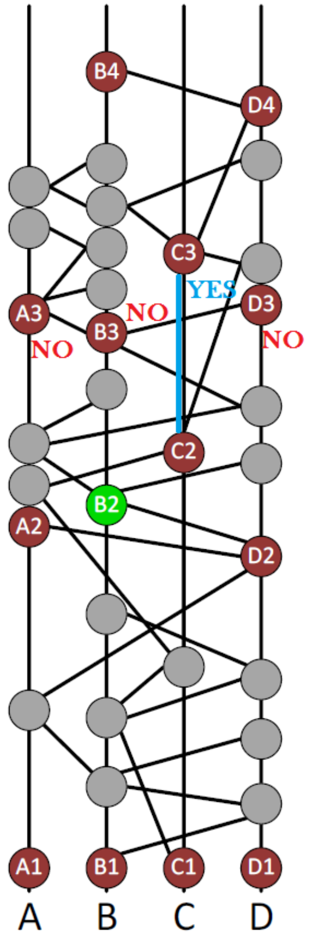
Decide - YES

- Supermajority: YES
- Decide: declare the winner, end election
- B4 has received YES from a supermajority:
  - Election result: YES, B2 is famous!



Decide - NO

- Supermajority: NO
- B4 has received NO from a supermajority:
  - Election result: NO, C2 is famous!
- C2 is not famous



Decide - Other cases

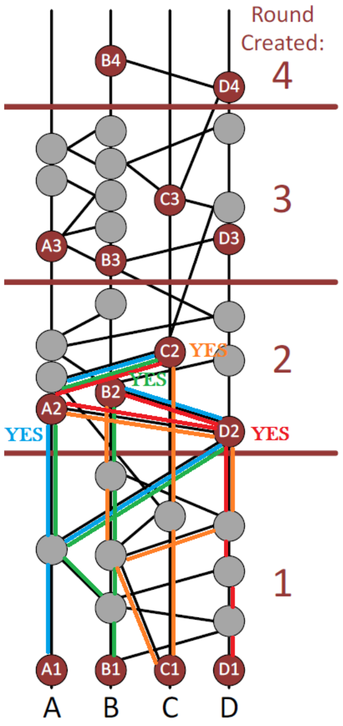
- If B4 wasn’t able to decide → Consider D4
- If D4 fails → Consider A4 or C4
- If none of the round-4 witnesses can decide:
  - Simply vote in accordance with the majority
  - If tie → vote YES
  - Perhaps the round-5 witnesses will be able to decide, if not rount-6 witnesses and so on

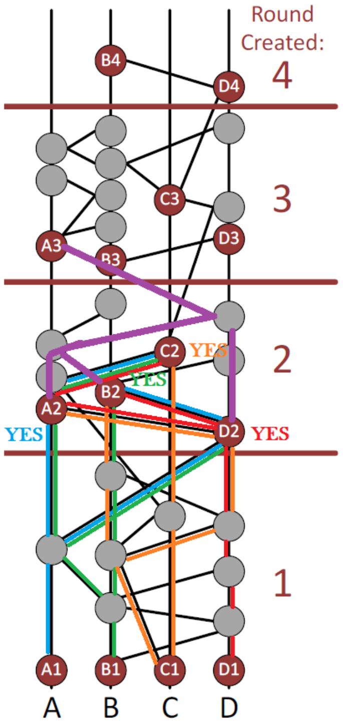
Coin round (theory)

- Normal round:
  - – Collect a supermajority → Decide
  - – Collect fewer → Vote majority
- Coin round (every 10th round)
  - – Collect a supermajority → Vote majority
  - – Collect fewer → Vote randomly
  - – “random”: middle bit of own digital signature
    - Bit 1: vote YES
    - Bit 0: vote NO

Round 1 witnesses

- Is A1 famous? YES
  - Blue paths
- Is B1 famous? YES
  - Green paths
- Is C1 famous? YES
  - Orange paths
- Is D1 famous? YES
  - Red paths
- A3 decides



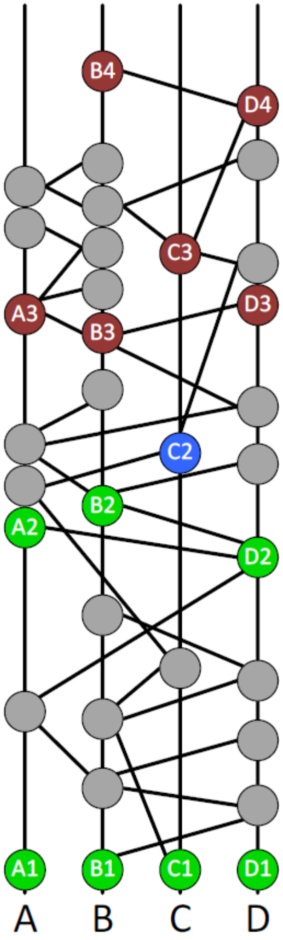


Recap

- As soon as you get an event you put into a round
- First event in each round is a witness
- Each witness have to decide if it's famous or not
- Hold an election, collect votes and decide
- Prob(decide) = 1, everybody decide the same

Next steps

- Hard part: agree on who is famous
- Find round received for earlier events (Below X2 witnesses)
- Gray events
  - Consensus order
  - Consensus timestamp

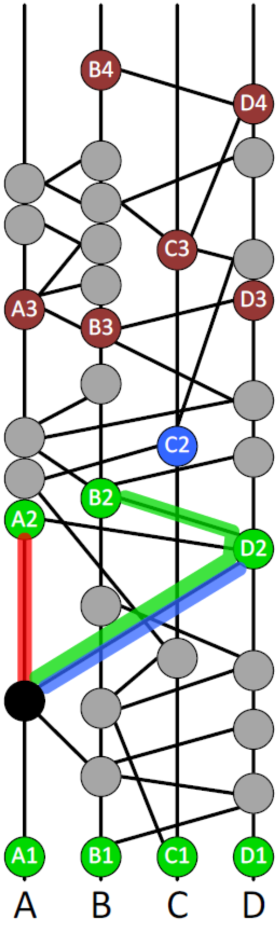


Round received

- The round received of an event x is defined to be the first round where all unique famous witnesses are descendants of x.

- All round-2 famous witnesses see the black event

- Black event → Received in round 2

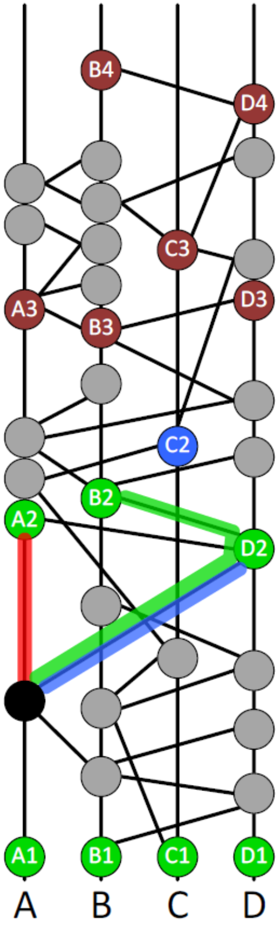


Consensus timestamp

- Median timestamp when A, B and D first saw it

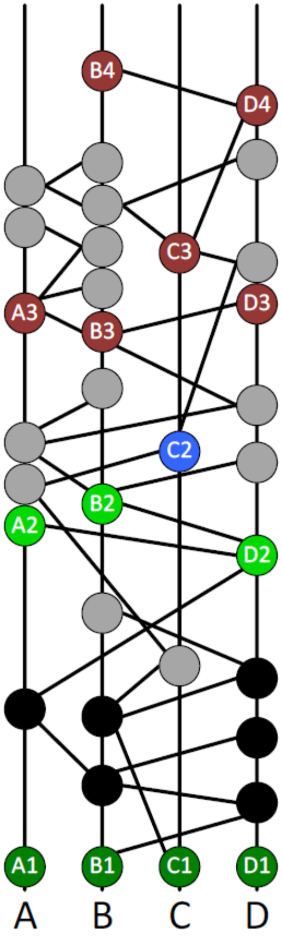
- Earliest event is D2 for D
- Earliest event is B2 for B
- Earliest event is BLACK for A

- Middle one from the list (second middle for even number)



Consensus order

- 10 events:
  - Round received: 2
  - Ties are broken with:
    - Consensus timestamp
  - Further ties broken:
    - Extended median
- Extended median:
  - Signature XORer with pseudorandom number

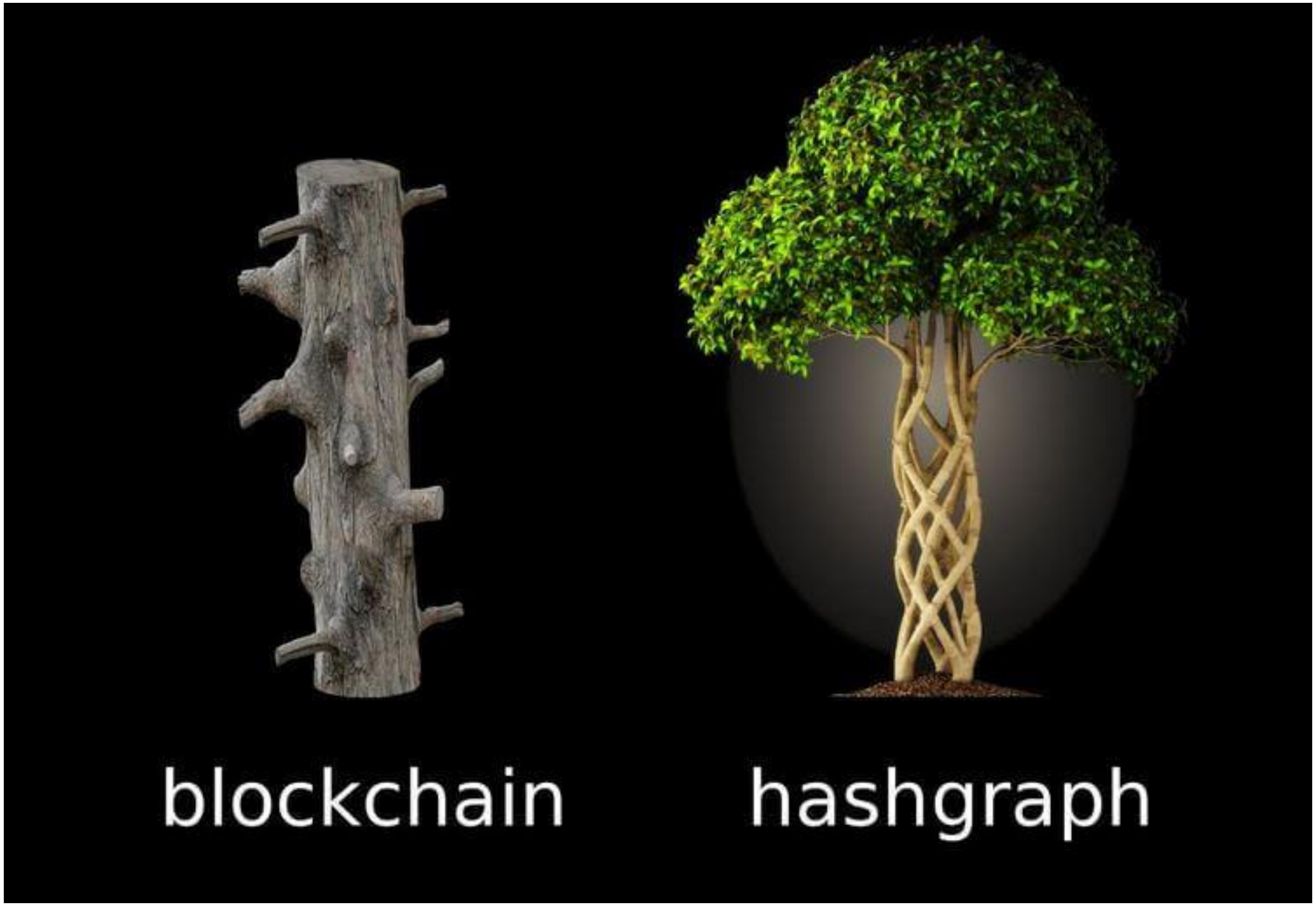


Use cases

- Hashgraph do everything blockchain does

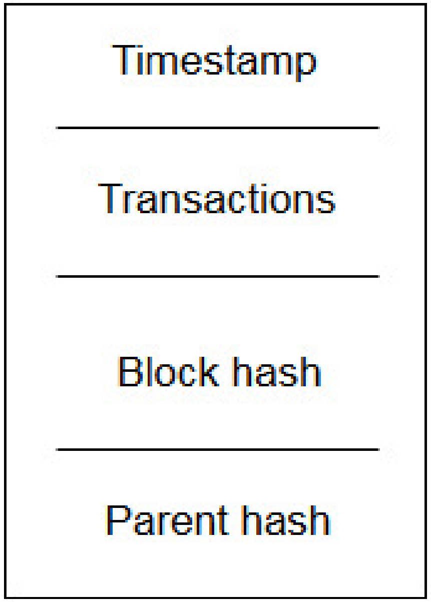
- Because of the fairness properties
  - Build a fair distributed stock market
  - Build World of Warcraft, a distributed World of Warcraft
  - Could build an eBay, a distributed eBay
  - Identity management

Hashgraph vs Blockchain



Data structure

Block (Blockchain)



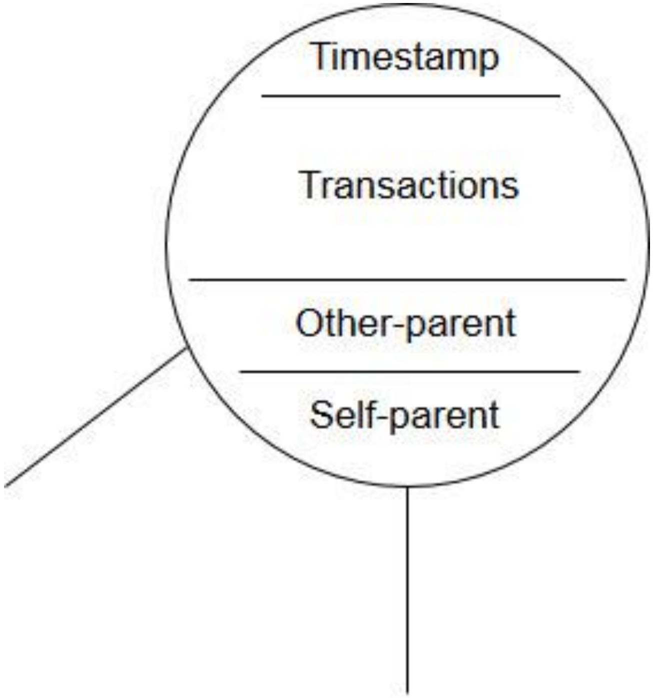
Timestamp

Transactions

Block hash

Parent hash

Event (Hashgraph)



Timestamp

Transactions

Other-parent

Self-parent

Hashgraph vs Blockchain

- No PoW or PoS, all nodes contribute.
- No miners, timestamp consensus
- Over 250.000 tps (~10 tps Ethereum) only limited by bandwidth. Ethereum or Bitcoin limited by their consensus protocol.
- Permissioned network. Technical details for its deployment as a public ledger? Security?

References

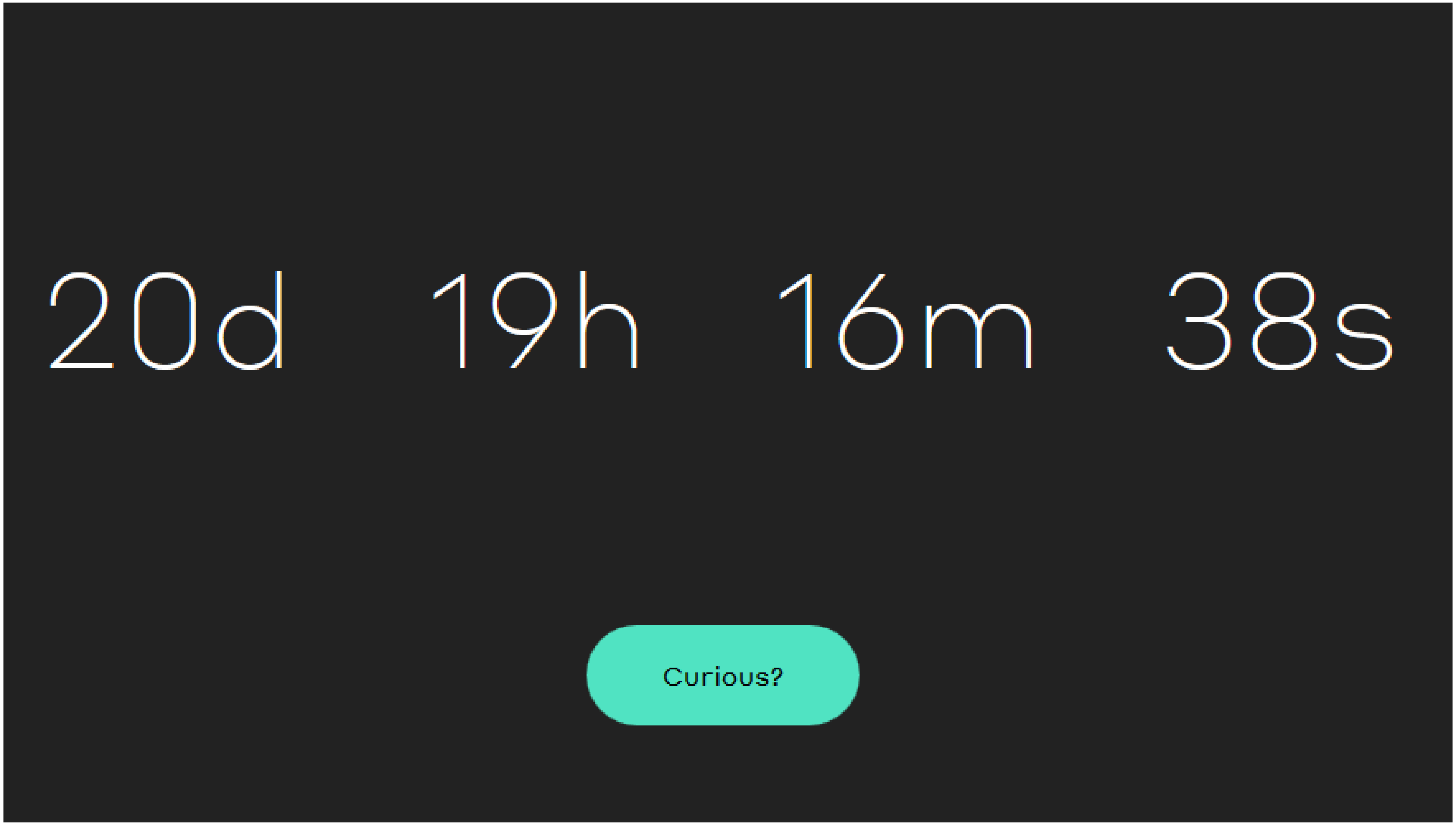
- Web:
  - https://hashgraph.com/

- Whitepaper:
  - https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

- SDK:
  - https://www.swirlds.com/download/

- Gossip protocol:
  - https://en.wikipedia.org/wiki/Gossip_protocol

Announcement



20d 19h 16m 38s

Thanks!