Lesson - Introduction to

SWIRLDS Hashgraph Consensus Algorithm

Practice Examination

1. The best definition of consensus is:
    a. A majority of members agree on a result
    b. All members agree on a result
    c. ⅓ members agree on a result
    d. ⅔ members agree on a result

2. What is the best description of virtual voting
    a. A witness counts the votes sent to it
    b. Everyone pretends to be another member on the hashgraph and knowing how that member would vote and casting and counting their vote on their behalf
    c. Asking a member to send a vote so it can be counted
    d. Everyone pretends to be a vote collector and count votes that a member has sent you

3. What is the first step to conduct a virtual vote
    a. divide the hashgraph into rounds created
    b. divide the hashgraph into rounds received
    c. obtain a consensus vote from round members
    d. obtain a consensus vote from famous witnesses

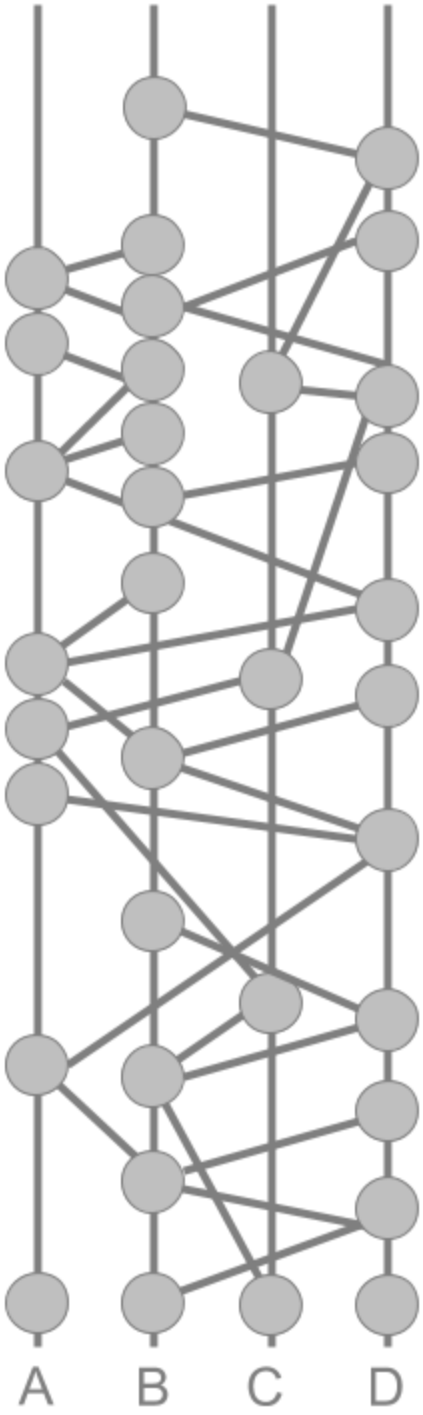
4. What is an important principle to be remembered for virtual voting
    a. As soon as a vote is counted there is immediate consensus for when it was counted
    b. As soon as an event is created the round that event was created in can be immediately determined based on a vote
    c. As soon as an event is created the round that event was received in can be immediately determined based on a famous witness
    d. As soon as an event is created the round that event was created in can be immediately determined

5. What best describes how to determine what round an event is created created in?
    a. An event is always created in the same round as it's parent event
    b. An event is always created in the same round as it's other parent's event

c. An event is created in the same event as it's parent unless if it strongly sees the witnesses in that round then it will be considered to be a witness of the next round (add 1 to round created)
d. An event is created in the same event as it's parent unless if it strongly sees the witnesses in that round then it will be considered to be a witness of the next round (subtract 1 from the parents round)

6. What best describes when a virtual vote election is over
    a. As soon as a majority decides Yes or No the election is over
    b. As soon as a majority decides the election is over
    c. As soon as a supermajority decides Yes or No the election is over
    d. As soon as a supermajority of members decides Yes or No the election is over

7. If one event collects a supermajority of "No" votes and another event collects a supermajority of "Yes" votes what will happen
    a. A new election will take place in the next round
    b. Another event will count the votes
    c. A coin round will take place
    d. It is impossible for this to occur using the consensus algorithm



8. The best definition of consensus is:
    a. A majority of members agree on a result
    b. All members agree on a result
    c. ⅓ members agree on a result
    d. ⅔ members agree on a result

9. List the 5 types of Distributed Ledger Technologies (DLT)s

    _____

    _____

    _____

    _____

    _____

    Ans: Proof of Work, Leader Based, Economy Based, Voter Based, Virtual Voting

10. What type of DLT is blockchain

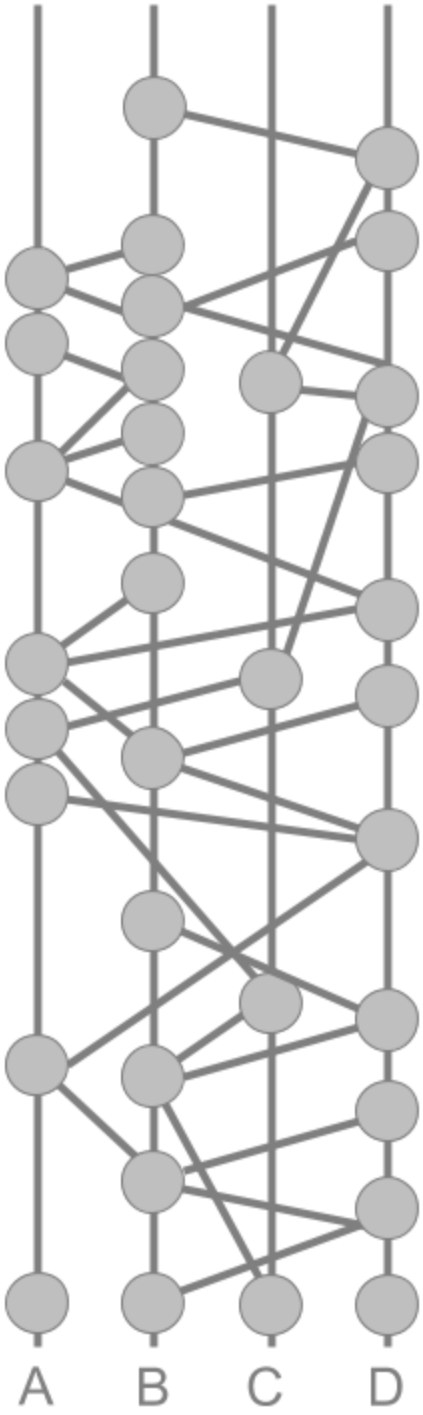
    a. Proof of work

    b. Leader Based

    c. Economy Based

    d. Voter Based

11. What type of DLT is SWIRLDS Consensus Algorithm



a. Proof of work

b. Leader Based

c. Voter Based

d. Virtual Voting Based

12. The best description of Asynchronous Byzantine Fault Tolerance (ABFT) is:

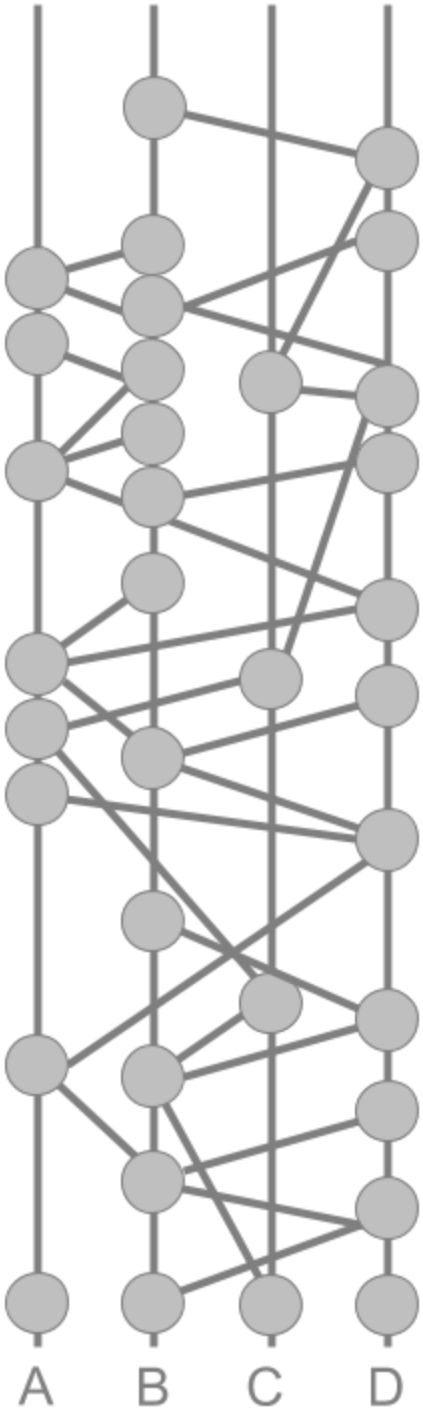
a. the highest degree of security that a consensus algorithm can provide ABFT means that a) a finality of consensus will never be reached with a finality of 1 if b) attackers control less than ⅓ of the participants and c) an assumption only that messages from an honest node will eventually get through, but makes no assumptions about how long that takes.

b. one of the highest degree of security that a consensus algorithm can provide ABFT means that a) a finality of consensus will be reached with a finality of 1 if b) attackers control less than ⅓ of the participants and c) an assumption only that messages from an honest node will eventually get through, but makes no assumptions about how long that takes.

c. the highest degree of security that a consensus algorithm can provide ABFT means that a) a finality of consensus will be reached with a finality of 1 if b) attackers control less than ⅓ of the participants and c) an assumption only that messages from an honest node will eventually get through, but makes no assumptions about how long that takes.

d. the highest degree of security that a consensus algorithm can provide ABFT means that a) a finality of consensus will be reached with a finality of 0 if b) attackers control less than ½ of the participants and c) an assumption only that messages from an honest node will not get through, but makes assumptions about how long that takes.

13. What is the goal of the Swirlds Hashgraph Consensus Algorithm?



a. 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 the *exact time* an event took place (and so for each transaction)

b. is for the members of the community to come to a partial *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)

c. is for the members of the community to come to a *consensus* (agreement) on the near *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)

d. 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)

14. To have a consensus what must the algorithm defend against?

a. denial of service attacks only

b. unfair influence over order and timestamps

c. prevention of consensus and conflicting consensus

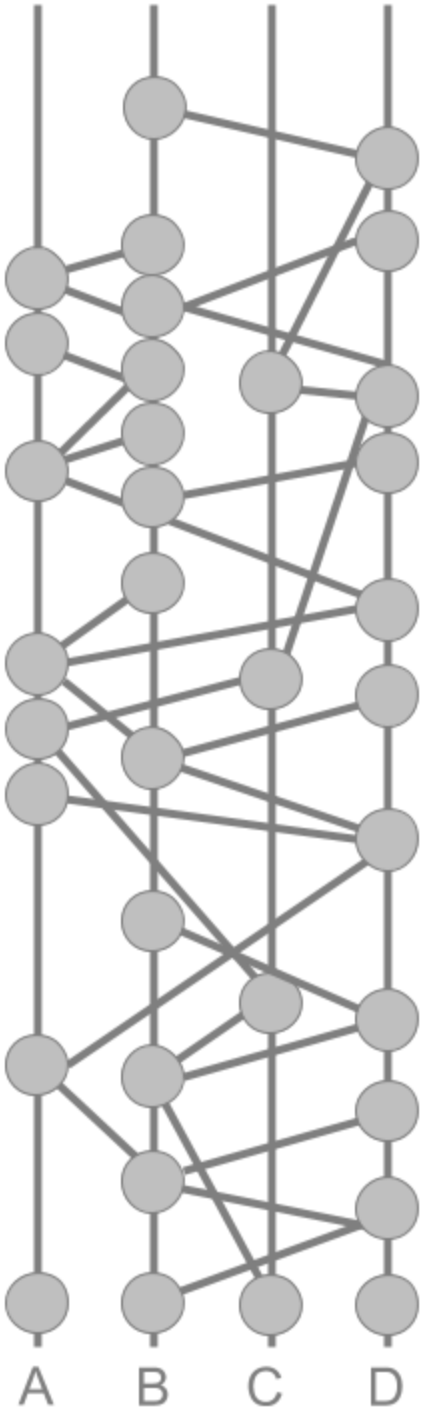
d. both b and c

15. When counting for a supermajority

a. you only see and count the next member and the member at the end of the path

b. you always see and count the beginning and end of the path

c. you only see and count the beginning of the path and not the ancestor at the end of the path



d. you always see and count only the events you go through and do NOT count the beginning and end

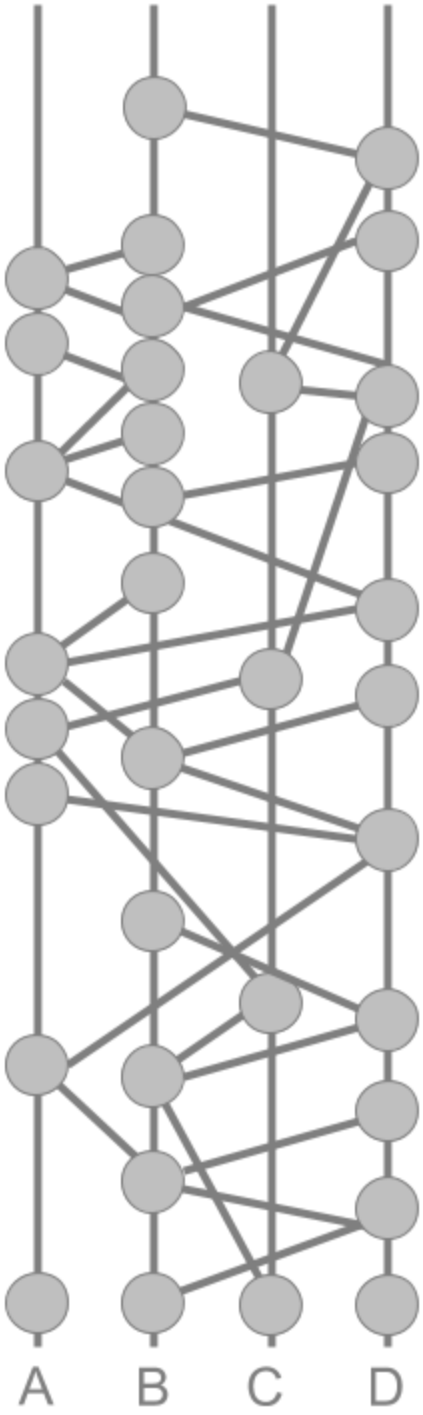
16. What is the best description of a hashgraph

a. an algorithm that records who gossiped to whom, and in what order
b. a data structure that records who gossiped to whom, and in no particular order
c. a data structure that records who gossiped to whom, and in what order
d. a data structure that records who gossiped to whom, and in no particular order

17. Within the context of the consensus algorithm how is fairness defined

a. it should be difficult for a small group of attackers to unfairly influence the order of transactions that is chosen as the consensus.
b. it should be difficult for a large group of attackers to unfairly influence the order of transactions that is chosen as the consensus.
c. it should be difficult for a small group of attackers to unfairly influence transactions
d. it should be difficult for a large group of attackers to unfairly influence transactions.

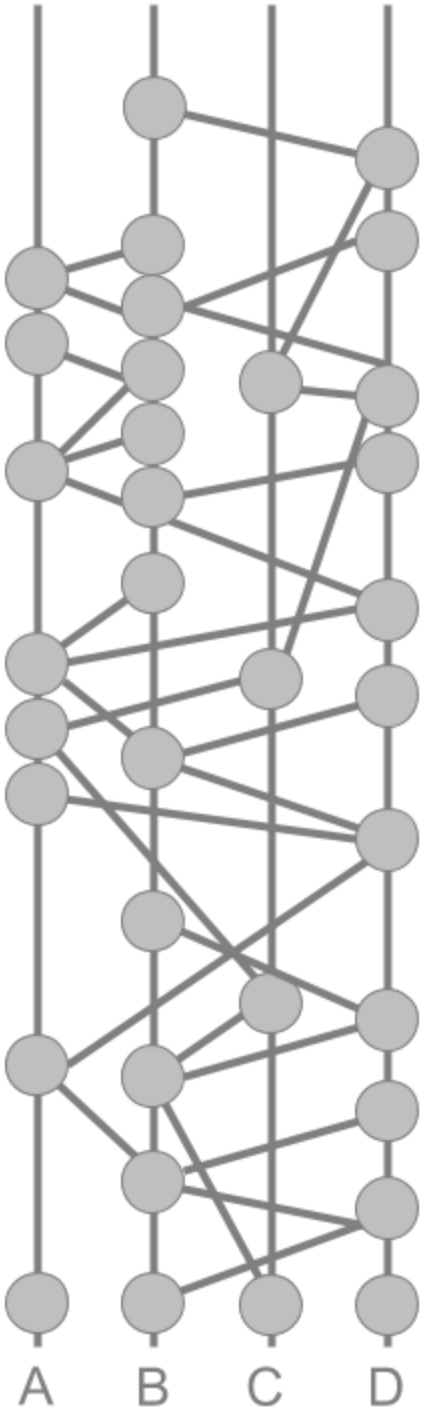
18. Within the context of the SWIRLDS Consensus Algorithm how is gossip defined

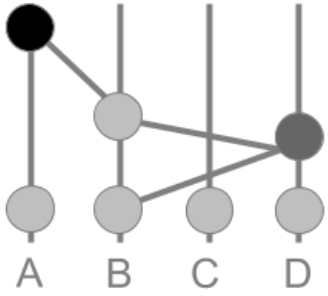


a. information spreads by each member choosing single member at random, and telling them all they know
b. information spreads by each member repeatedly choosing another member sequentially, and telling them all they know
c. information spreads by each member repeatedly choosing another member at random, and telling them all they know
d. information spreads by each member repeatedly choosing another member at random, and telling them about their transaction(s)

19. What best describes gossip about gossip

a. information being gossiped is the gossip itself
b. information being gossiped is the history of the transactions in the hashgraph
c. information being gossiped is the history of the gossip itself
d. information being gossiped is the history of direct communication from one member to another





20. How many events does (A)lice know about at the black event

a. 1 - the event on the vertical line directly below the black event

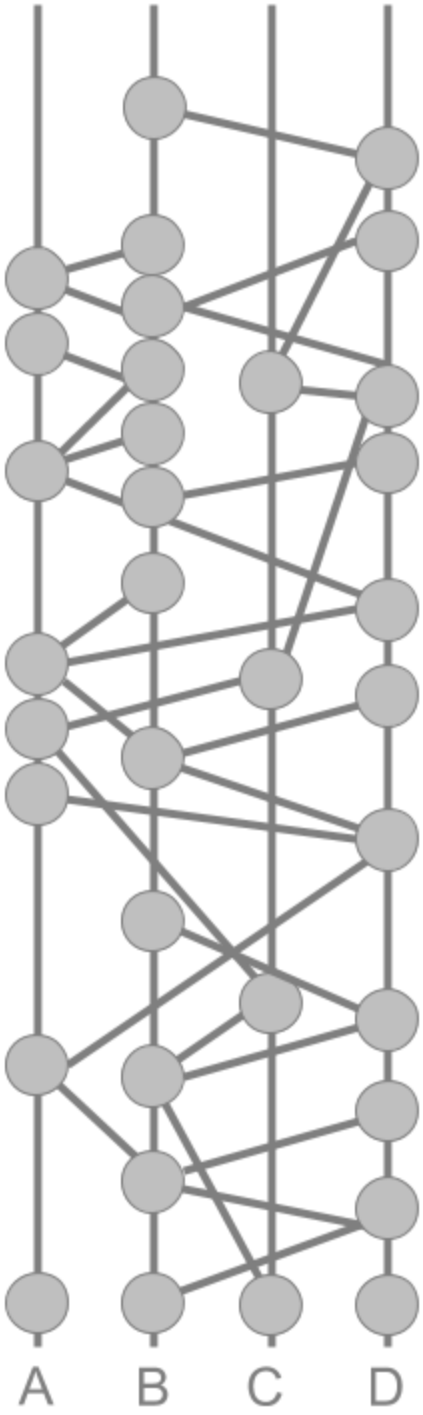
b. 2 - the black event and the event from the other parent

c. 6 - the black event, the event on the vertical line below the black event, the two events from (B)ob and the 2 events from (D)avid.

d. 7 - all the events on the graph

21. What is the best description of virtual voting

a. every member has a copy of the hashgraph, so Alice can calculate what vote Bob *would have* sent her, if they had been running a traditional Byzantine agreement protocol that involved sending votes. So Bob doesn't need to actually [send] her the vote. Every member can reach Byzantine agreement on any number of decisions, without a single vote ever being sent. The



hashgraph alone is sufficient. So zero bandwidth is used, beyond simply gossiping the hashgraph.

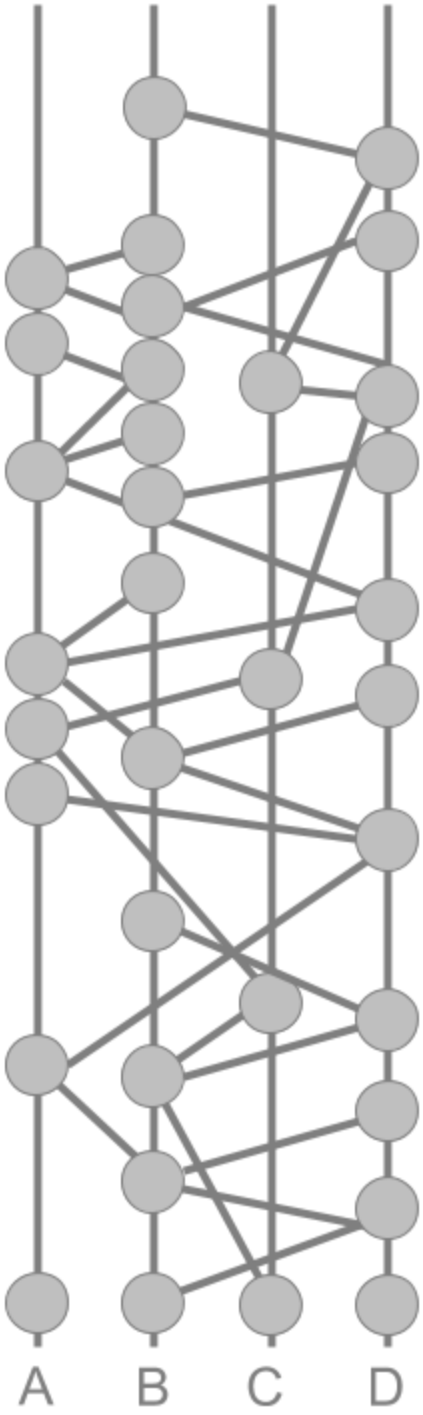
b. every member has a copy of the hashgraph, so Alice can calculate what vote Bob *would have* sent her, if they had been running a traditional Byzantine agreement protocol that involved sending votes. So Bob sends her a single vote for confirmation. Every member can reach Byzantine agreement on any number of decisions, So very little bandwidth is used, beyond simply gossiping the hashgraph.

c. a single member (Alice) has a copy of the hashgraph, so Alice can calculate what vote Bob *would have* sent her, if they had been running a traditional Byzantine agreement protocol that involved sending votes. So Bob sends her a single vote for confirmation. Every member can reach Byzantine agreement on any number of decisions, So very little bandwidth is used, beyond simply gossiping the hashgraph.

d. every member has a copy of the hashgraph, so Alice can calculate what vote Bob *would have* sent her, if they had been running a traditional Byzantine agreement protocol that involved sending votes. So Bob doesn't need to actually [send] her the vote. Every member can reach Byzantine agreement on any number of decisions, without a single vote ever being sent. The hashgraph alone is sufficient. So the bandwidth used is limited to the size of the transaction and the size of the hashgraph

22. Which statement best describes a cryptographic hash

a. a cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum and everytime the data goes through the algorithm the checksum should be different



b. a cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum and everytime the data goes through the algorithm the checksum should the same

c. a cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum and everytime the data goes through the algorithm the checksum should be different and always the same length

d. a cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum and everytime the data goes through the algorithm the checksum should be the same and always the same length as long as the data has not changed

23. What does a circle on a hashgraph represent

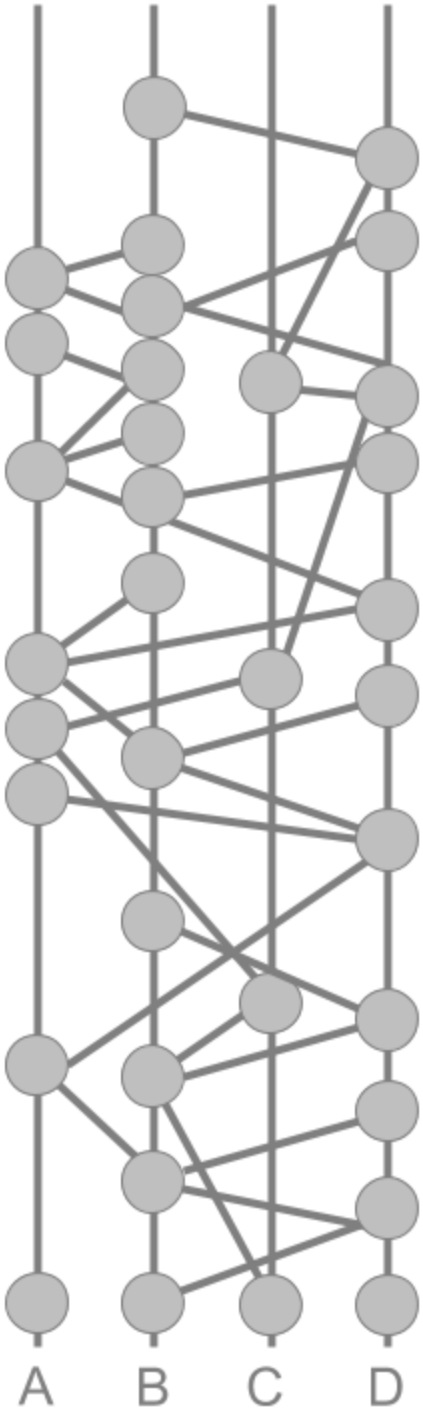
a. Event
b. Member (Node)
c. Vote
d. Timestamp

24. Members on the hashgraph vote

a. True
b. False

25. What does a vertical line on the hashgraph represent?

a. Event
b. Member (Node)



c. Vote
d. Timestamp

26. What is the best description of an honest member

a. An *honest* member tries to sync only once with every other member, creates a valid event after each sync (with hashes of the latest self-parent and other-parent), and never creates two events that are forks with each other.

b. An *honest* member tries to sync infinitely often with every other member, creates a valid event after each sync (with hashes of the latest self-parent and other-parent), and creates two events that are forks with each other.

c. An *honest* member tries to sync only once with every other member, creates a valid event after each sync (with hashes of the latest self-parent and other-parent), and creates two events that are forks with each other.

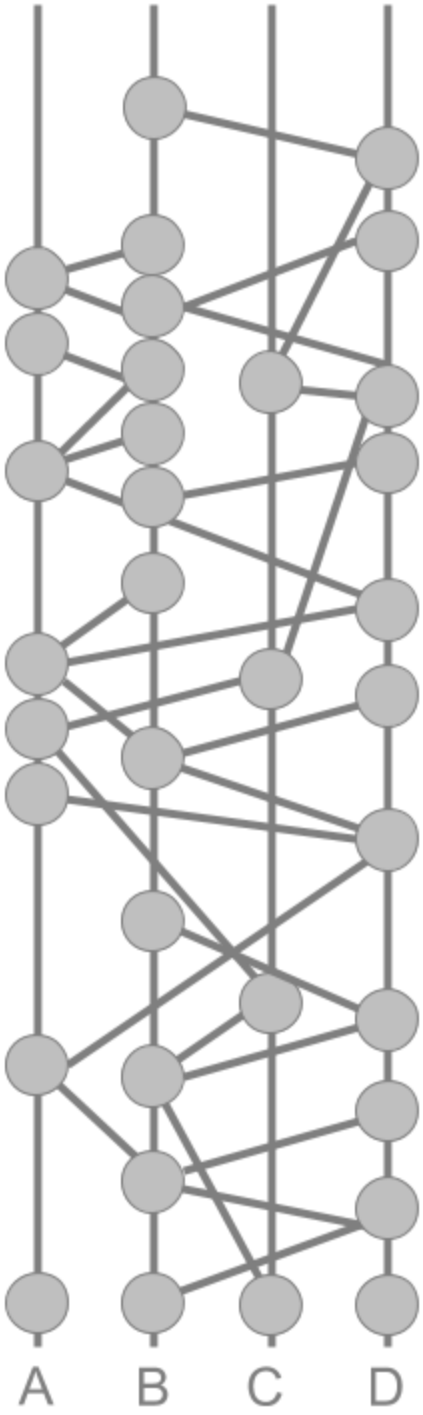
d. An *honest* member tries to sync infinitely often with every other member, creates a valid event after each sync (with hashes of the latest self-parent and other-parent), and never creates two events that are forks with each other.

27. What is a hashgraph event?

a. a data structure containing the two witnesses to the two events below itself (its *witness* and its *famous-witness*)

b. a data structure containing the two hashes of the two events below itself (its *transaction* and its *witness to a transaction*)

c. a data structure containing the two hashes of the two events below itself (its *timestamp* and its vote) and it must contain a transaction



d. a data structure containing the two hashes of the two events below itself (its *self-parent* and its *other-parent*) and it optionally can contain zero or more transactions

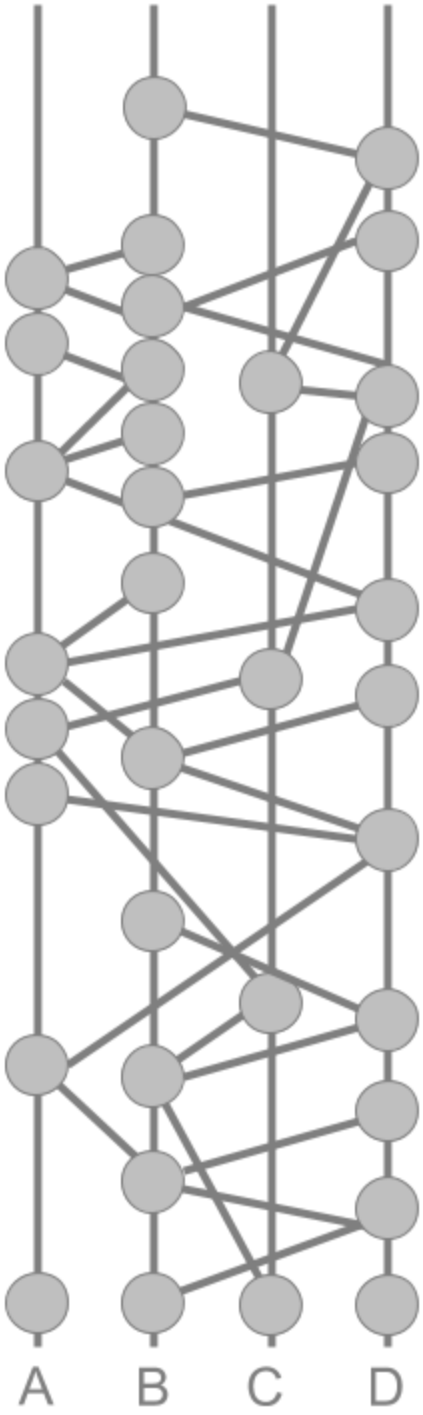
28. What is the best description of a transaction within the context of the hashgraph algorithm

a. any member can create a signed transaction at any time. All members get a copy of it, and the community reaches Byzantine agreement on the order of those transactions.
b. any member can create a transaction at any time. All members get a copy of it, and the community reaches Byzantine agreement on the order of those transactions.
c. any member can create a signed transaction at any time. Most members get a copy of it, and the community reaches Byzantine agreement on the order of those transactions.
d. any member can create a transaction at any time. Most members get a copy of it, and the community reaches Byzantine agreement on the order of those transactions.

29. Draw a hashgraph **event** that displays it's critical attributes from the list below attributes?

ANS: The diagram should be a circle with 3 horizontal lines drawn through it. Between the lines from top to bottom it should have timestamp, transaction, hash, hash with a diagonal line drawn from to the top hash label (other parent) and a vertical line drawn from the bottom hash label (self parent)

30. What is the definition of a "Super Majority" in the Swirlds Hashgraph Consensus Algorithm?



a. any number that is larger than ⅓ of the population

b. any number that is larger than ½ of the population

c. any number that is larger than ¼ of the population

d. any number that is larger than ⅔ of the population

31. Which of the following is the best description of event A3 seeing B2?

a. means that there is at least a single entirely-upward path from A3 to B2

b. means that there is at least a single entirely-downward path from A3 to B2

c. means that there direct vertical path downward between A3 to B2

d. means that there enough different downward paths between A3 to B2 so that together the paths go through a supermajority of the population (members).

32. Which of the following is the best description of event A3 strongly seeing B2

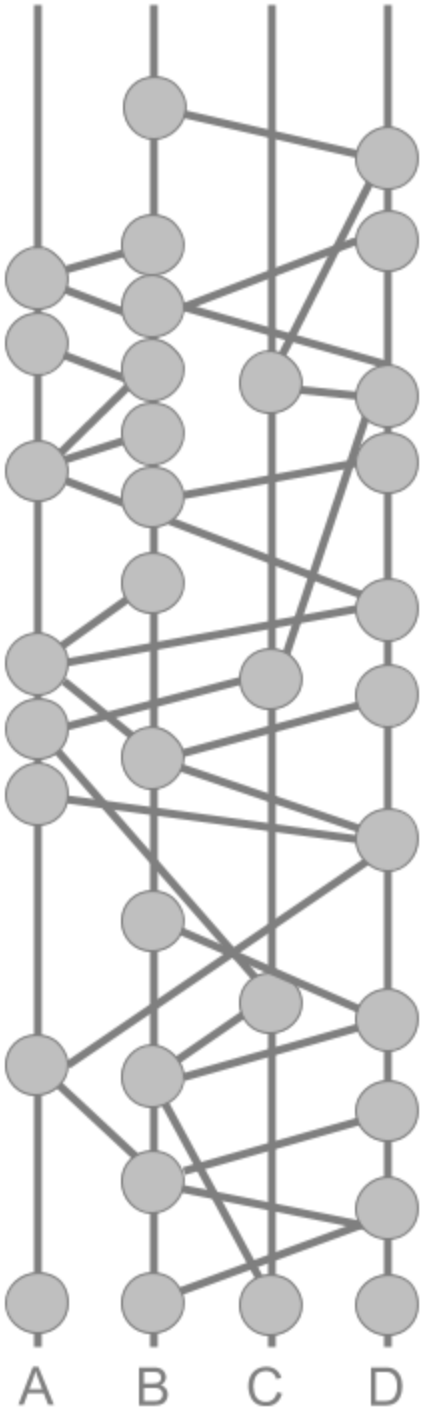
a. means that there is at least a single entirely-upward path from A3 to B2

b. means that there is at least a single entirely-downward path from A3 to B2

c. means that there enough different upward paths between A3 to B2 so that together the paths go through a supermajority of the population (members).

d. means that there a enough different downward paths between A3 to B2 so that together the paths go through a supermajority of the population (members).

33. Choose all the procedures that the concept of strongly seeing is used in and for what reason?



a. the createEvent procedure only and to designate the event as a witness

b. the divideRounds procedure to determine if an event is created in the next round

c. the finalOrder procedure to determine if an event is created in the next round

d. in the decideFame procedure to count the vote of a witness

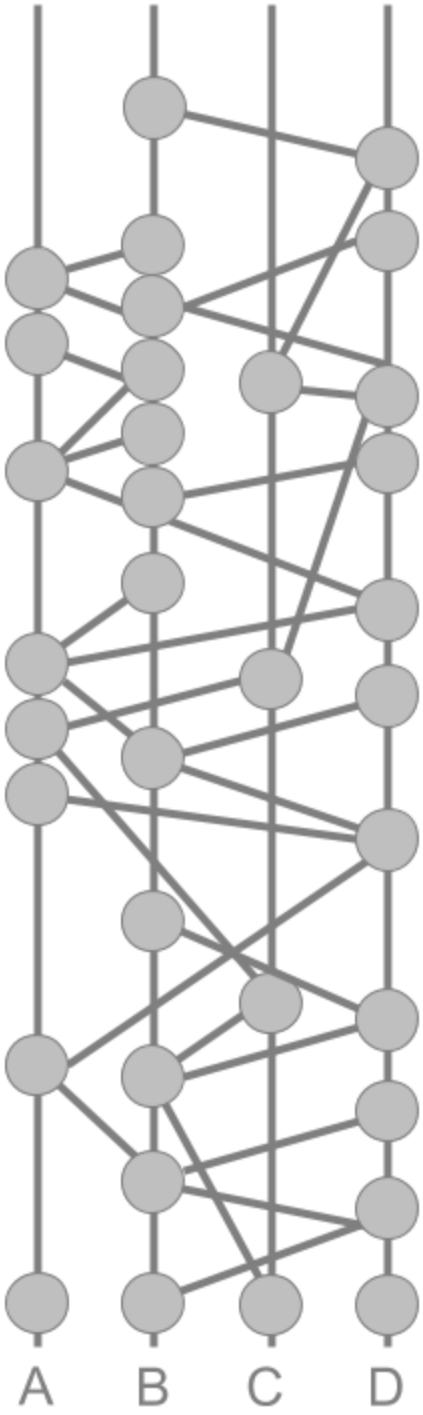
34. What are the 3 procedures contained within the Swirlds Hashgraph Consensus Algorithm?

a. the createEvent, decideFame and finalOrder
b. the divideRounds, findSupermajority and finalOrder
c. the divideRounds, decideFame and finalOrder
d. createEvent, transmitEvent and finalOrder

35. In the divideRounds procedure when would an event increment the +i counter?

a. if it can strongly see a Supermajority (2n/3) witnesses in round r
b. if it can see a Supermajority (2n/3) witnesses in round r
c. if it can see a majority of witnesses in round r
d. if it can strongly see a majority witnesses in round

36. Given the hashgraph below draw a line to designate the separation of events in round 1 and round 2 and identify events A2, B2, C2 and D2.



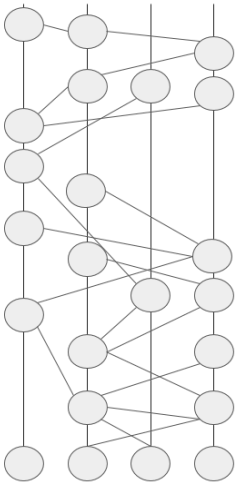


Figure 1 - Round Created

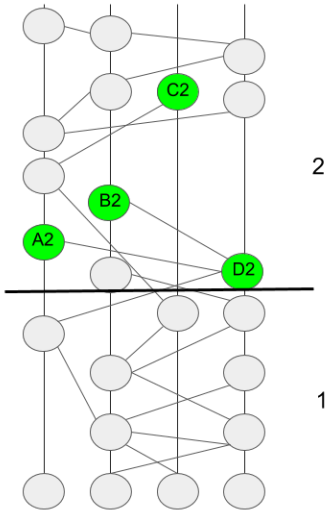


Figure 1 - Round Created

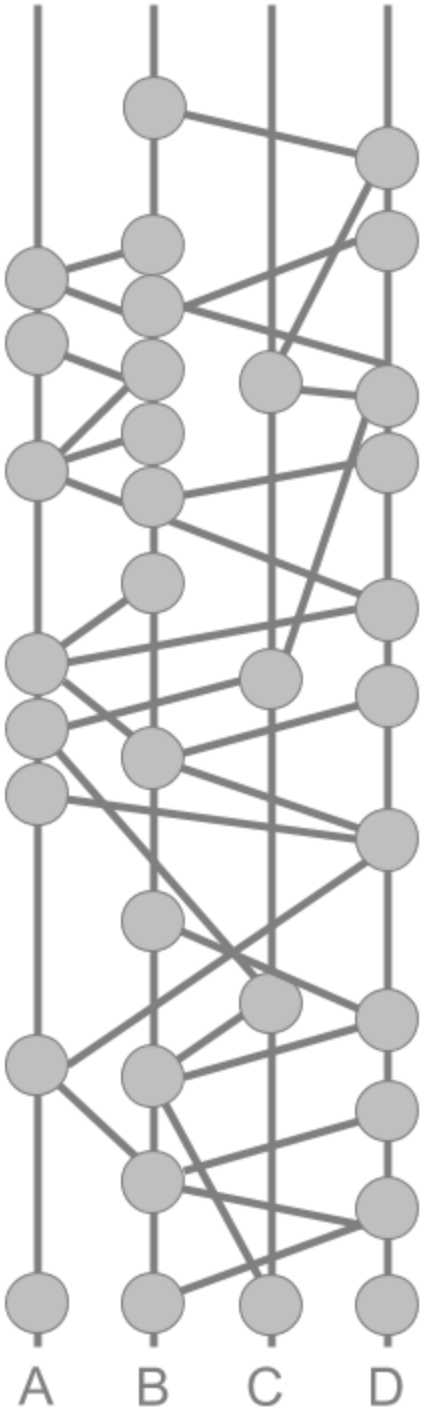
NOTE: The round created number of an event x is defined to be r+i, where r is the maximum number of x (or 1 if it has no parents), and i is defined to be 1 if x can strongly see more than 2n/3 witnesses in round r (or 0 if it can't).

37. Using the graph in the question above events A2, B2, C2 and D2 now can be identified as:

    a. Supermajority
    b. Famous Witnesses
    c. Events
    d. Witnesses

38. Using the graph in the question above the events A2, B2, C2 and D2 were designated as such it best describes what hashgraph algorithm concept

    a. Round received
    b. Round invented
    c. Round created



d. Super Majority

39. Using the graph in the question above why were the events designated to be A2, B2, C2 and D2?

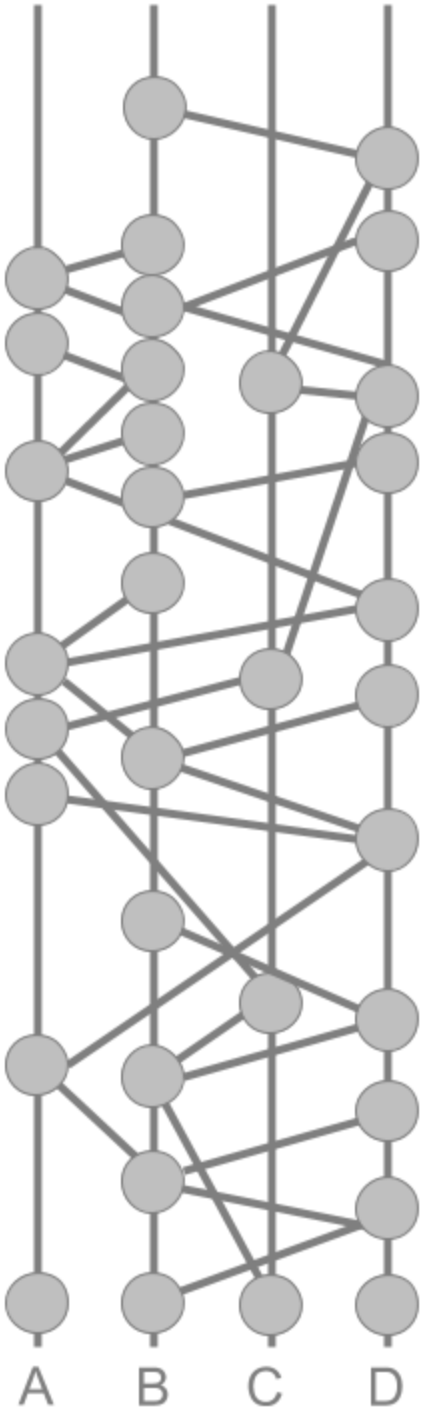
a. because the round created number of an event x is defined to be r+i, where r is the maximum number of x (or 1 if it has no parents), and i is defined to be 1 if x can strongly see more than 2n/3 witnesses in round r (or 0 if it can't)
b. because the round created number of an event x defined to be r+i, where r is the maximum number of x (or 1 if it has no parents), and i is defined to be 1 if x can strongly see more than 2n/3 witnesses in round r (or 1 if it can't)
c. because the round received number of an event x defined to be 2r+i, where r is the maximum number of x (or 2 if it has no parents), and i is defined to be 1 if x can strongly see more than 2n/3 witnesses in round r (or 0 if it can't)
d. because the round created number of an event x defined to be r+i, where r is the maximum number of x (or 1 if it has no parents), and i is defined as the round received

40. For an event to cast a YES famous witness vote for a witness it must be able to

a. strongly see the witness
b. see the witness through a downward path
c. see the witness through sef-parents only
d. strongly see the witness through other parents only

An event x is defined to be r+i, where r is the maximum round number of the parents of x (or 1 if it has no parents), and i is defined to be 1 if x can strongly see more than 2n/3 witnesses in round r (or 0 if it can't)

41. Using the hashgraph in the left hand column draw a line between the vertices to designate Rounds 1, 2, 3, and 4



42. Using the hashgraph in the left hand column identify witnesses A1, B1, C1 and D1

43. Using the hashgraph in the left hand column identify witnesses A2, B2, C2 and D2

44. Using the hashgraph in the left hand column identify witnesses A3, B3, C3, D3

45. Using the hashgraph in the left hand column identify all the witnesses in round 4

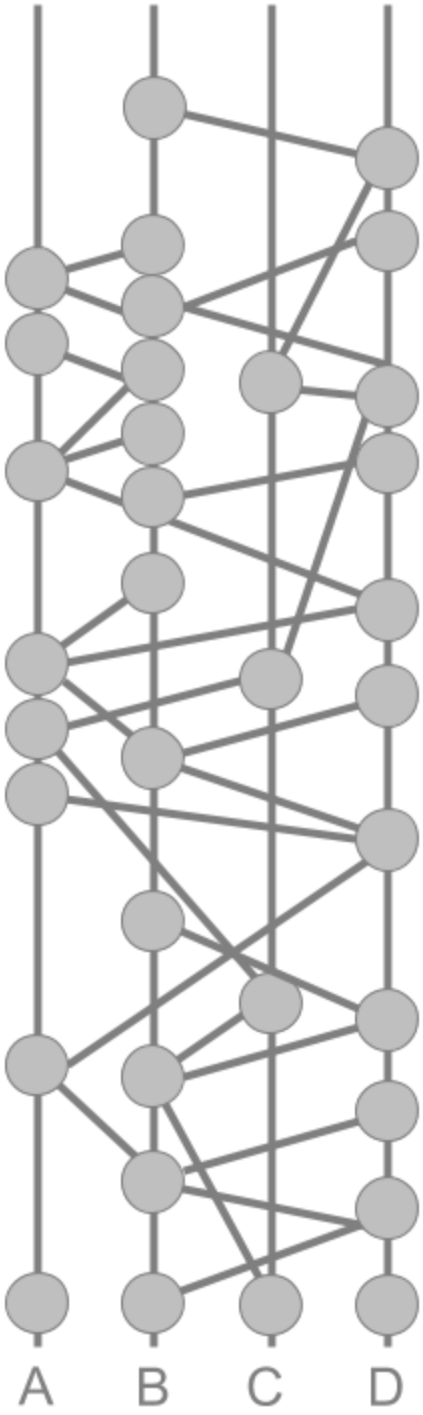
46. The concept of virtual voting includes which of the following critical attributes
    a. every member sends every member a copy of their hashgraph
    b. every member has a copy of the hashgraph
    c. each witness will send their vote to another witness so it can be counted
    d. a witness can pretend to be another witness and calculate what pretended witness would vote because each member has a copy of the hashgraph
    e. every member can reach Byzantine agreement on any number of decisions, without a single vote being sent
    f. zero bandwidth is used, beyond simply gossiping the hashgraph
    g. bandwidth used is only the amount needed to send a single witness vote

47. Using the hashgraph in the left hand column identify all the witnesses of each round

48. Using the hashgraph in the left hand column hold a vote and determine how A3, B3, C3 and D3 cast their vote for B2's fame

A3	B3	C3	D3
Y	Y	Y	Y

49. Using the hashgraph in the left hand column to identify if B4 "strongly sees" each witness and record a vote for each witness B4 "strongly sees"



A3	B3	C3	D3
Strongly Sees?			
Y	Y	Y	Y
Vote Collected			
Y	Y	Y	Y

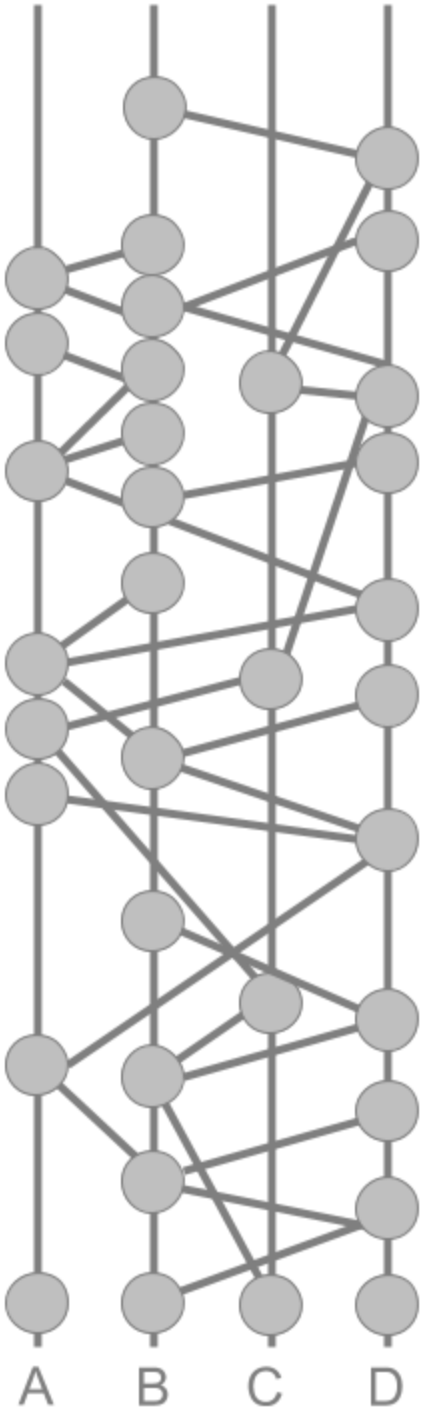
B2 is famous True or False

50. Using the hashgraph in the left hand column identify all the witnesses of each round

51. Using the hashgraph in the left hand column hold a vote and determine how A3, B3, C3 and D3 cast their vote for A2's fame

A3	B3	C3	D3
Y	Y	Y	Y

52. Using the hashgraph in the left hand column to identify if B4 "strongly sees" each witness and record a vote for each witness B4 "strongly sees"



A3	B3	C3	D3
Strongly Sees?			
Y	Y	Y	Y
Vote Collected			
Y	Y	Y	Y

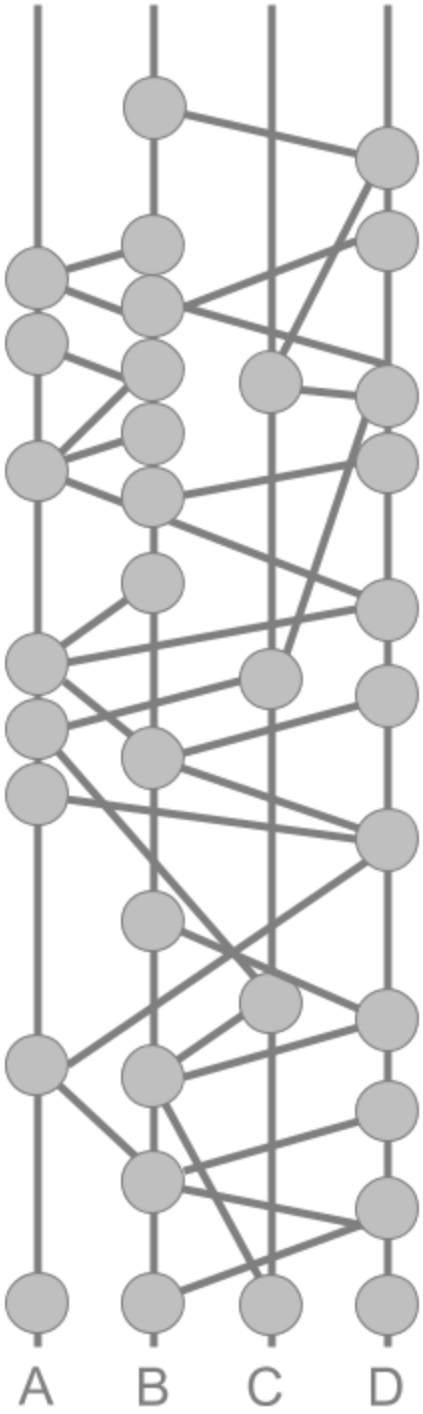
A2 is famous True or False

53. Using the hashgraph in the left hand column identify all the witnesses of each round

54. Using the hashgraph in the left hand column hold a vote and determine how A3, B3, C3 and D3 cast their vote for C2's fame

A3	B3	C3	D3
N	N	Y	N

55. Using the hashgraph in the left hand column to identify if B4 "strongly sees" each witness and record a vote for each witness B4 "strongly sees"



A3	B3	C3	D3
Strongly Sees?			
Y	Y	Y	Y
Vote Collected			
N	N	Y	N

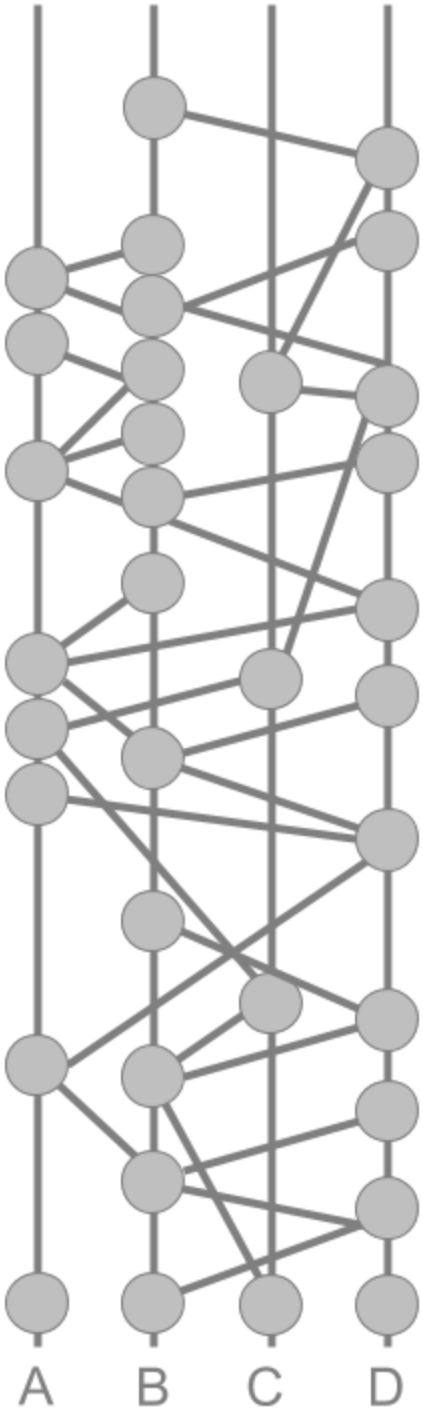
C2 is famous True or False

56. Using the hashgraph in the left hand column identify all the witnesses of each round

57. Using the hashgraph in the left hand column hold a vote and determine how A3, B3, C3 and D3 cast their vote for D2's fame

A3	B3	C3	D3
Y	Y	Y	Y

58. Using the hashgraph in the left hand column to identify if B4 "strongly sees" each witness and record a vote for each witness B4 "strongly sees"



A3	B3	C3	D3
Strongly Sees?			
Y	Y	Y	Y
Vote Collected			
Y	Y	Y	Y

D2 is famous True or False

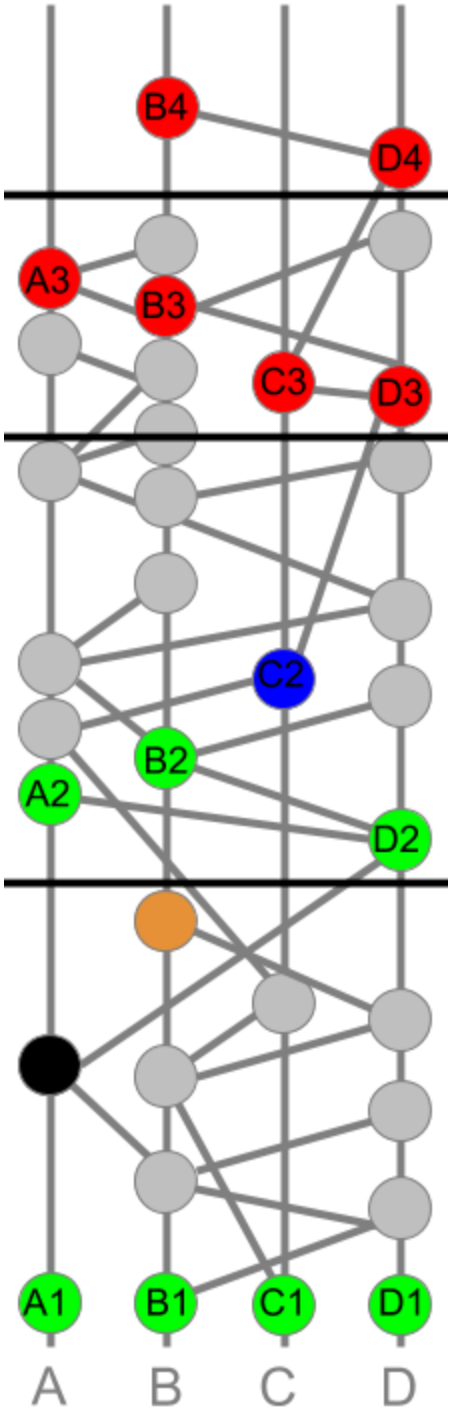
59. Questions 40 and 41 are a demonstration of which hashgraph concept?

    a. Transaction counting of votes sent to each member
    b. Vote counting of votes sent toe each member
    c. Virtual voting of votes without any votes being sent
    d. Gossip about gossip

60. Every person taking this quiz, counting the same votes from the same hashgraph using the SWIRLDS Consensus Algorithm are examples of which of the following concepts

    a. Fairness
    b. Consensus
    c. Byzantine Fault Tolerance of the Algorithm
    d. All of the above

61. What is the best definition of the round received number (or round received) of an event?



a. the first round where all unique witnesses are descendants of x (can see x)
b. the first round where all unique witnesses are ancestors of x (can see x)
c. the first round where all unique famous witnesses are descendants of x (can see x)
d. the first round where all unique famous witnesses are descendants of x (can see x)

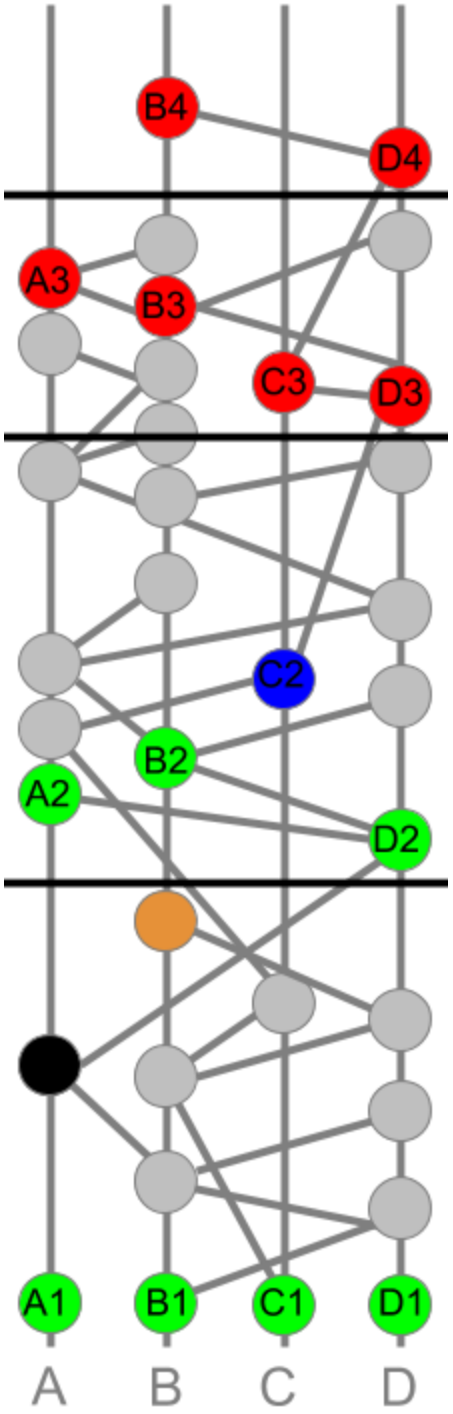
62. Using the hashgraph to the left how many events have a round received number of 1?

a. 4
b. 6
c. 8
d. 10
e. 12

63. Using the table below what is the consensus timestamp of the black event?

a. September 16 2019, 7:00:00 PM
b. September 16 2019, 7:00:02 PM
c. September 16 2019, 7:00:05 PM
d. September 16 2019, 7:00:04 PM

Event	Timestamp
A1	September 16 2019, 7:00:00 PM
B1	September 16 2019, 7:00:00 PM
Black Event	September 16 2019, 7:00:01 PM
A2	September 16 2019, 7:00:04 PM
B2	September 16 2019, 7:00:05 PM



D2	September 16 2019, 7:00:02 PM

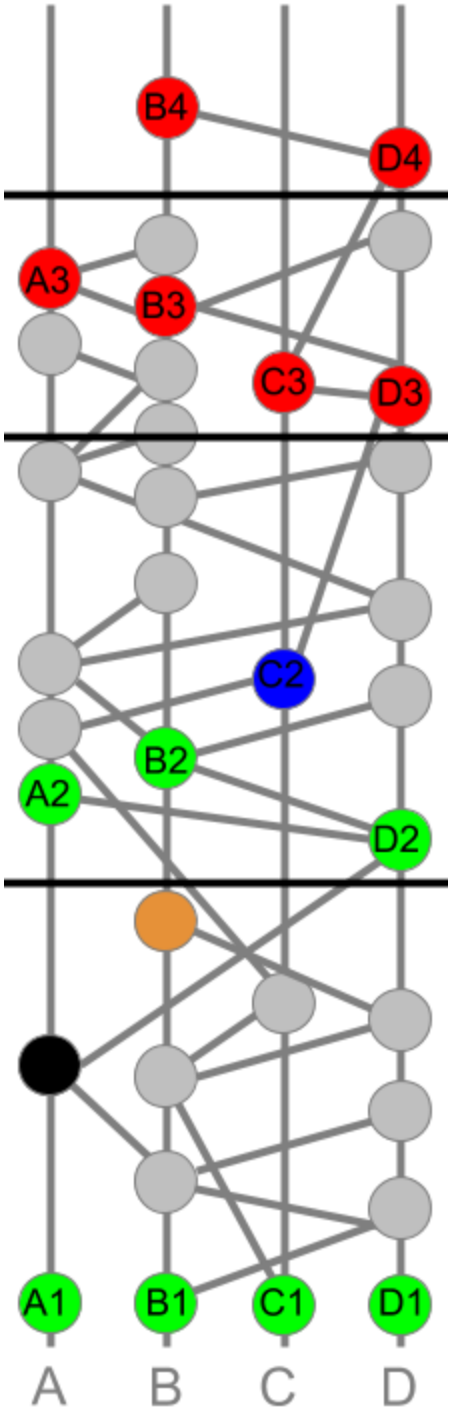
64. Using the table below what is the consensus timestamp of the orange event?

a. September 16 2019, 7:00:00 PM
b. September 16 2019, 7:00:01 PM
c. September 16 2019, 7:00:01 PM
d. Cannot be determined because it cannot be seen by all the famous witnesses

Event	Timestamp
A1	September 16 2019, 7:00:00 PM
B1	September 16 2019, 7:00:00 PM
Orange Event	September 16 2019, 7:00:02 PM
A2	September 16 2019, 7:00:04 PM
B2	September 16 2019, 7:00:05 PM
D2	September 16 2019, 7:00:03 PM

65. What is the best description of the difference between Round Created and Round Received?

a. Round Created is used for virtual voting and Round Received is used to determine the consensus timestamp

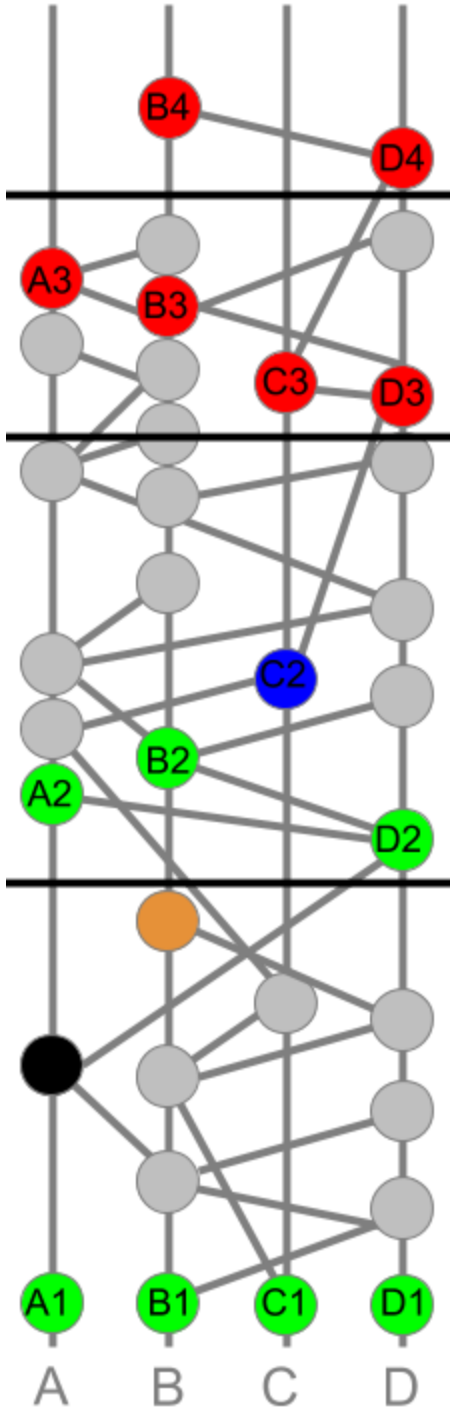


b. Round Created is used to determine the consensus timestamp and Round Received is used for virtual voting
c. Round Created is used to determine if the event is strongly seen and Round Received is used to determine if the event is seen
d. Round Created is used to determine if the event is seen and Round Received is used to determine if the event is strongly seen

66. What is the best description of the difference between an event timestamp and a consensus timestamp

a. An event timestamp is the time value within the event data structure when the famous witnesses sign the transaction and the consensus timestamp is when the event was seen to occur by a witness
b. An event timestamp is the time value within the event data structure when the famous witnesses sign the transaction and the consensus timestamp is when the event was seen to occur by a witness
c. An event timestamp is the time value within the event data structure of when the event occurred and the consensus timestamp is the median of the earliest timestamps collected by famous witnesses
d. they are both the same when a famous witness sees the next event

67. Name 3 use cases or scenarios where the consensus algorithm could be used to improve fairness, security or reliability of reaching a consensus



END OF EXAM
