SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 11:

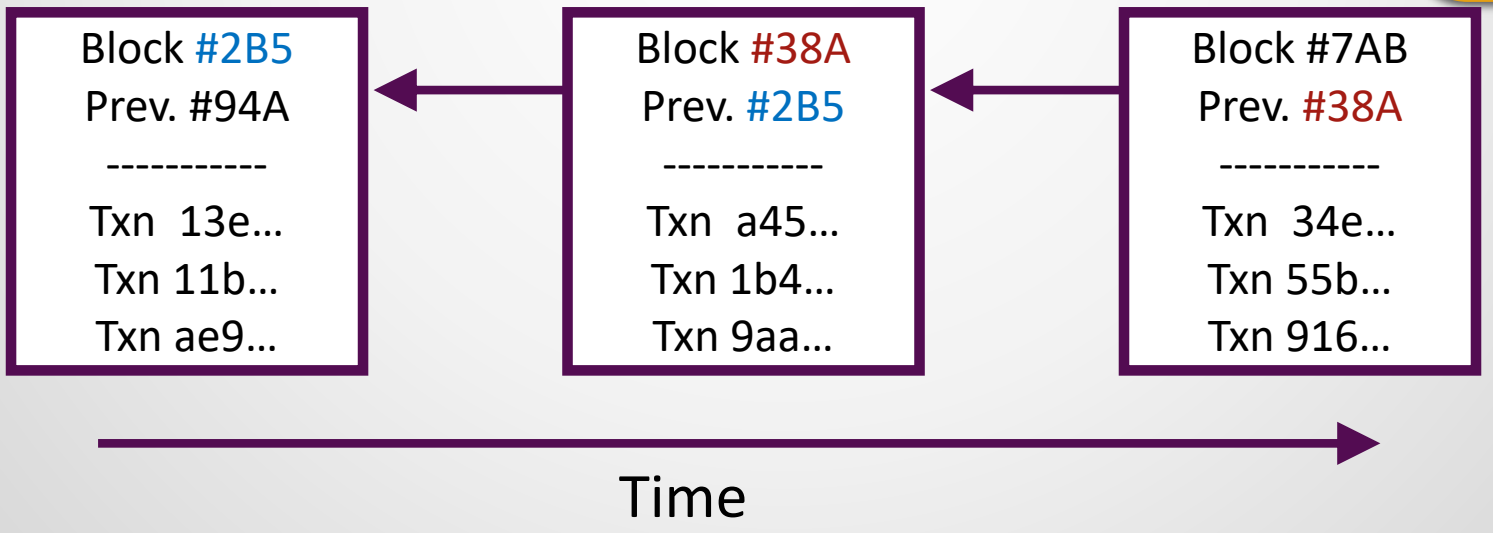
DAG-based DLTs

Module 1 – IOTA

Blockchain Technology

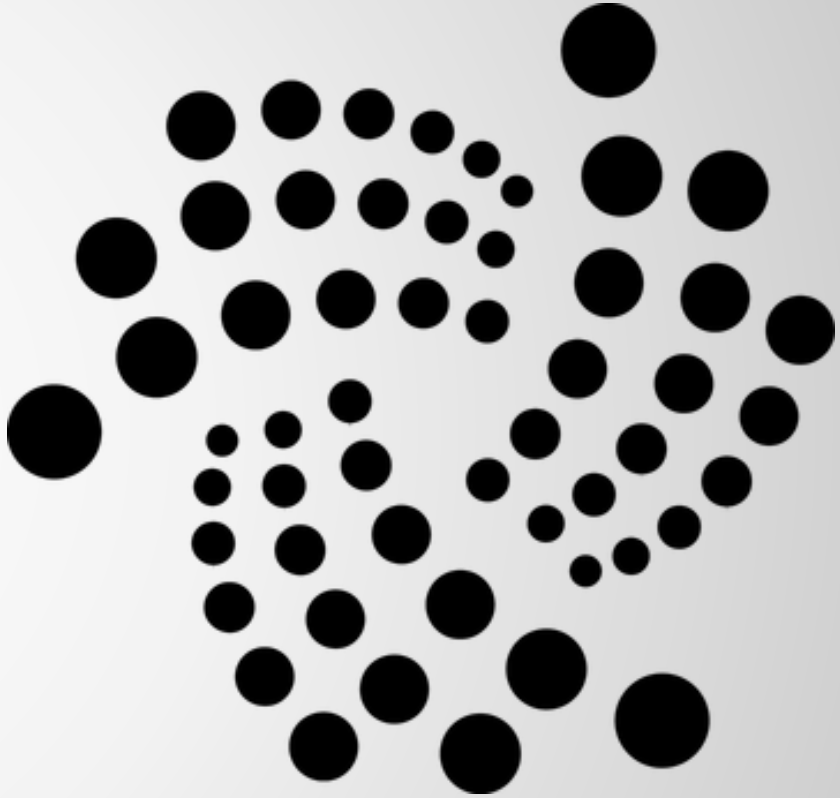
- We saw how blockchain can help us put transactions in order and create a consensus on that order.
  - But blockchain is not the only technology that can do so.

Each block is a set of transactions plus a reference to chain it to the previous block.



IOTA

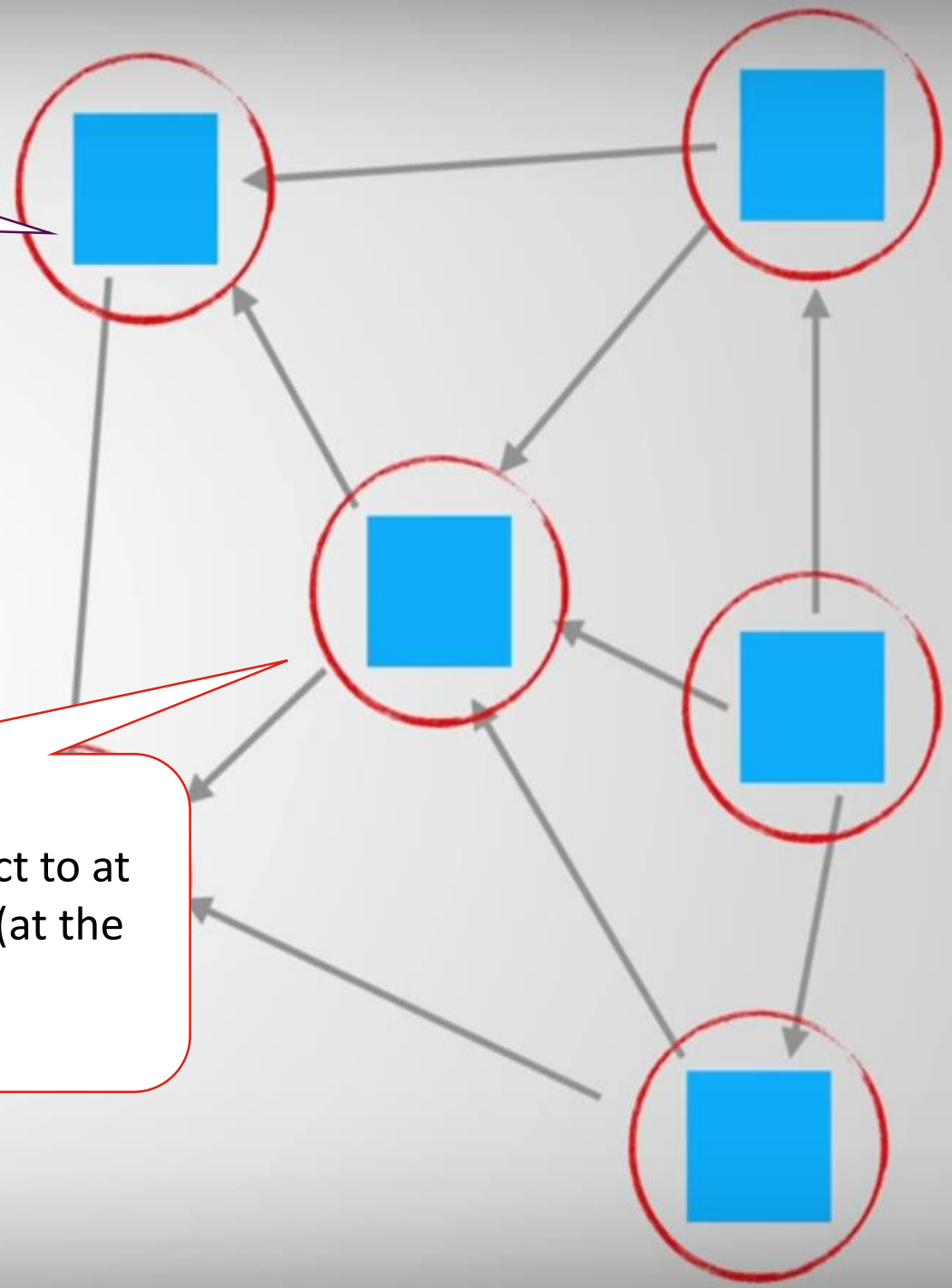
- Blockchains are not always fast.
  - They are struggling with their low TPS.
  - Bitcoin: 7 Trans./s
- IOTA is not based on chained blocks.
  - It uses Directed Acyclic Graph (DAG) or Tangle.

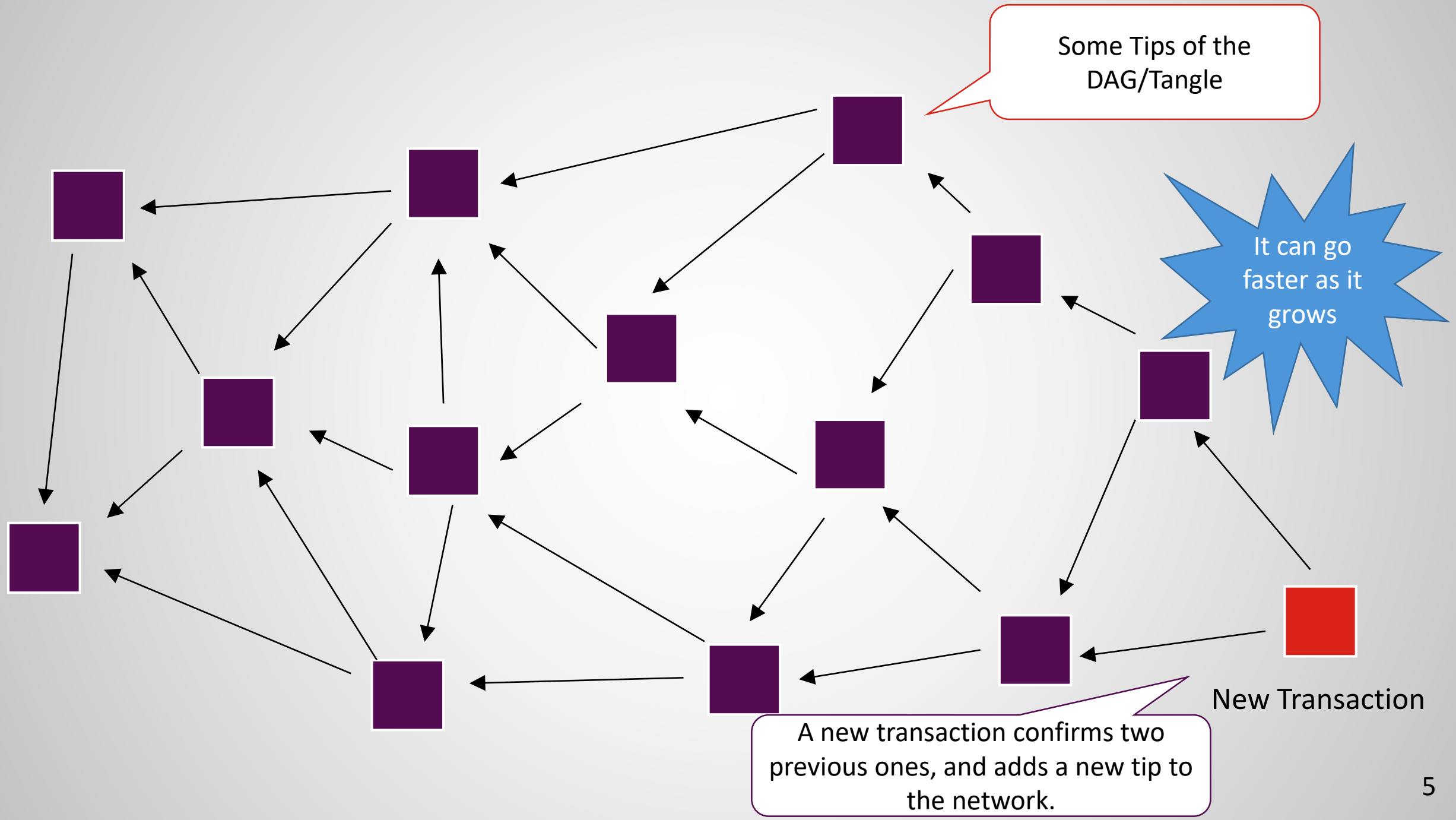


Site / transaction

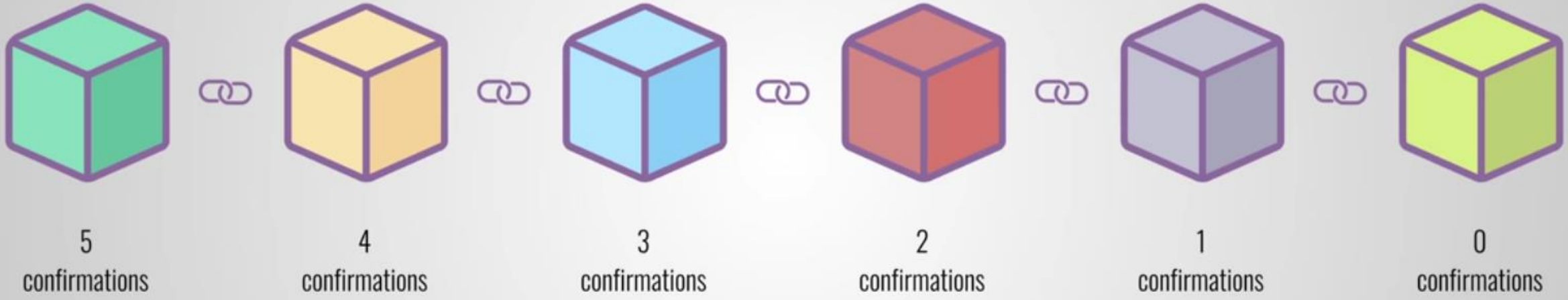
Each Site (node) represents a transaction (with every details of it, e.g. sender, receiver, money amount). It can even be a message.

Each transaction must connect to at least two other transactions (at the edge of the graph).




Some Tips of the DAG/Tangle
It can go faster as it grows
New Transaction
A new transaction confirms two previous ones, and adds a new tip to the network.

How a Blockchain Confirms Transactions



Each Transaction has a cumulative weight.

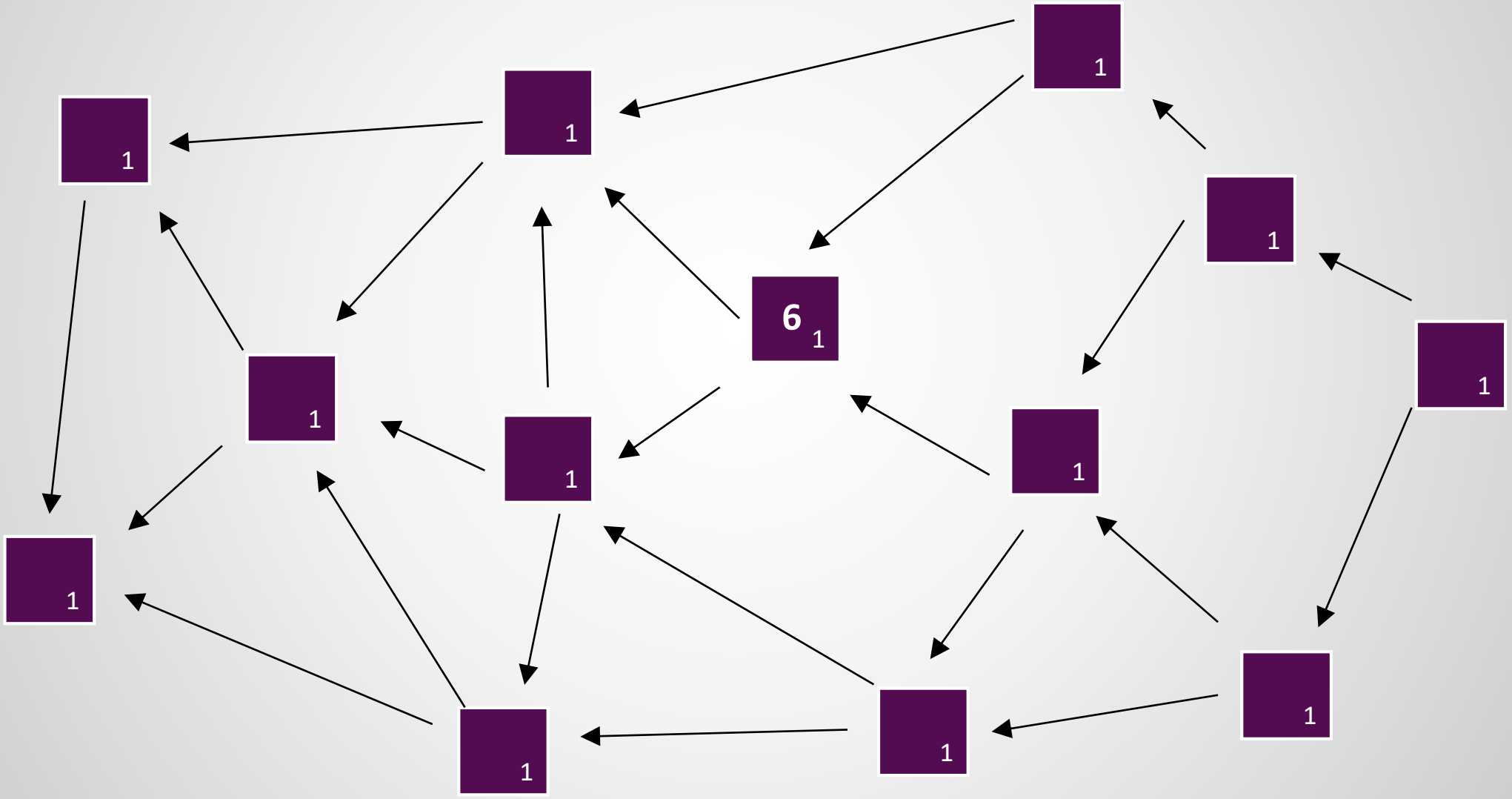
Sum of all connected Transactions

Site / transaction

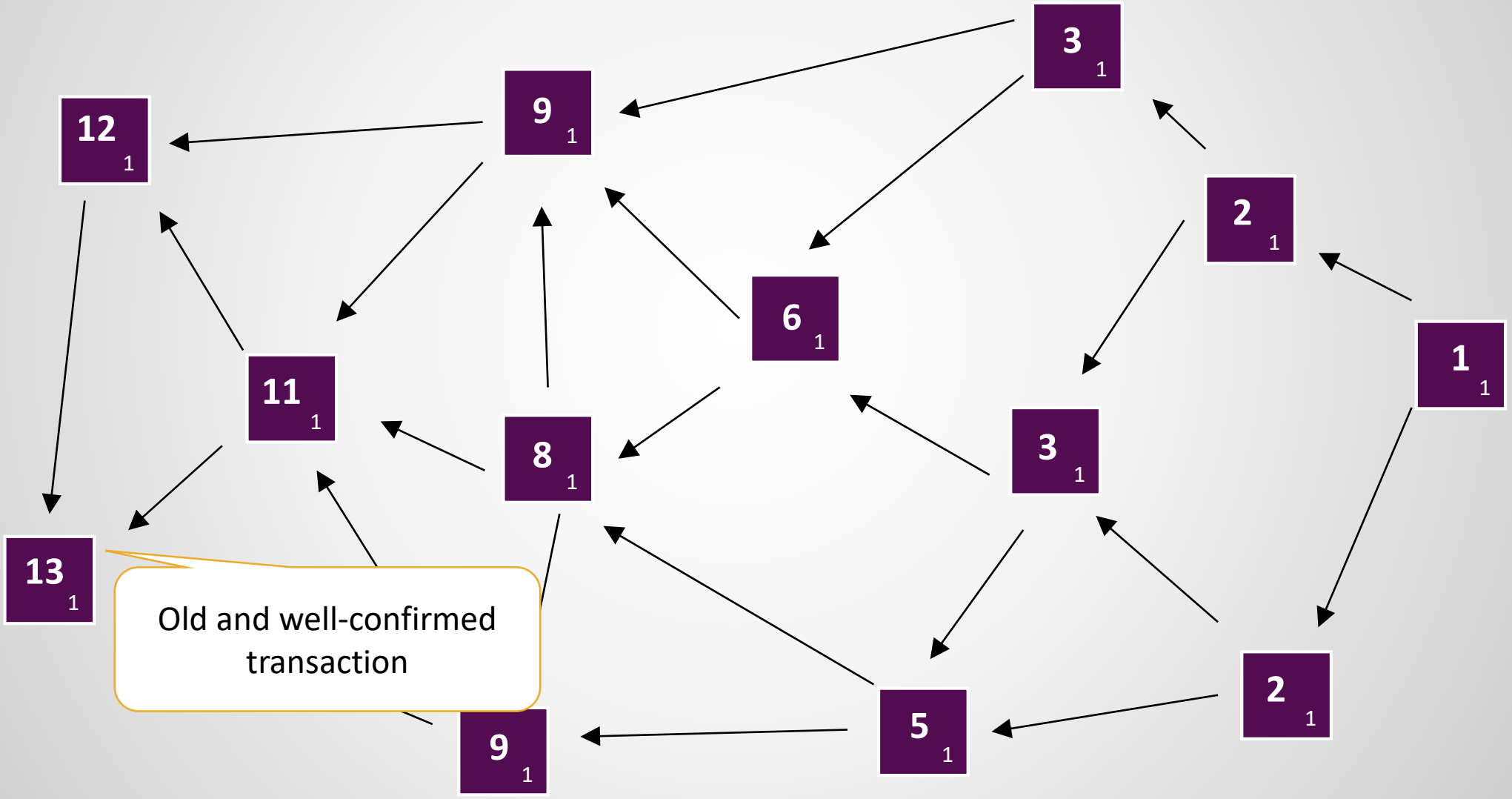
Each Transaction has a weight

It signifies the amount of work the node has done for this transaction (PoW).

How IOTA Confirms Transactions



How IOTA Confirms Transactions



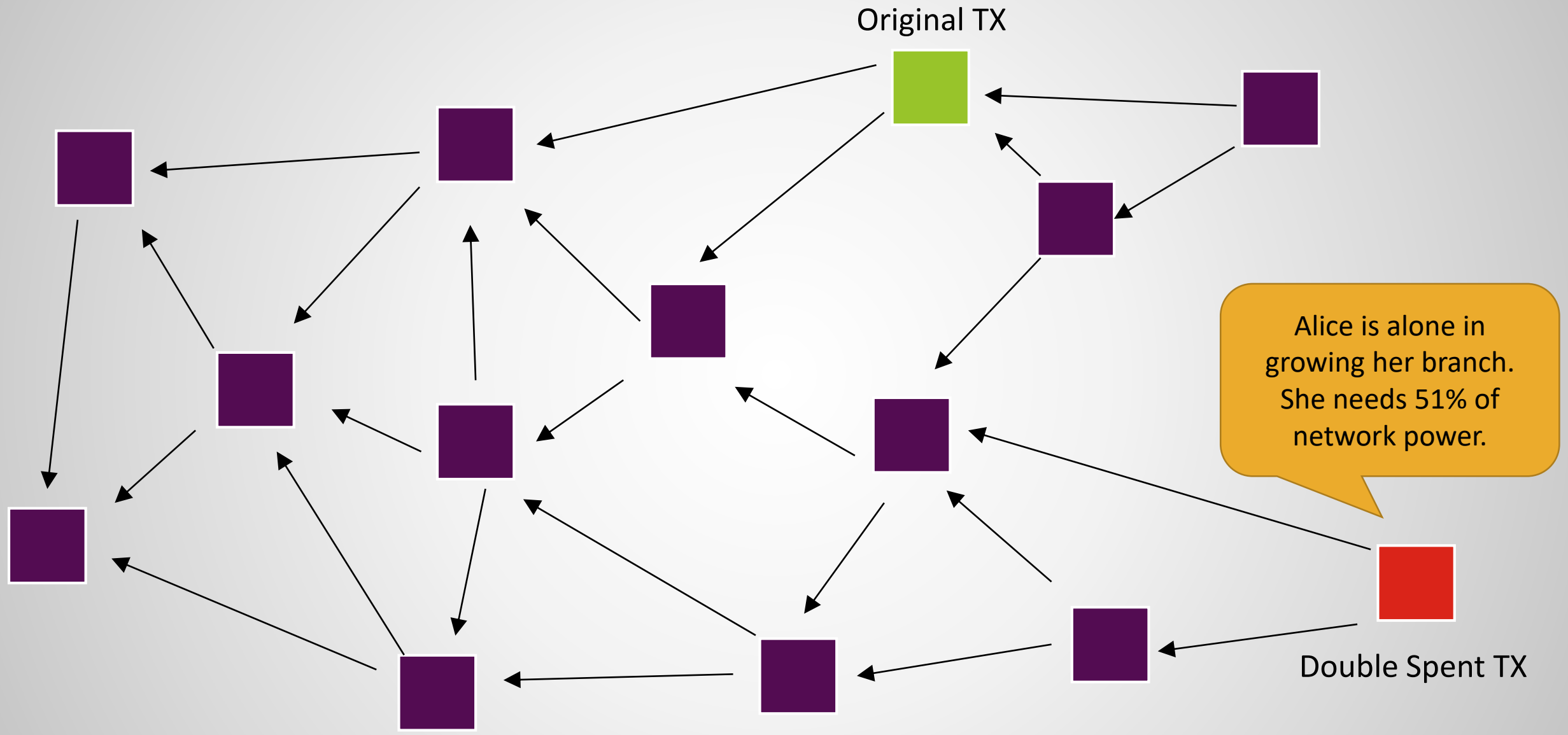
Double Spending on DAGs

- Let's say Alice pays Bob at 12:00. It goes on the tangle. Bob waits for a while and ships the item.

- At 14:00, Alice issues a transaction that transfers the same money to her own account.
  - She picks 2 sites/nodes and attaches her new transaction to them.

- Others are constantly creating TXs and connecting them to the DAG. By the time Alice issues her double-spending TX, some have already connected their sites to the previous TX and its cumulative weight has grown.

- Others find the new transaction and the previous ones conflicting. So they will not connect the two edges of their TXs to the new double-spending TX.
  - In the event a site confirms the 2nd transaction by one leg, it will be left abandoned, because others know that if they connect to this branch, no one will connect to them (because that means indirectly confirming the double-spending TX). So their transactions will be left abandoned and will not gain weight and confirmed.


Original TX
Alice is alone in growing her branch. She needs 51% of network power.
Double Spent TX

Some IOTA Features

Fast Transactions

Almost no Speed Limit.

Proof of Work-based

Nodes do the PoW work. This stops spam and Sybil attacks. A threat similar to 51% attack exists.

Scalability

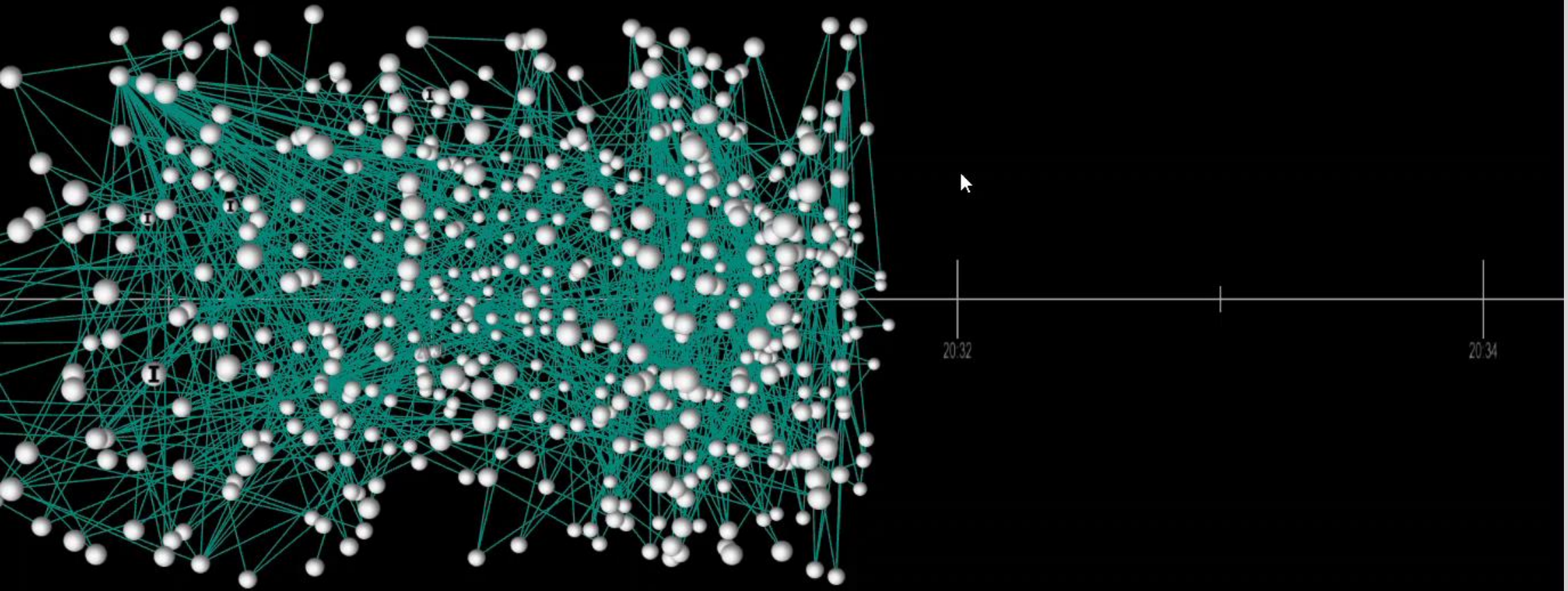
It grows bigger if more transactions are required.

No Mining

All IOTAs have been pre-generated. Transactions do not have commissions.

Quantum Computer Resistant?!

IOTA Live Transactions



What Comes Next …

- We learned about a different architecture for DLTs which is based on DAGs.
- We saw IOTA as an example of DAG-based DLTs.
- Next we introduce Hashgraph, a different member of the DAG-based distributed ledgers.

See you in the next module …