Tangle/IOTA

Using a DAG instead of a blockchain

Arian Baloochestani

IOTA

Micropayments

General idea

- Small payments
- Day to day payments
- IOT devices
    - M2M micropayments

Micropayments

IOT

- Scenario: **EVM Smart Charging**
  - Decentralised Peer-to-Peer energy trading
  - A network of electric vehicle charging stations located throughout a city
    - Equipped with smart meters and sensors
      - Monitor energy consumption
      - Authenticate EVs
  - Electric vehicles can autonomously connect to these charging stations for recharging
  - The entire process is automated
  - Example: Trondheim!

Micropayments

Problems

- **Problem:** Block delay
  - Solution:
    - Committee-based blockchains

Micropayments

Problems

- **Problem:** Forks
  - Discarded forks are wasted energy
  - Maybe 2 blocks are not conflicting
    - Same parent
  - Solution:
    - Change blockchain structure
      - GHOST

Micropayments

Problems

- **Problem:** Scalability
  - More users —> more transactions
  - More miners —> harder to get consensus —> more forks
  - Solution:
    - Select few miners to run consensus
      - Committee-based blockchains

Micropayments

Problems

- **Problem:** Transaction fees
  - Miners need incentives
  - Solution:
    - Use none-economical incentives
      - Tit-for-tat
        - Removes the mining process!

IOTA

Introduction

- An open-source distributed ledger technology
- Designed for IoT devices
- Scalable
- Efficient
- Fee-less
  - No miners
- It has a currency: MIOTA

IOTA

Introduction

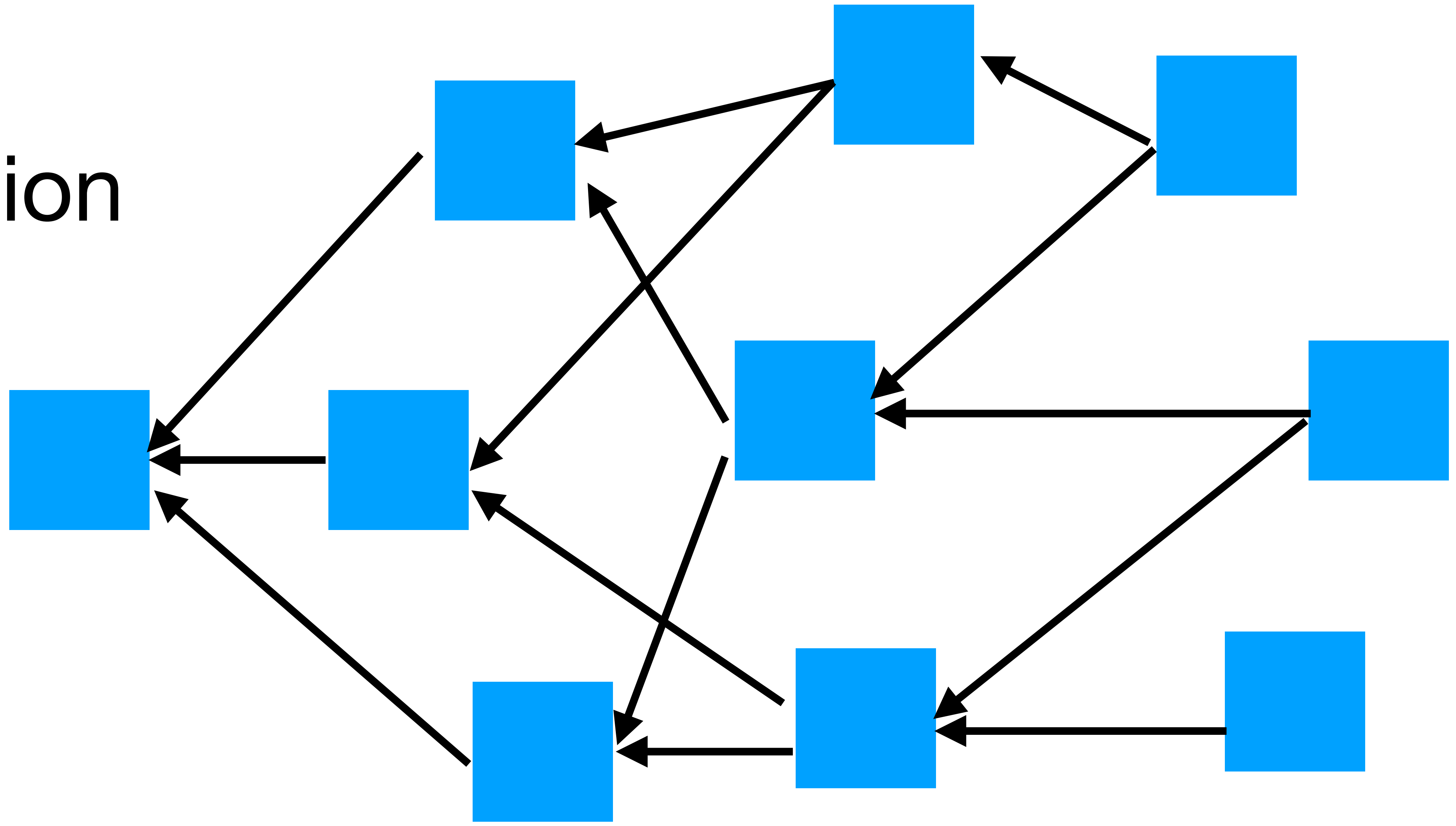
- No fees and economical incentives —> no miners
- “Help others, and others will help you”
  - “If you don’t help others, others will not help you”
  - Collaborative system
    - All users are miners
- No miners —> no blocks
- No blocks + “Help others” —> DAG —> Tangle

Tangle

Tangle

DAG

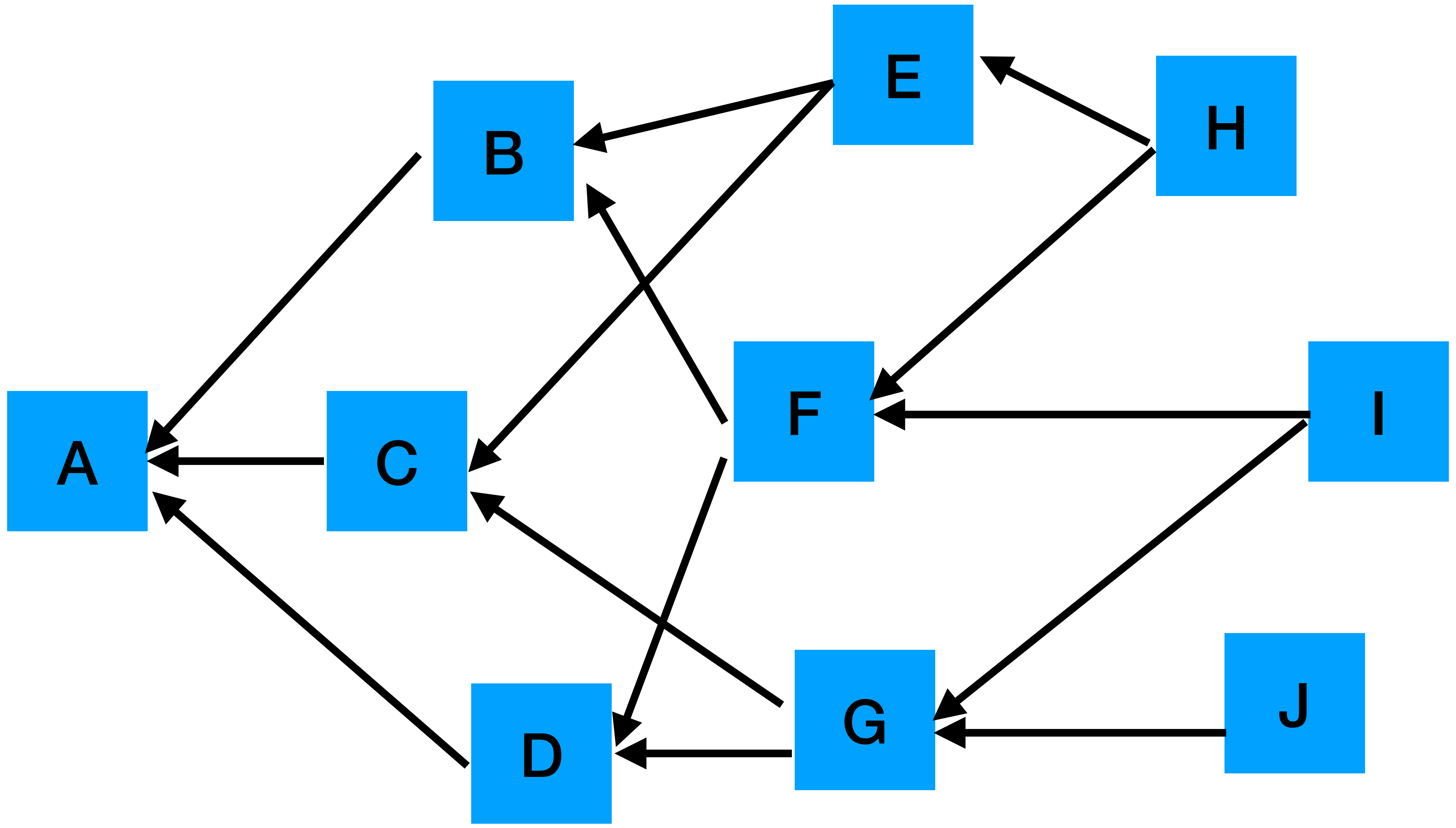
- Directed Acyclic Graph
  - Nodes connected with edges
  - Each edge has a one-way direction
  - No loop



Tangle

Nodes and edges

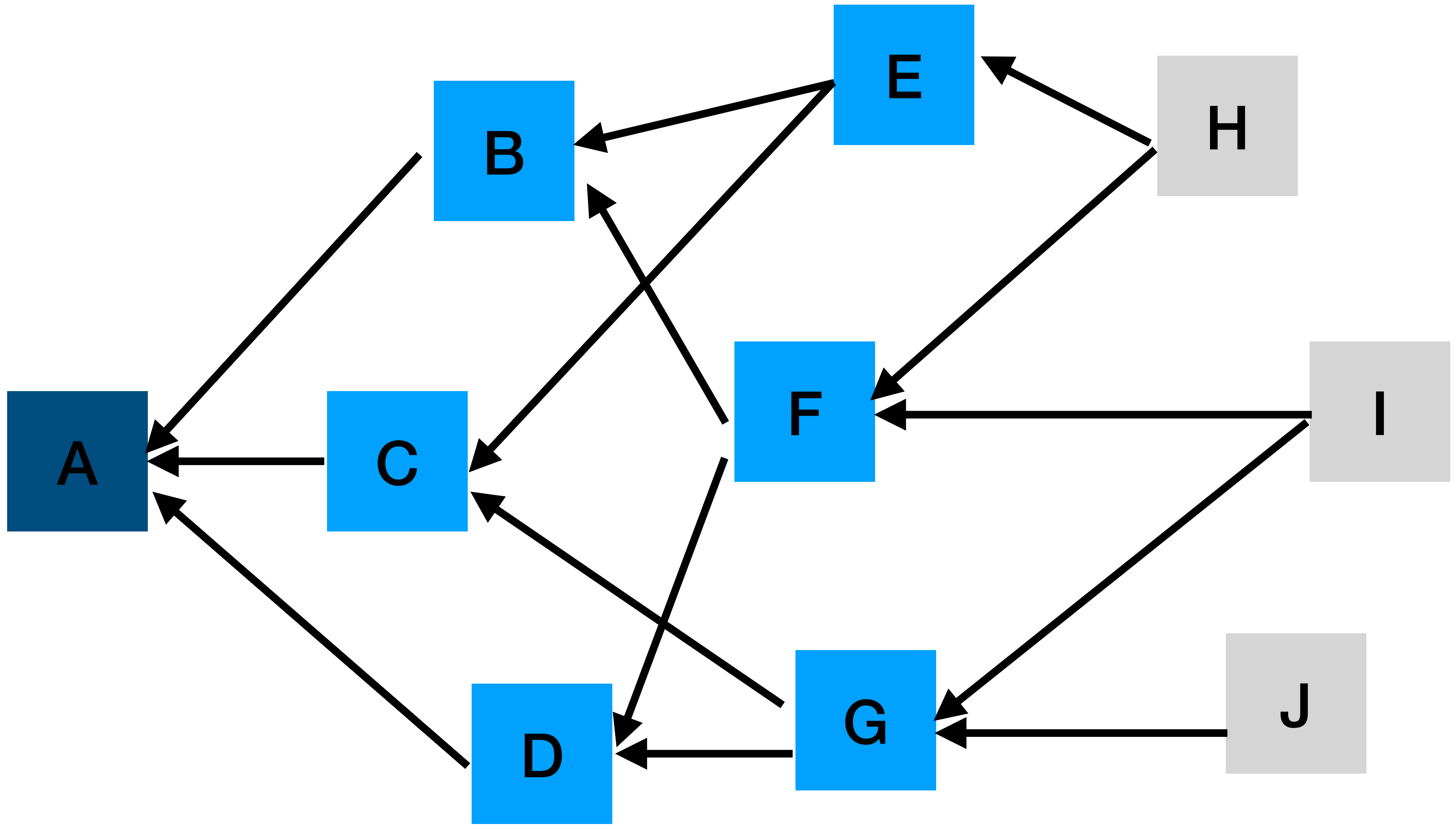
- Nodes (sites) are transactions (no blocks)
- Edges show approvals
  - Direct approval
    - e.g. I directly approves F
  - Indirect approval
    - e.g. H indirectly approves B



Tangle

Tips

- Tips
    - Newly generated transactions
    - No approvals
- Confirmed
    - Approved transactions
- Genesis
    - First transaction, approved by all



Tangle

Issuing a transaction

- Anyone wants to issue a transaction needs to contribute in the system
    - Users = miners
- Contribution means approving transactions
- A valid transaction needs to have two things
    - PoW
    - References to two other transactions

Tangle

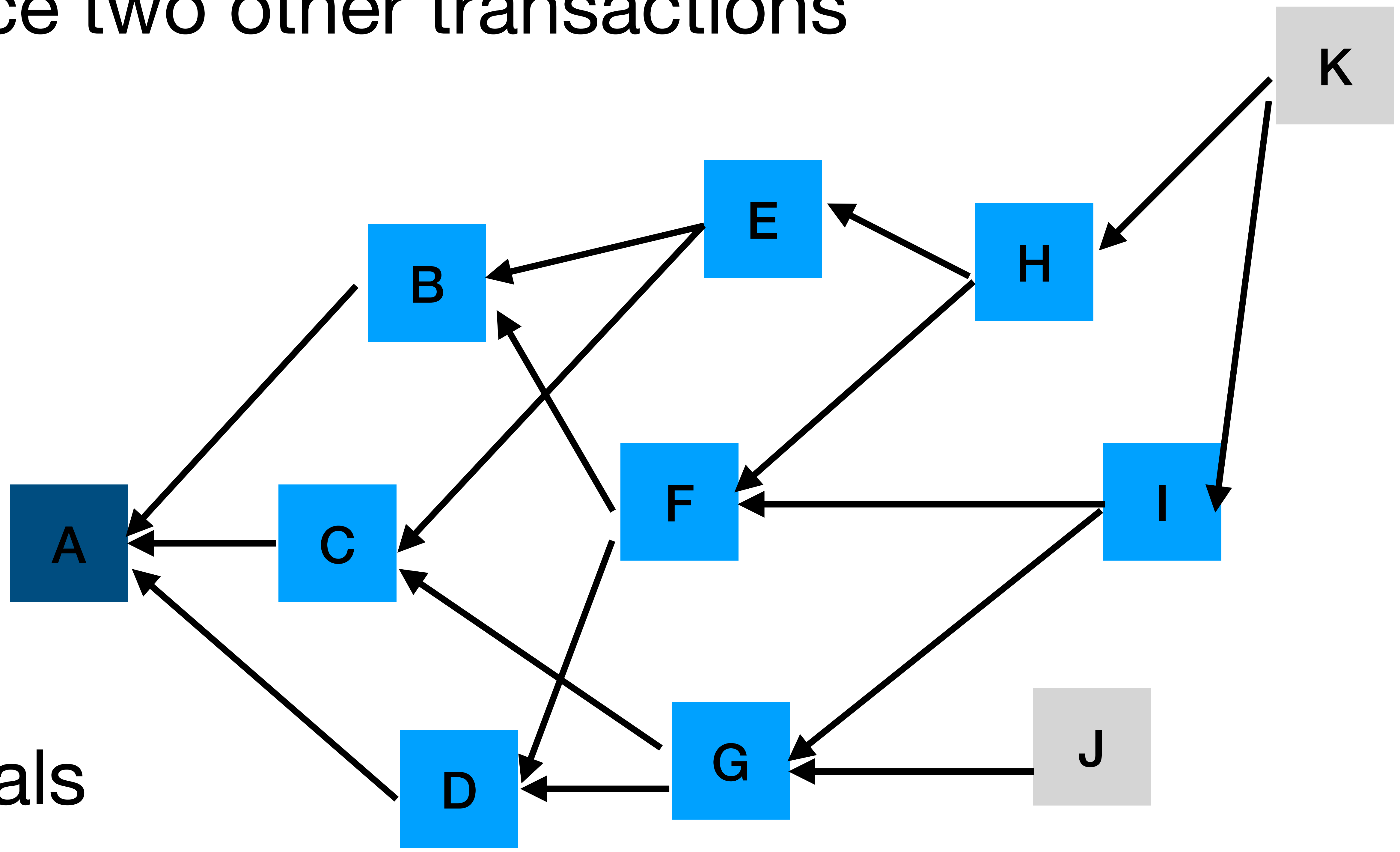
PoW

- Users need to compute a PoW similar to Bitcoin for each transaction
- PoW in Tangle is very light
  - IoT devices can compute the puzzle
- PoW makes it hard for others to spam the network with invalid transactions
  - Users need to invest computational resources
- A transaction with better PoW is considered safer, and has more weight in the system

Tangle

Approving others

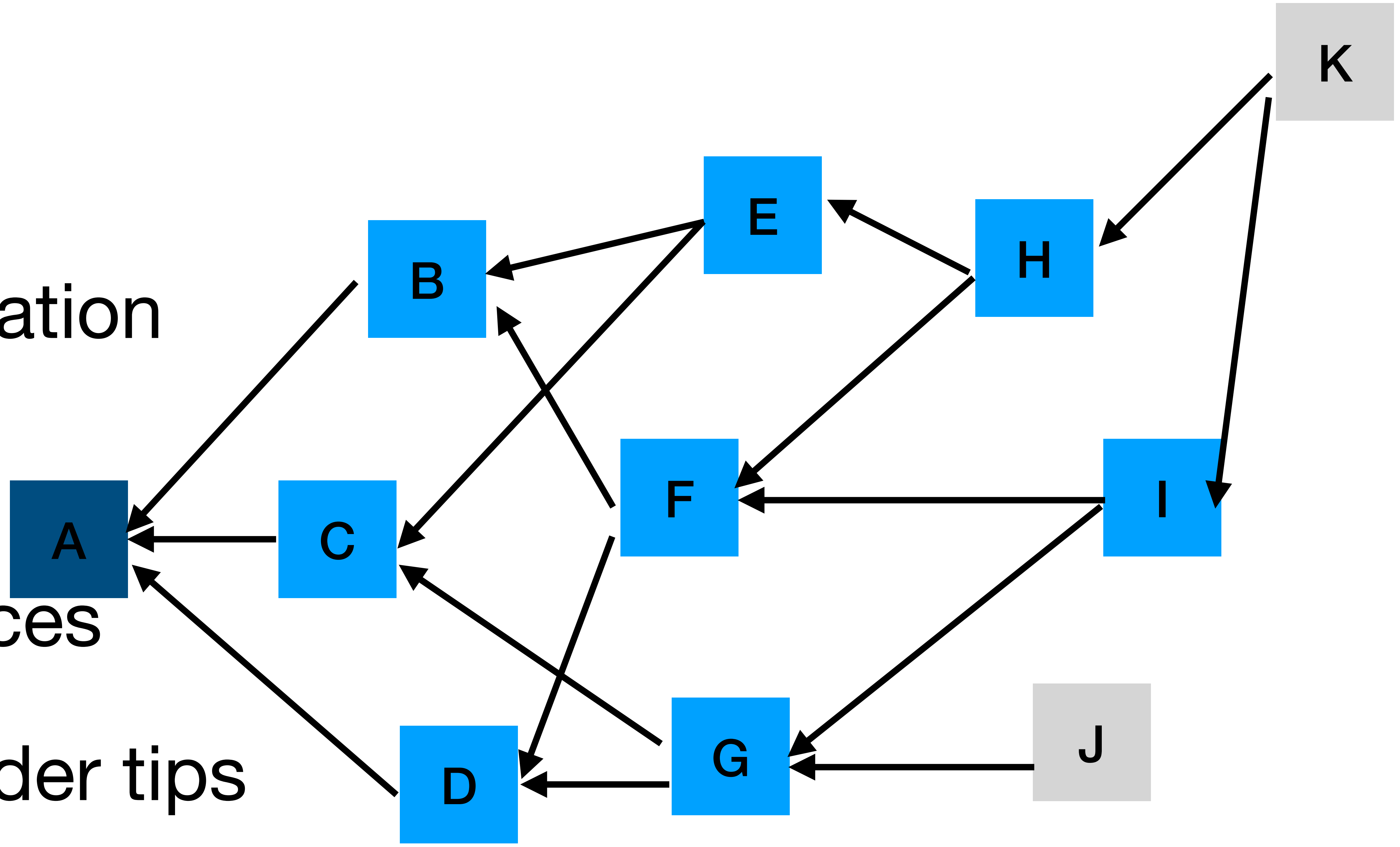
- Each transaction needs to reference two other transactions
- References are approvals (edges)
  - Users verify other transactions
- Users contribute by verifying
- Confirmed transactions
  - Transactions with lots of approvals



Tangle

Approving others

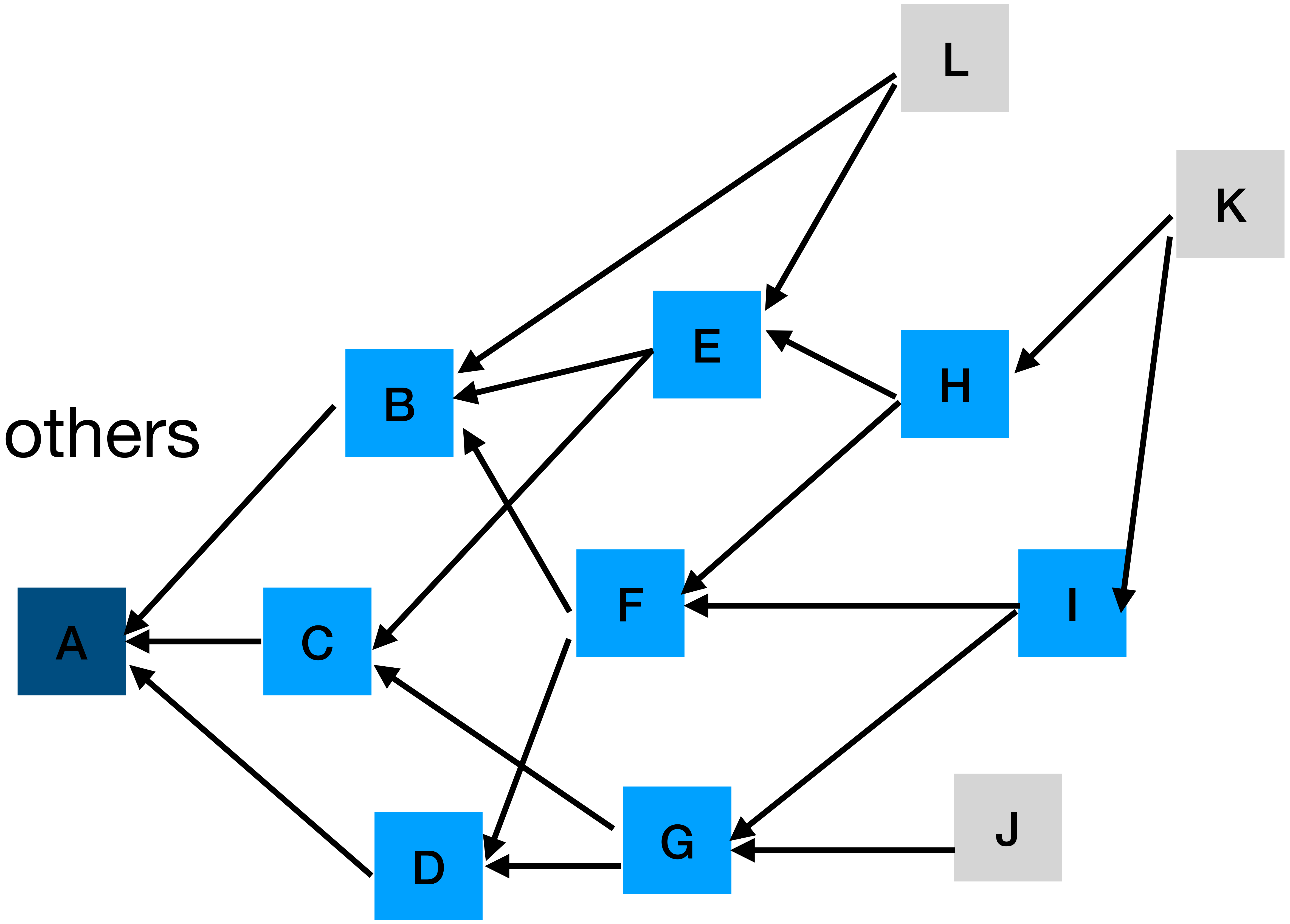
- Simple rule
  - Approve two other transactions
- Tips should be prioritized in verification
  - They don't have approvals
  - Indirectly approves their references
- Ideally new tips should approve older tips



Tangle

Lazy tips

- Simple rule
  - Approve two other transactions
- Why waste resources on verifying others
  - Approve already approved ones
- Lazy tips
  - Not helpful for the system



Tangle

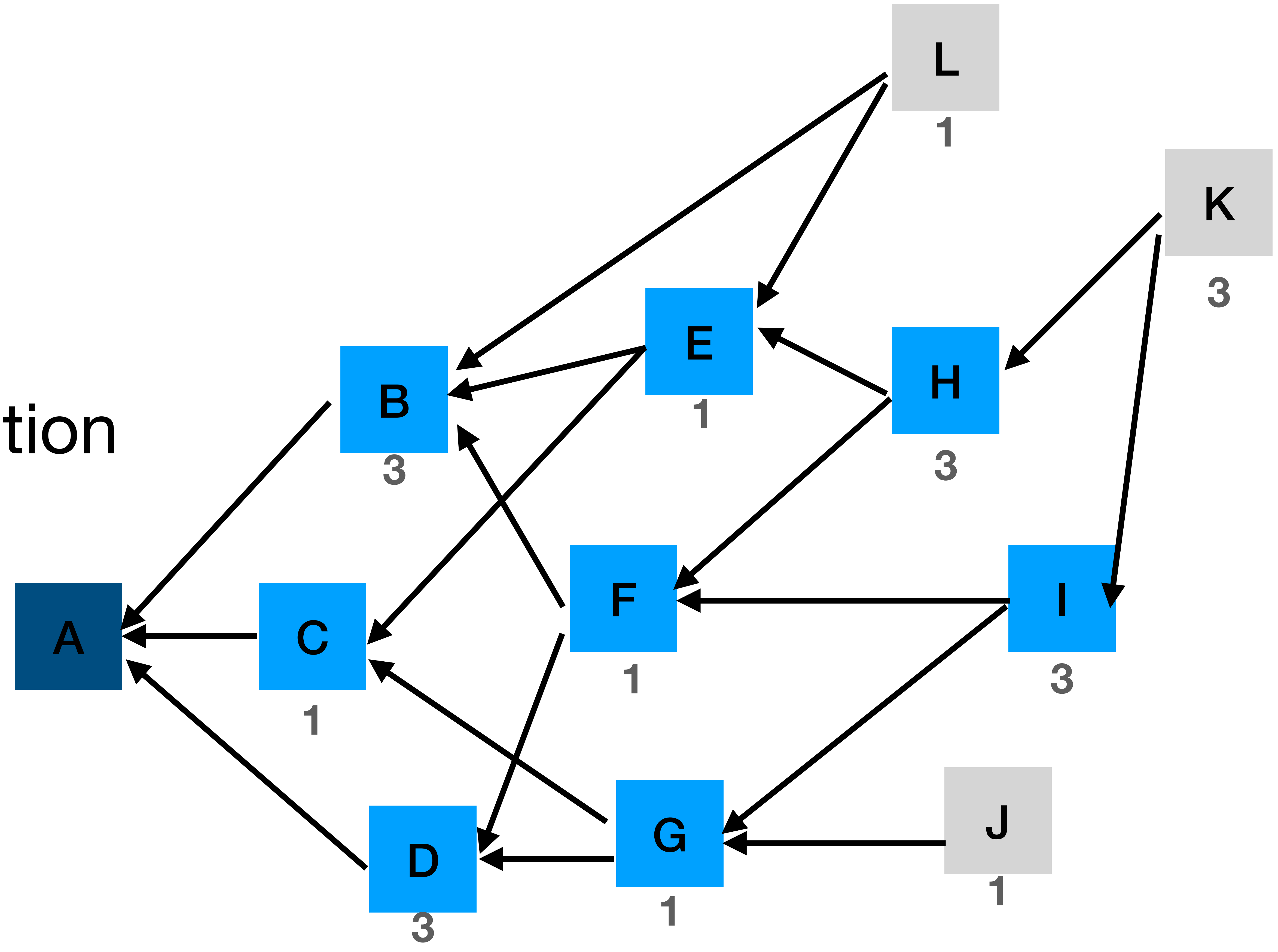
Weights

- How to prevent lazy tips?
  - Others don’t reference lazy tips
    - Won’t be confirmed
  - Need for a common tip selection algorithm
    - Everyone follow the same algorithm
      - Users are mostly IoT devices
- Which transaction should be selected?
  - Transaction weight

Tangle

Weights

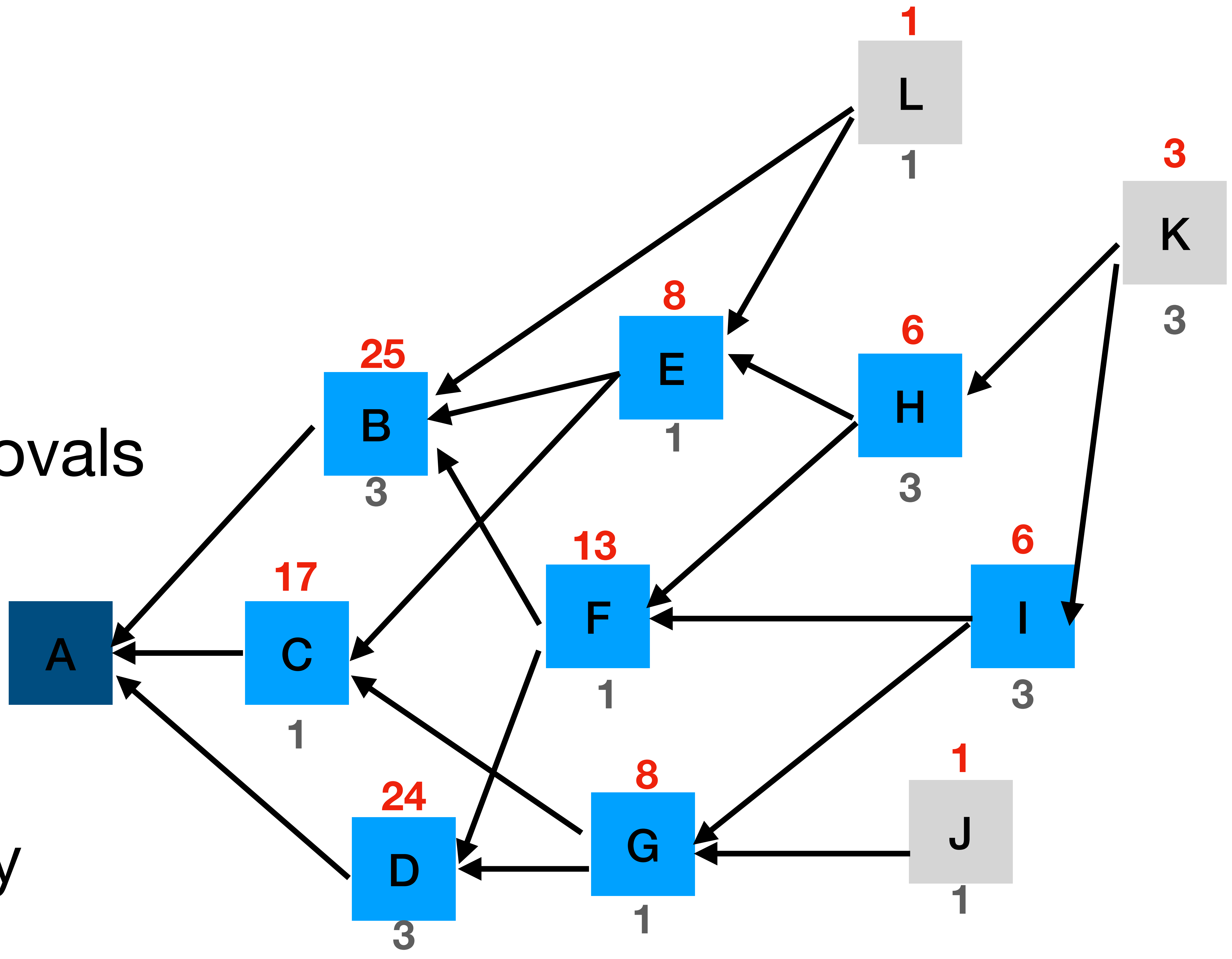
- Two weights for each transaction
- Own weight
  - The score given to each transaction
  - Determines how secure it is
  - Based on the provided PoW



Tangle

Weights

- Two weights for each transaction
- Cumulative weight
  - Sum of own weight and all approvals
  - Direct and indirect
  - Larger cumulative weight
    - Larger confirmation probability



Tangle

Random walk

- Transaction selection
  - Tips should be prioritised over already approved sites
    - Tip selection
  - Sites with more approvals are more secure
    - Cumulative weights
  - Selection should be evenly distributed based on weights
    - Tips with same weight have equal chances of being selected

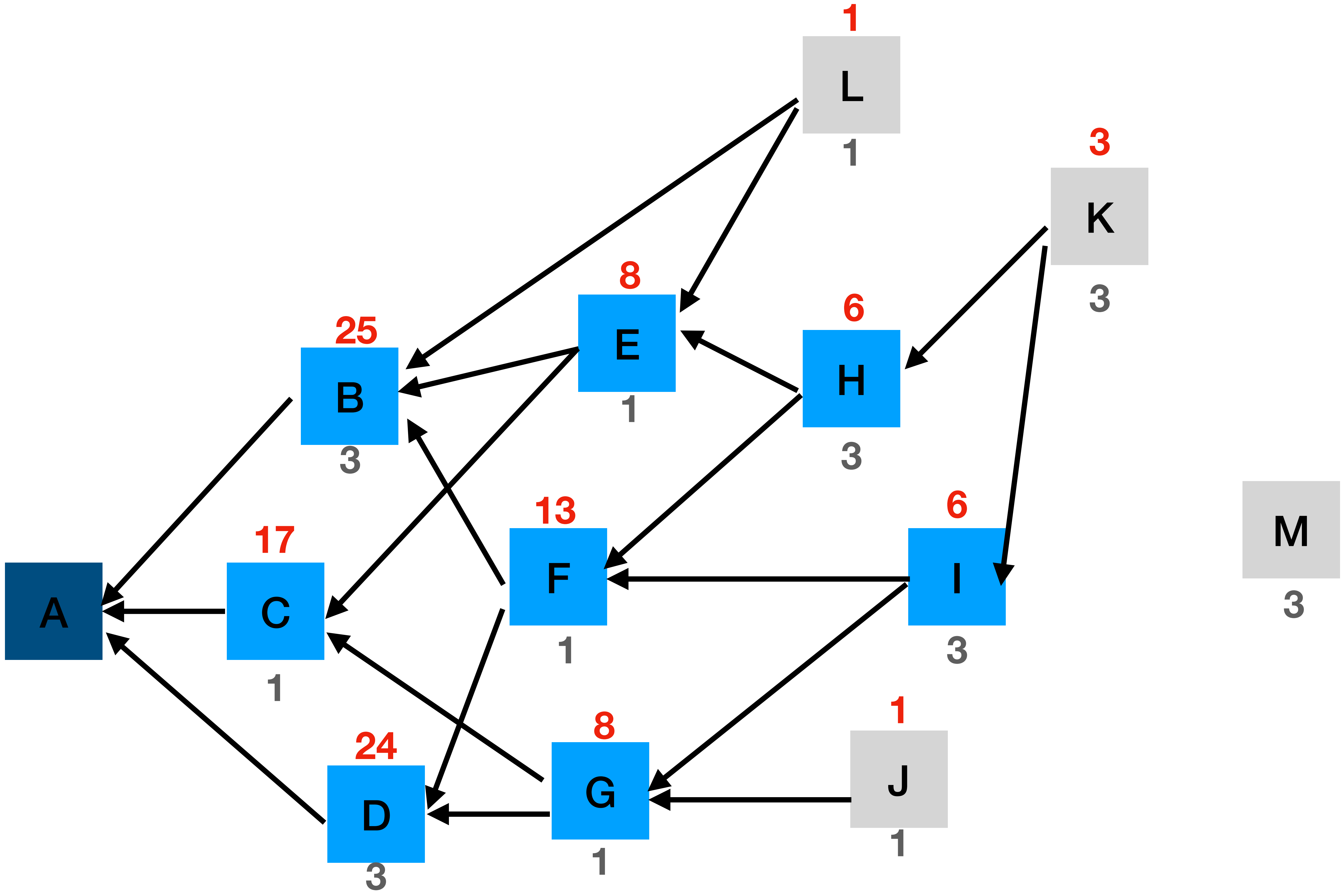
Tangle

Random walk

- Random walk
    - Start from genesis
    - Gather a list from all sites who referenced the transaction
    - Randomly choose one based on their cumulative weights
    - Repeat until it’s a tip

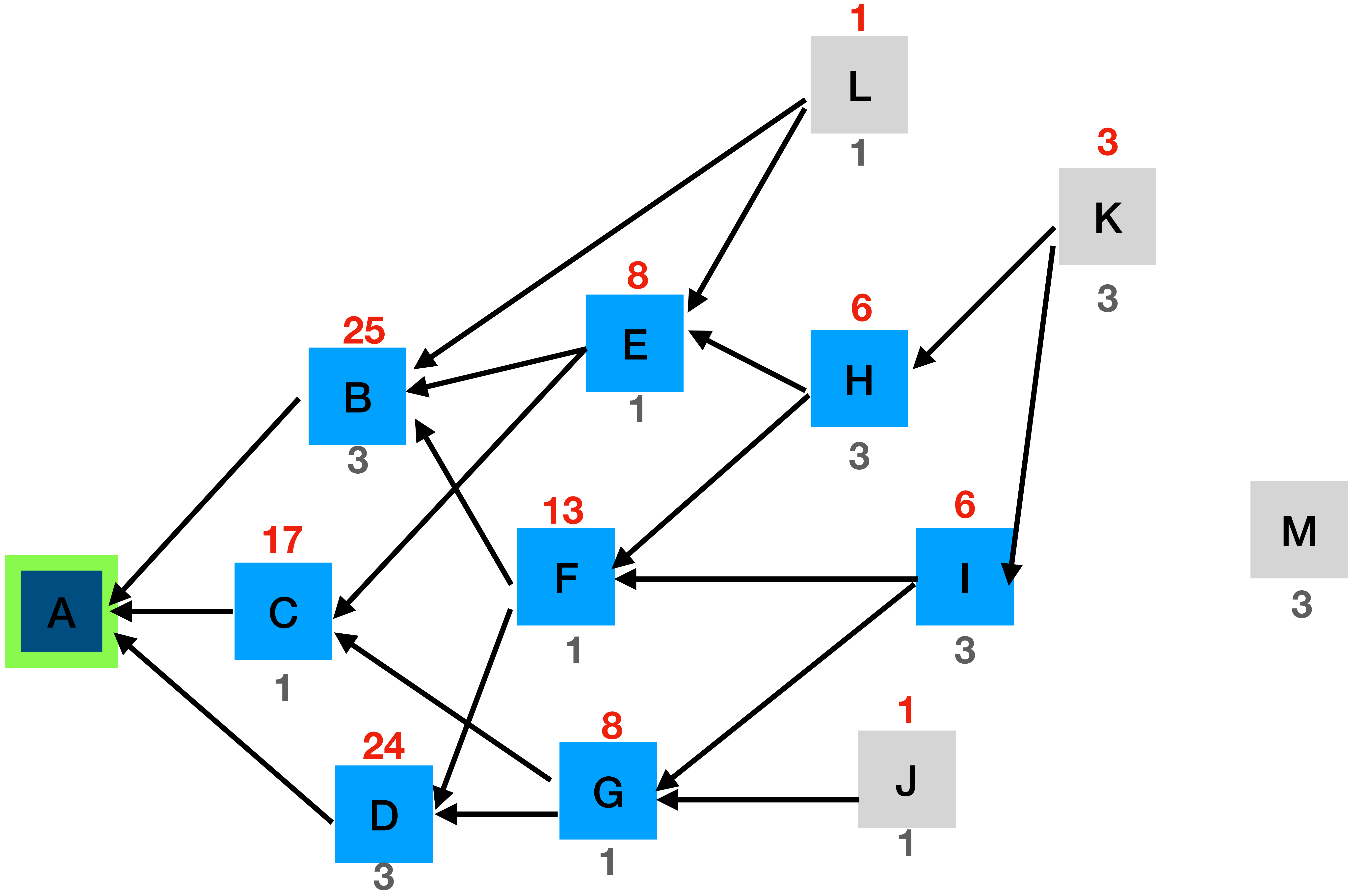
Tangle

Random walk



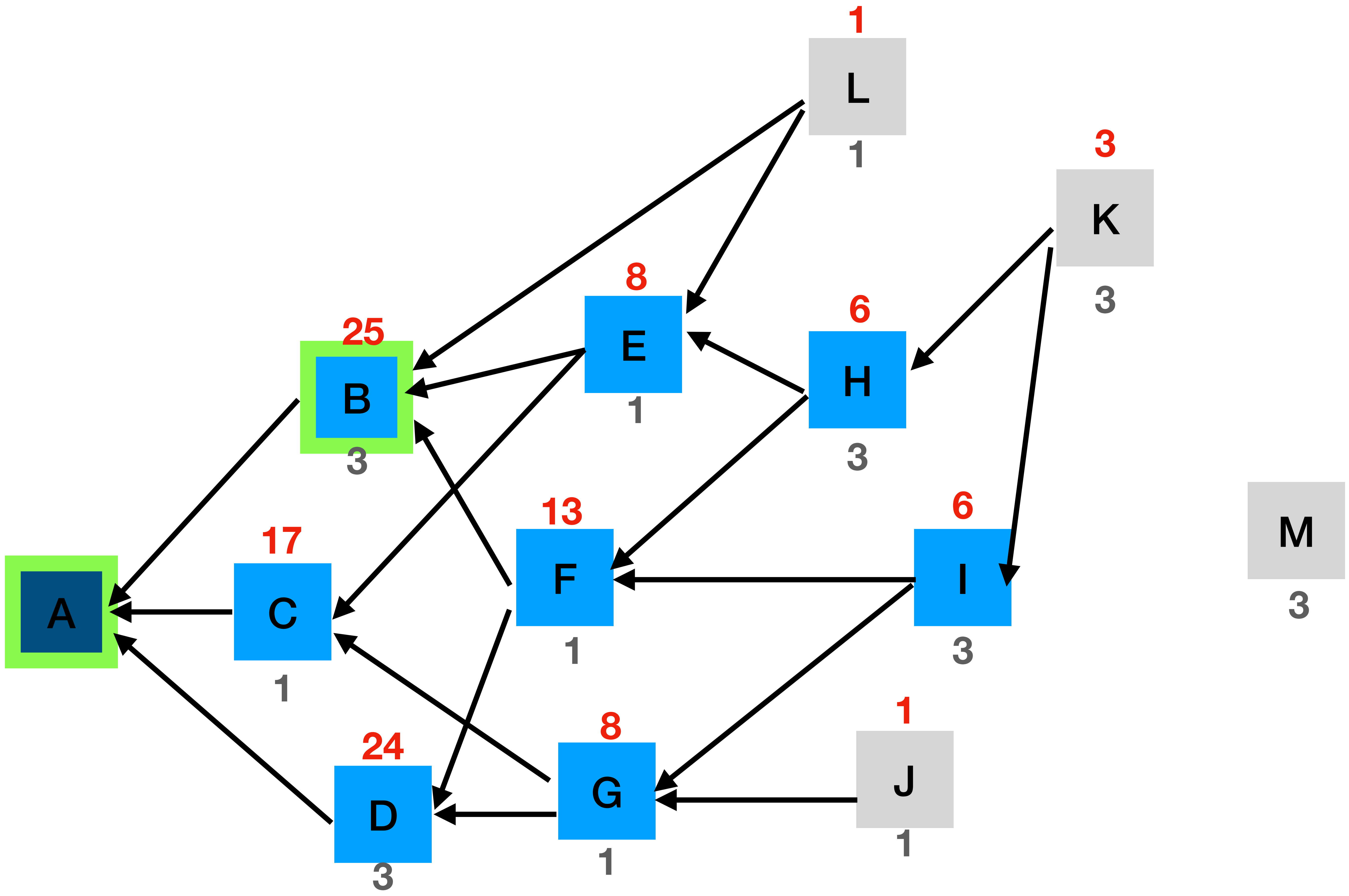
Tangle

Random walk



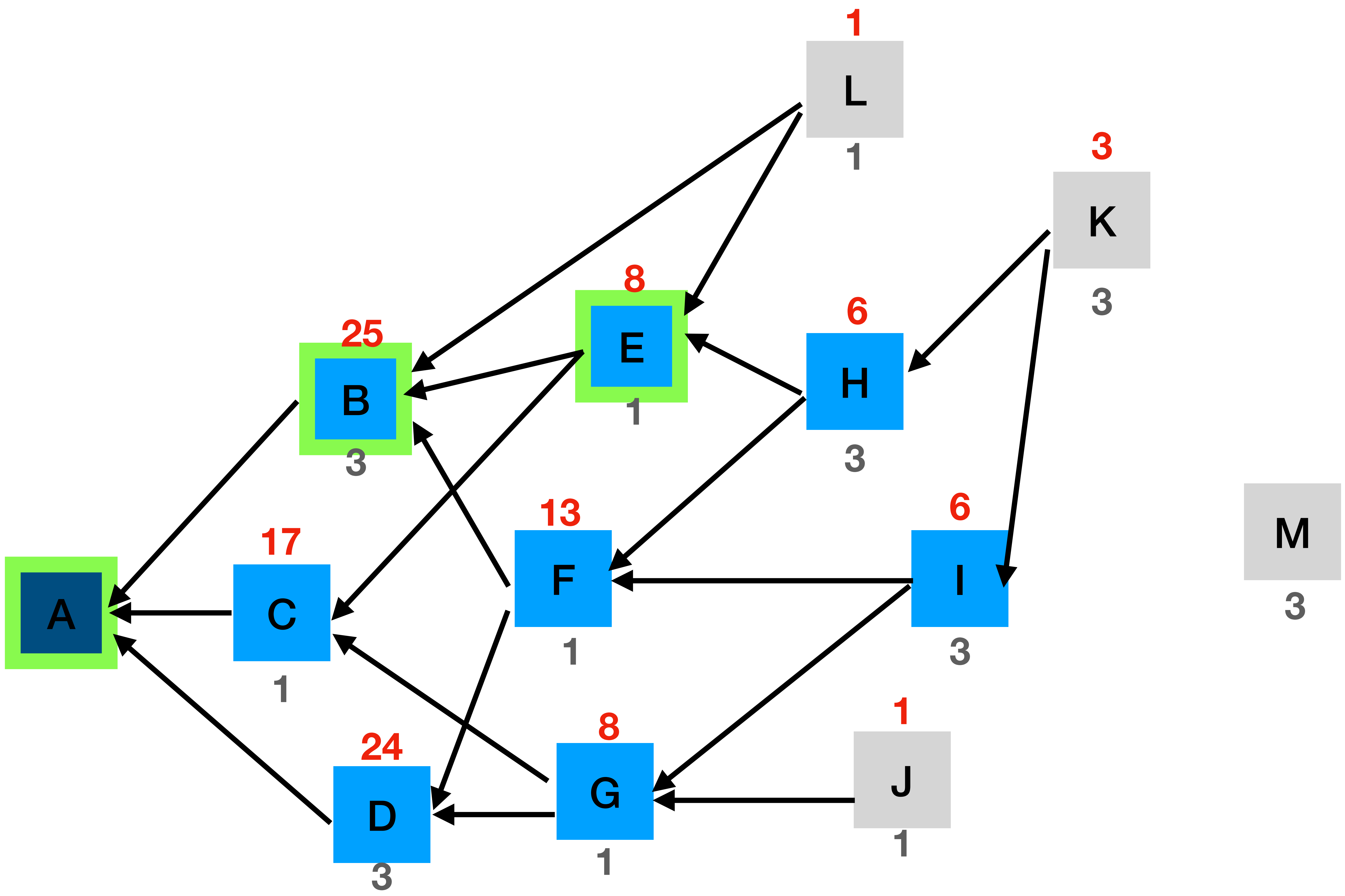
Tangle

Random walk



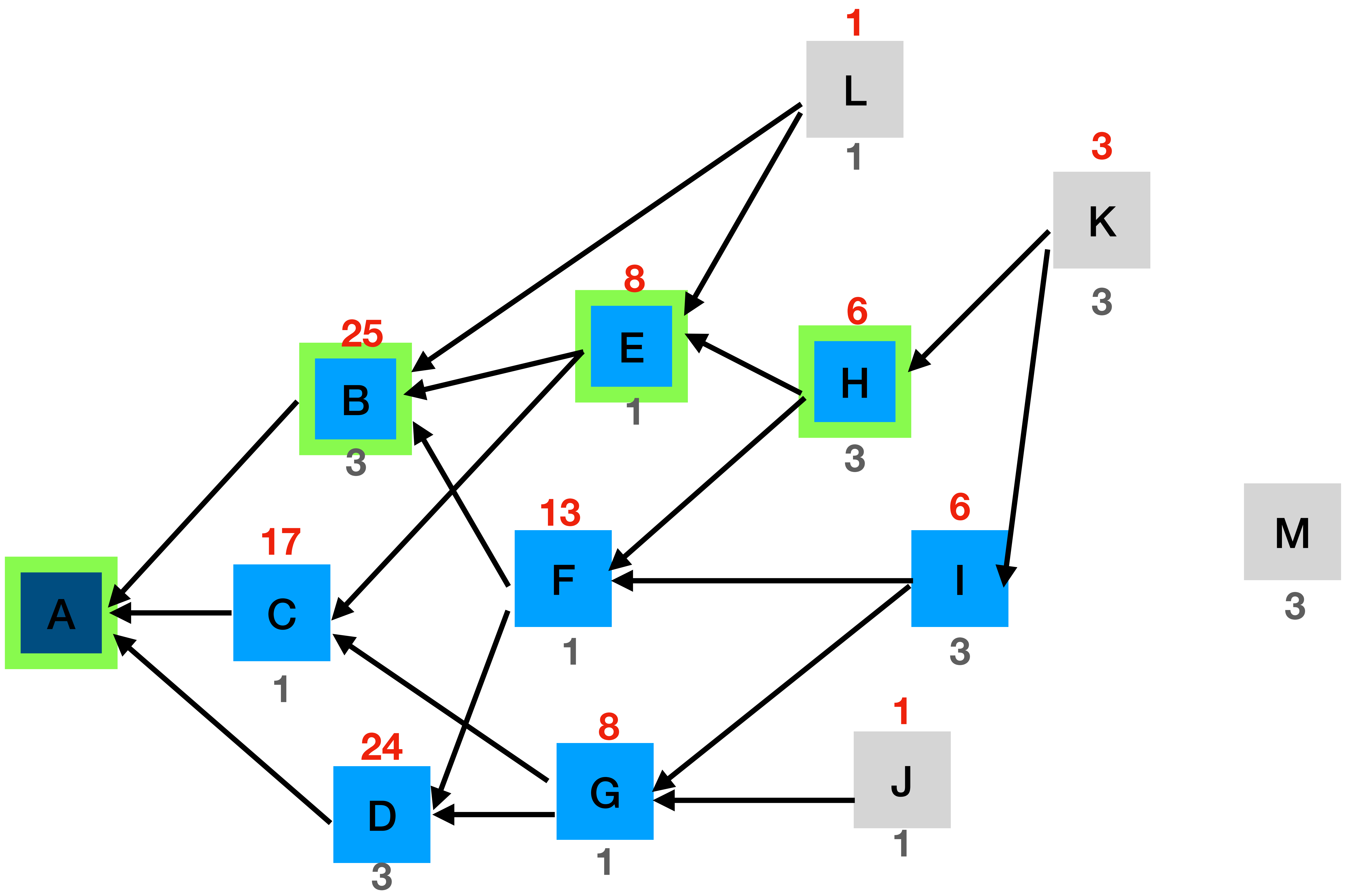
Tangle

Random walk



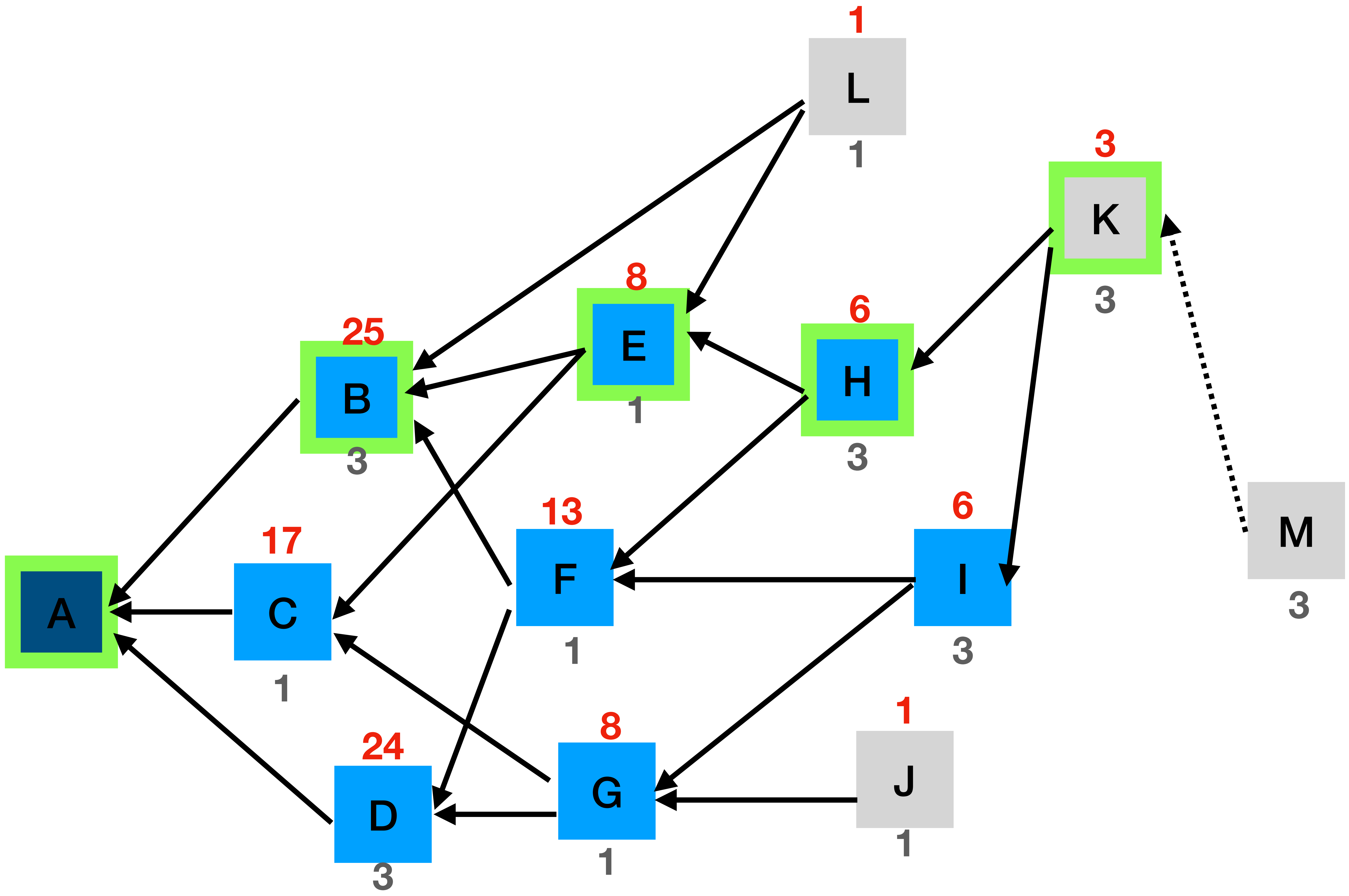
Tangle

Random walk



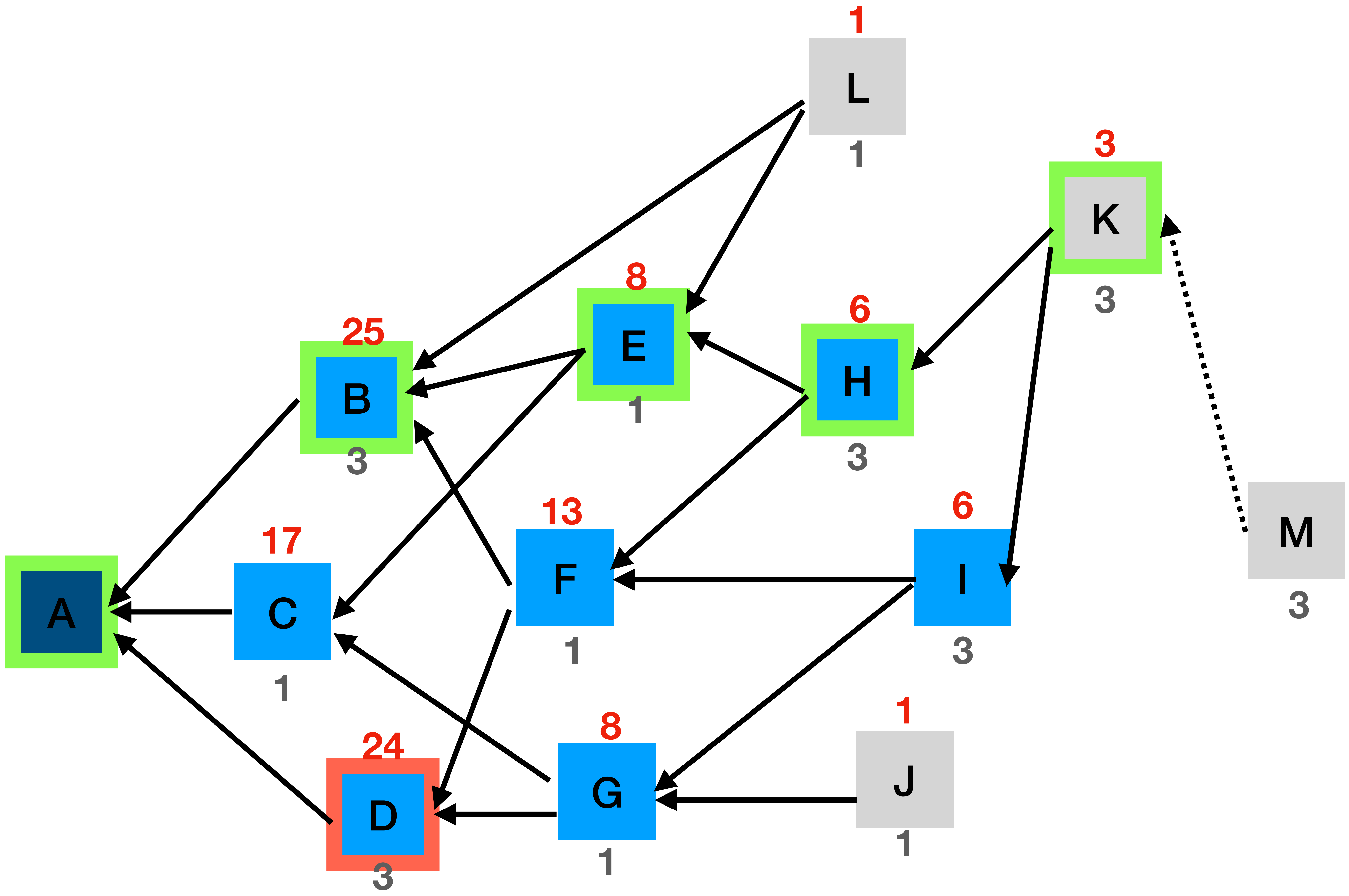
Tangle

Random walk



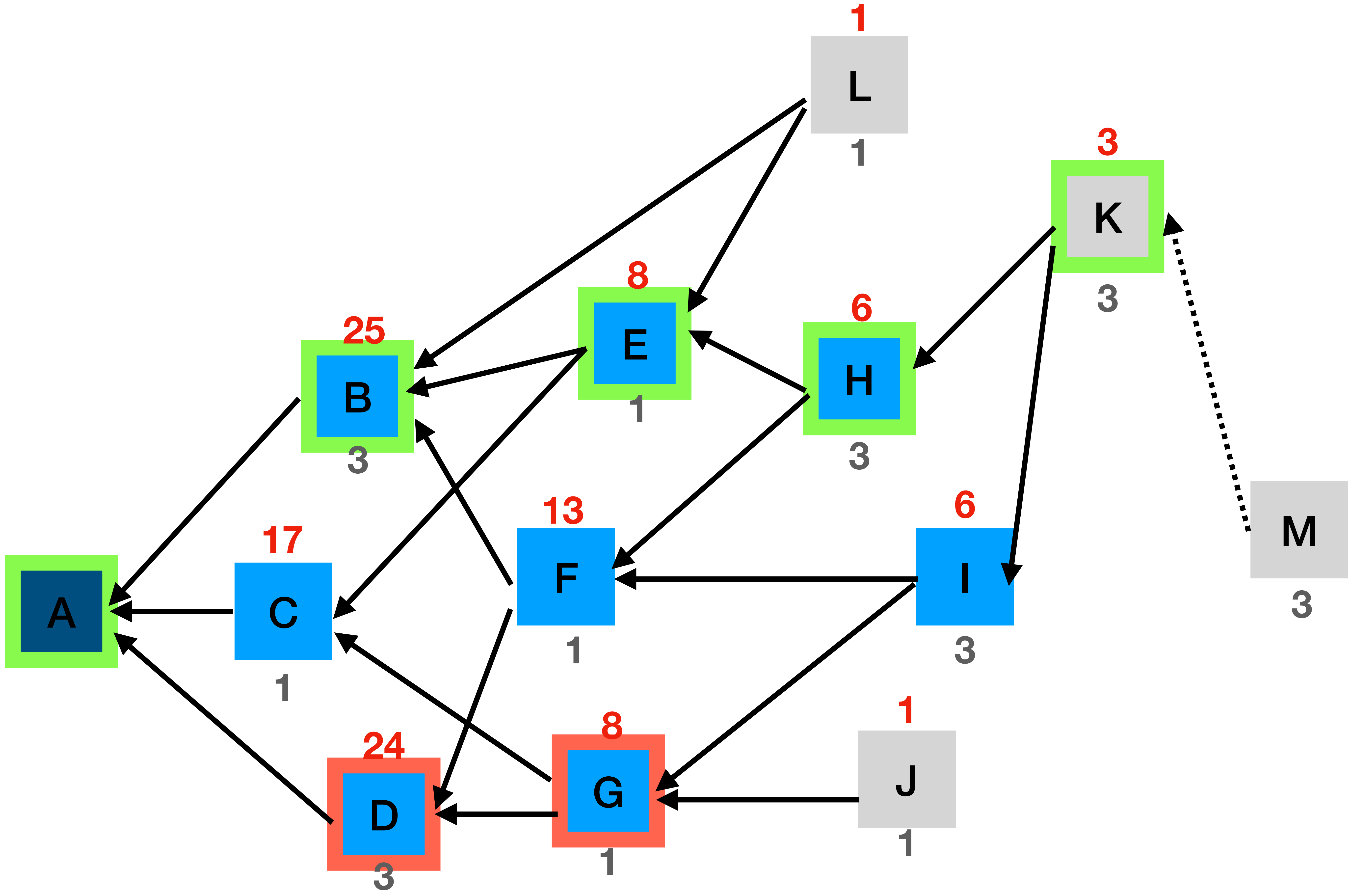
Tangle

Random walk



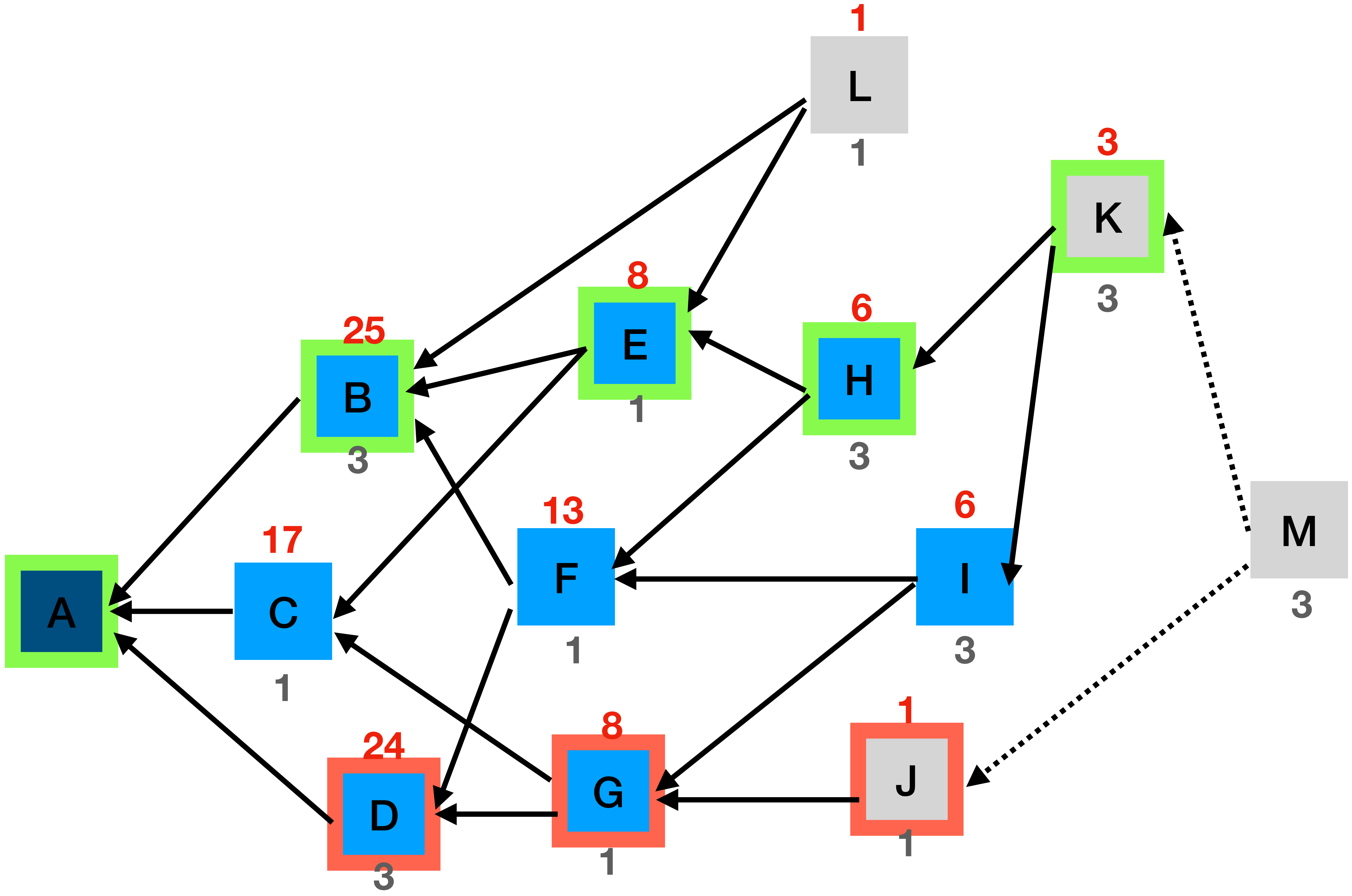
Tangle

Random walk



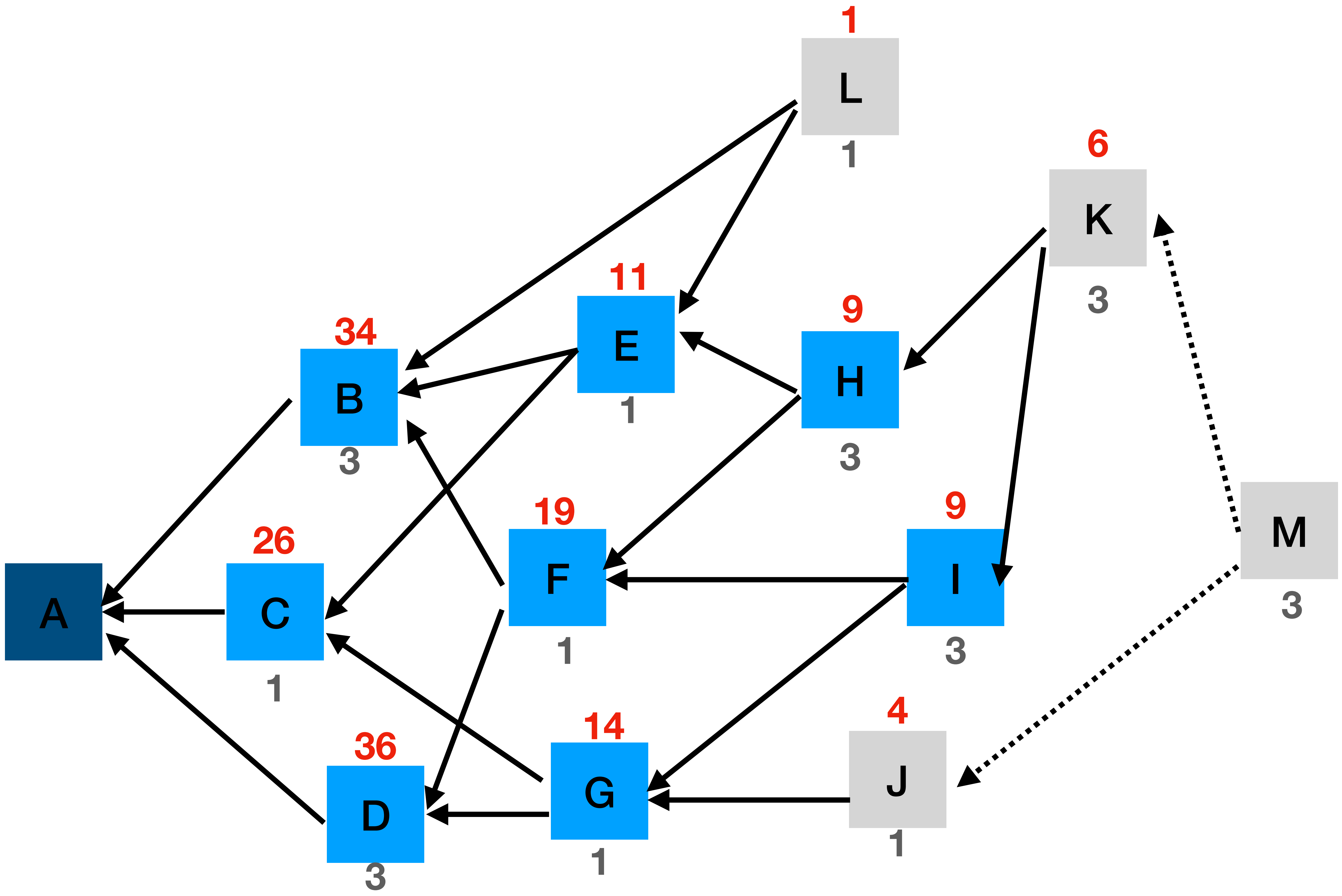
Tangle

Random walk



Tangle

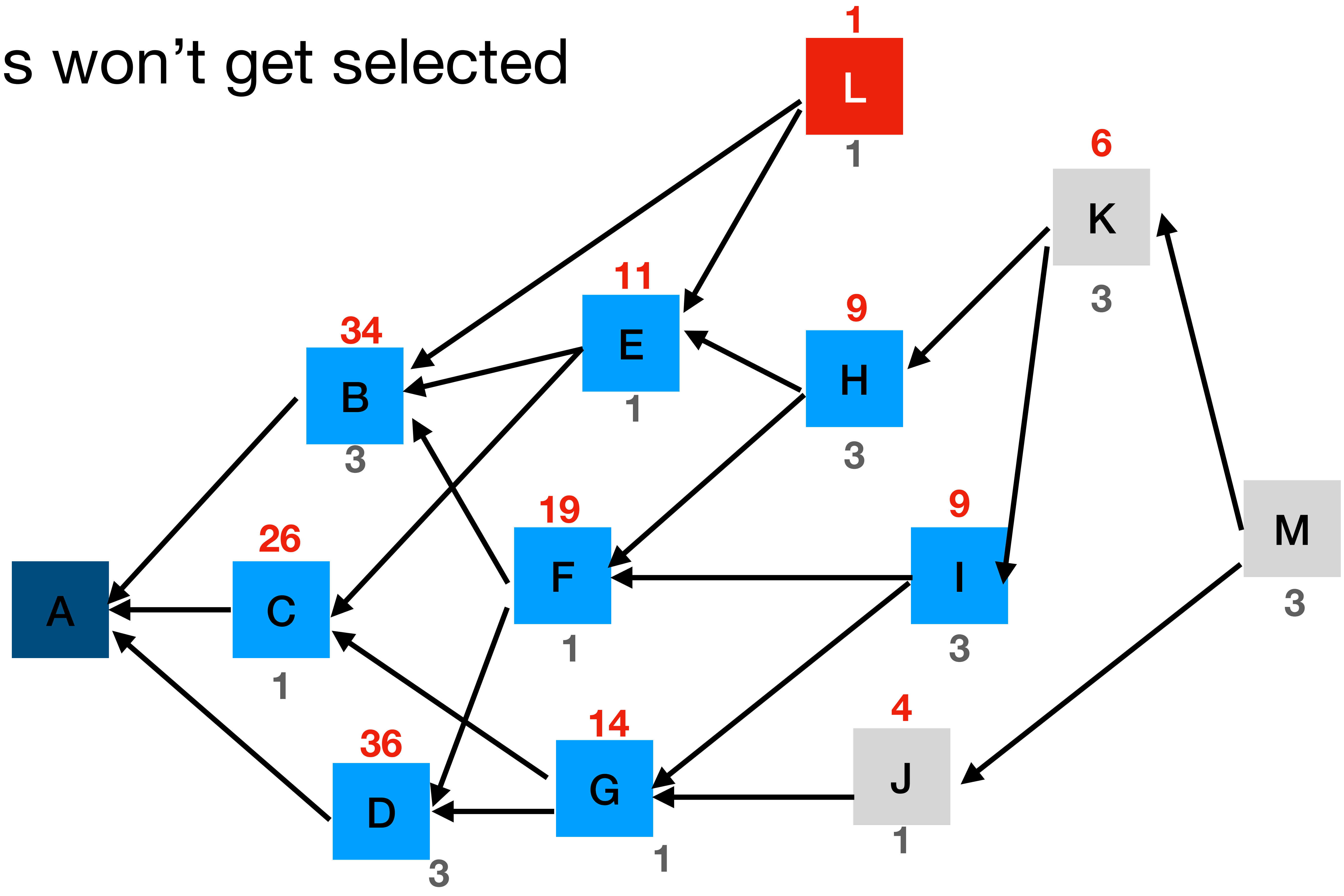
Random walk



Tangle

Orphan tips

- Due to random walk, lazy tips won't get selected
  - They get orphaned
  - Discarded after a while



Tangle

Milestones

- Random walk is slow
- It’s expensive to keep track of whole Tangle
- Milestones
  - Special transactions
  - Checkpoints
  - Mark the state of Tangle

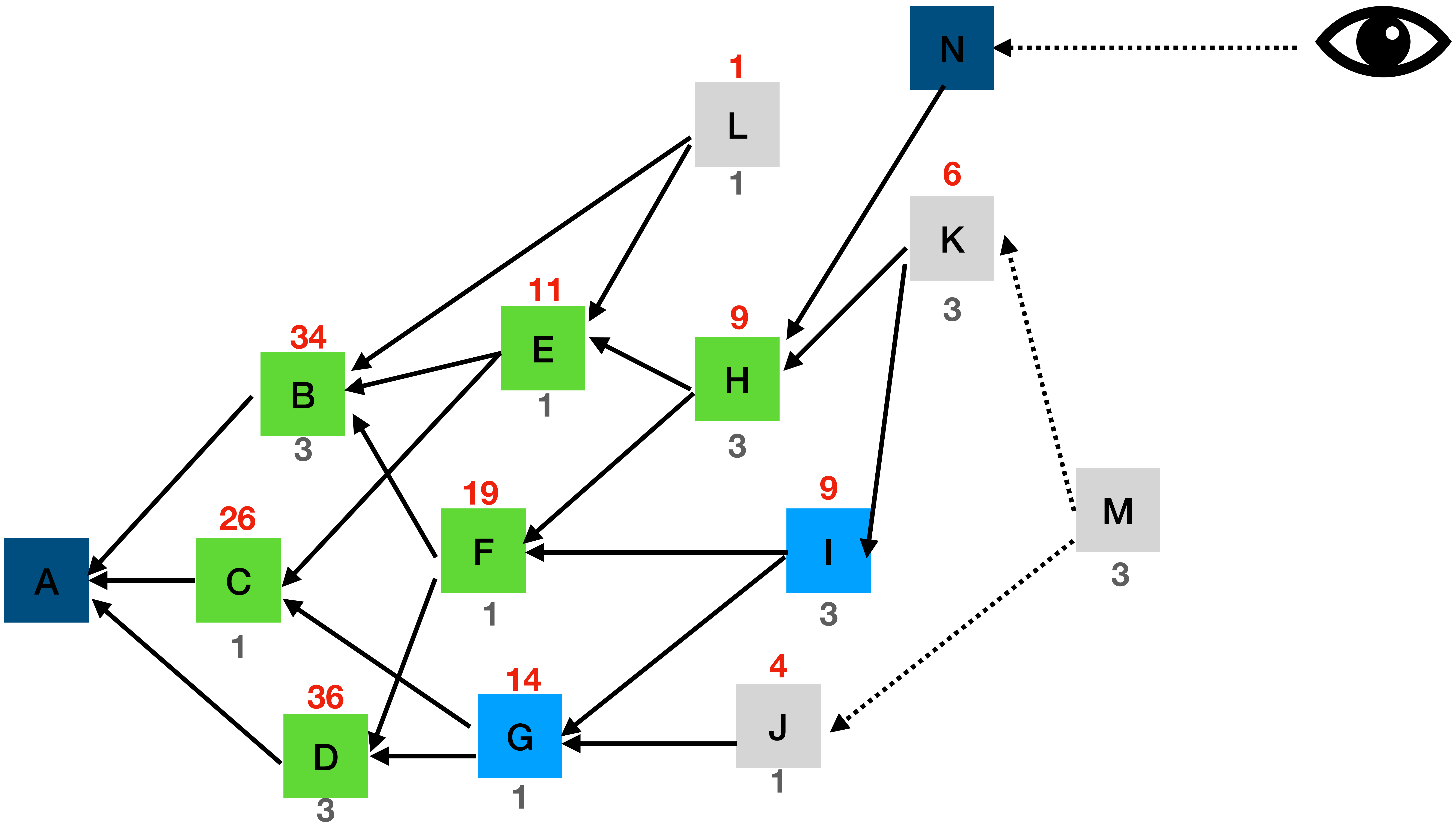
Tangle

Milestones

- Coordinator
  - Introduced in IOTA
  - Coordinators issues milestones
  - It orders Tangle
  - Milestones issued by coordinator are final
    - Anything directly or indirectly approves by a milestone is approved
    - Can be used as initial point for random walk

Tangle

Milestones



Tangle

Milestones

- Coordinator makes the system centralized
    - Single point of failure
- Instead, nodes can vote for determining the milestones
- But without economical incentives, how can they motivate participation?

Tangle

Mana system

- A reputation system
  - How trustworthy a node is
- Nodes gain Mana (reputation) by certain tasks
  - Being active in the network
  - Holding tokens for a certain period
  - Participating in voting rounds

Tangle

Mana system

- Mana is used for several stuff
    - Random walk takes Mana into account
        - Transactions with higher Mana are approved faster
    - Have a saying in consensus
        - Nodes can have a saying in determining milestones or other consensus related stuff

Tangle 2

Upgrades and future

- Coordicide
  - Removing the coordinator
- Shift from accounts to UTXO
    - Better aligned with the reputation-system
- Introducing smart contracts
- Introducing blocks instead of transactions
- Sharding