Discrete logarithm problem

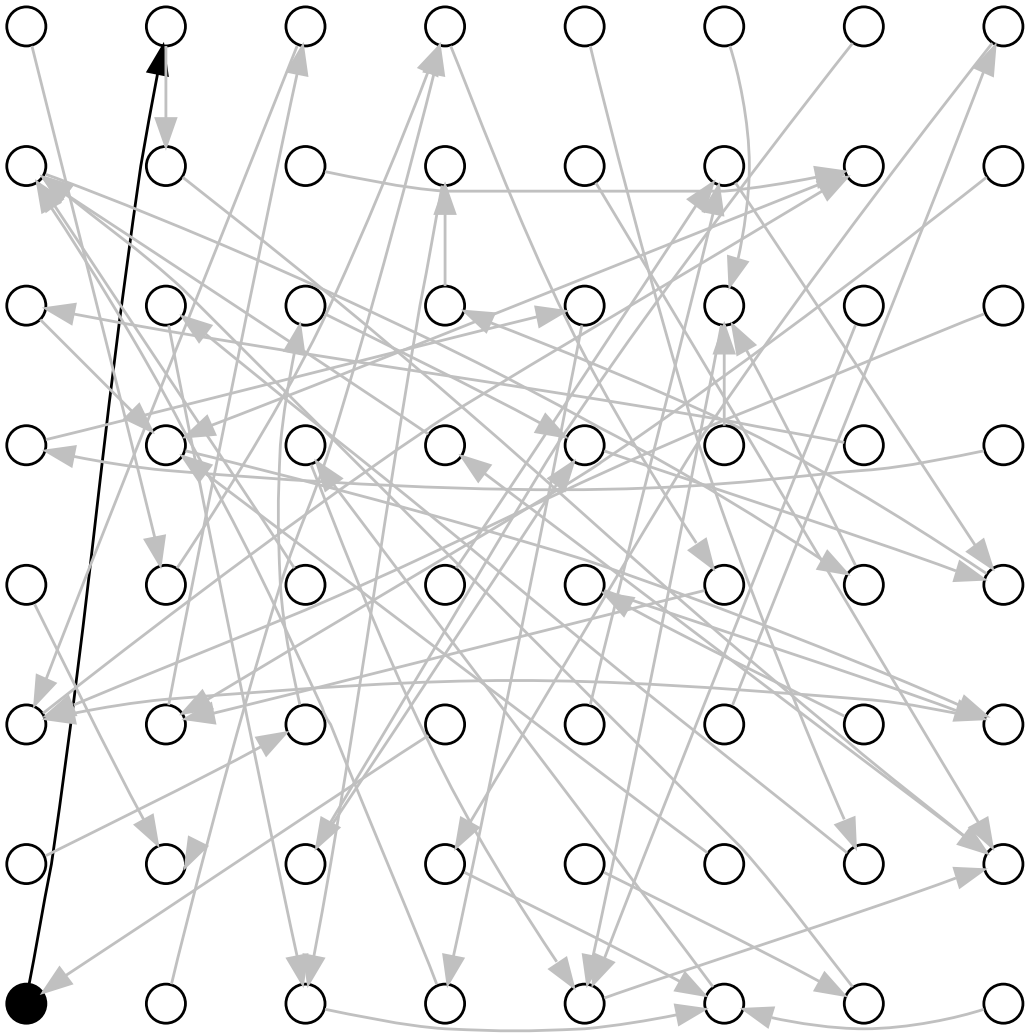
Pollard rhho

Tanja Lange

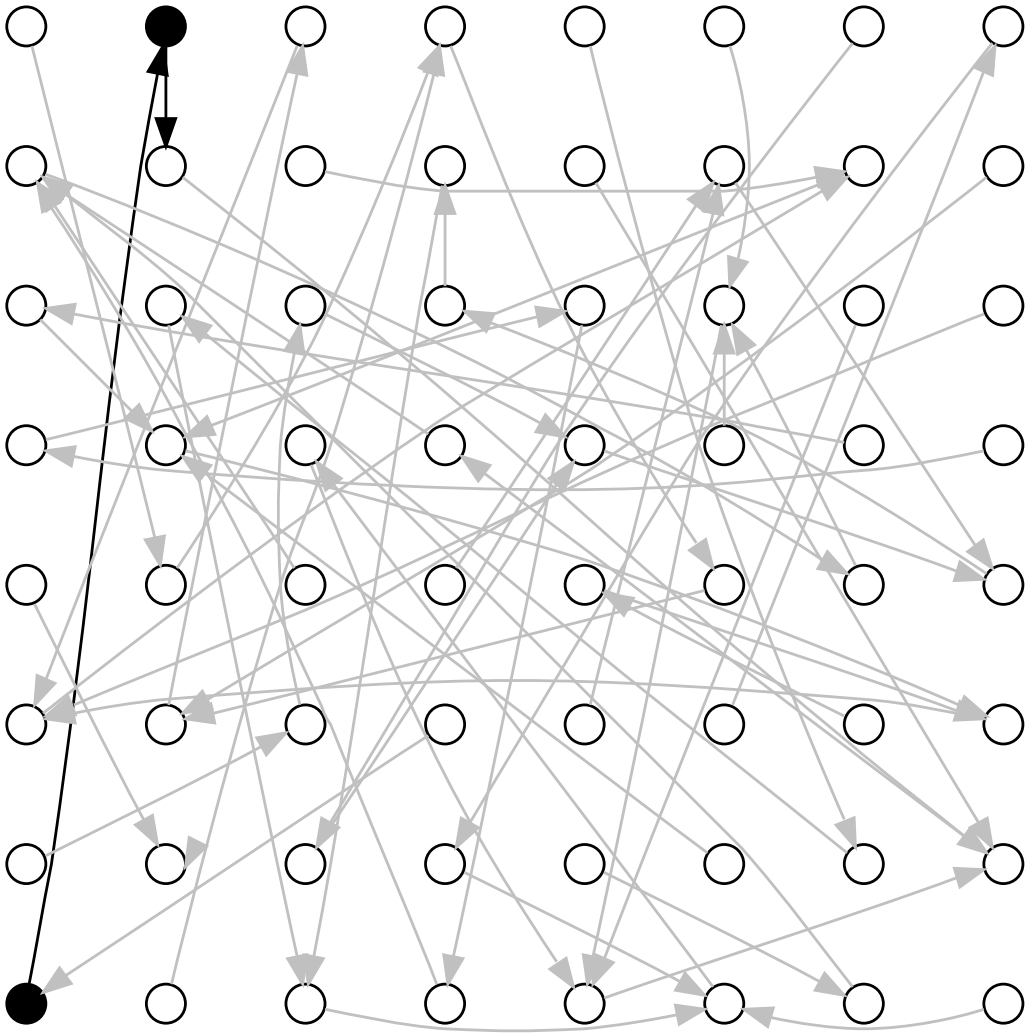
Eindhoven University of Technology

2MMC10 – Cryptology

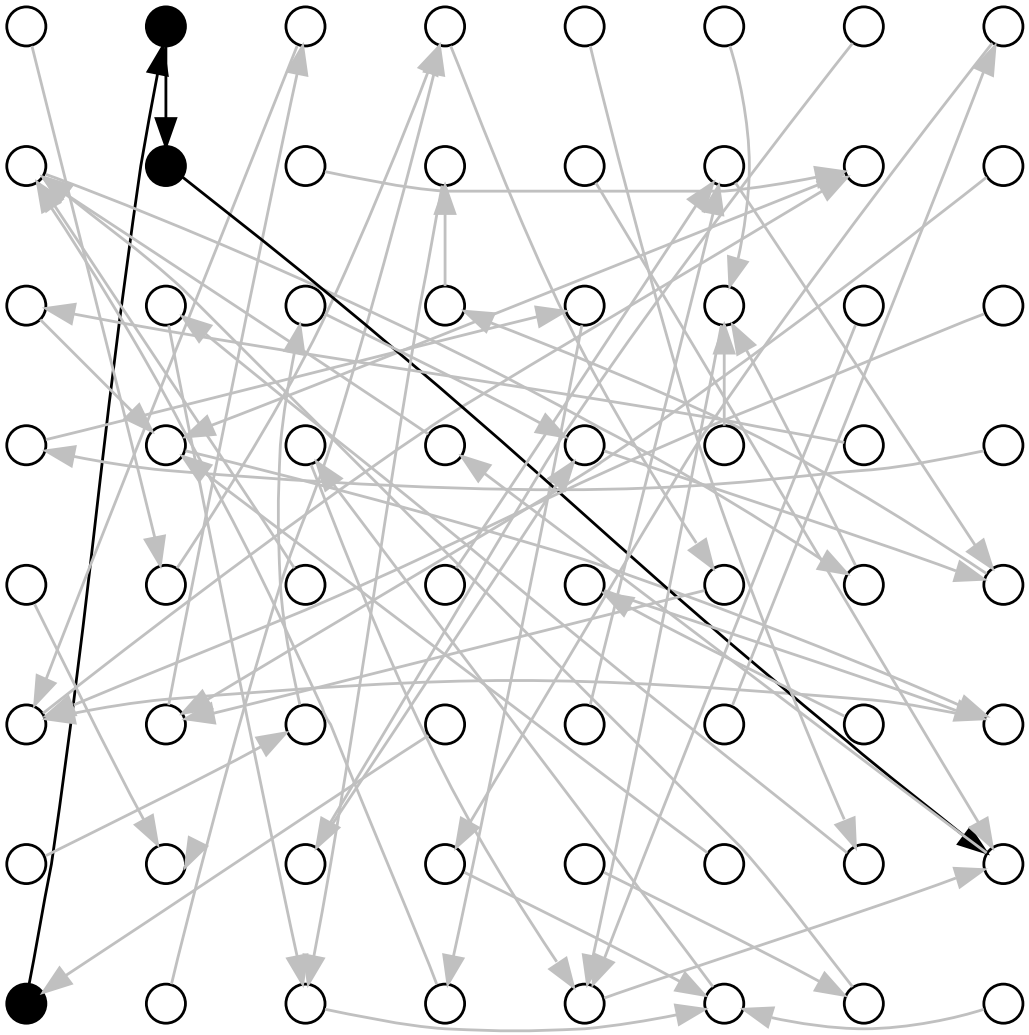
Random walks have collisions



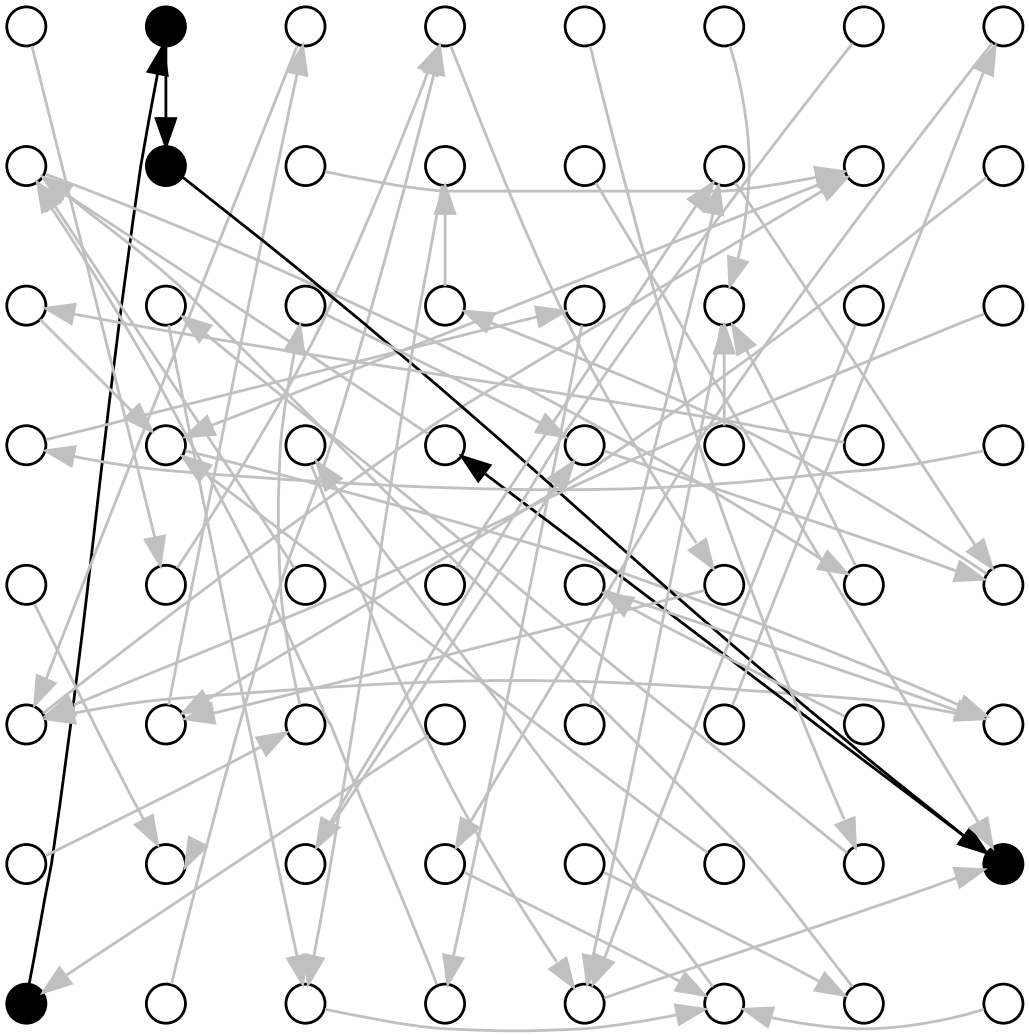
Random walks have collisions



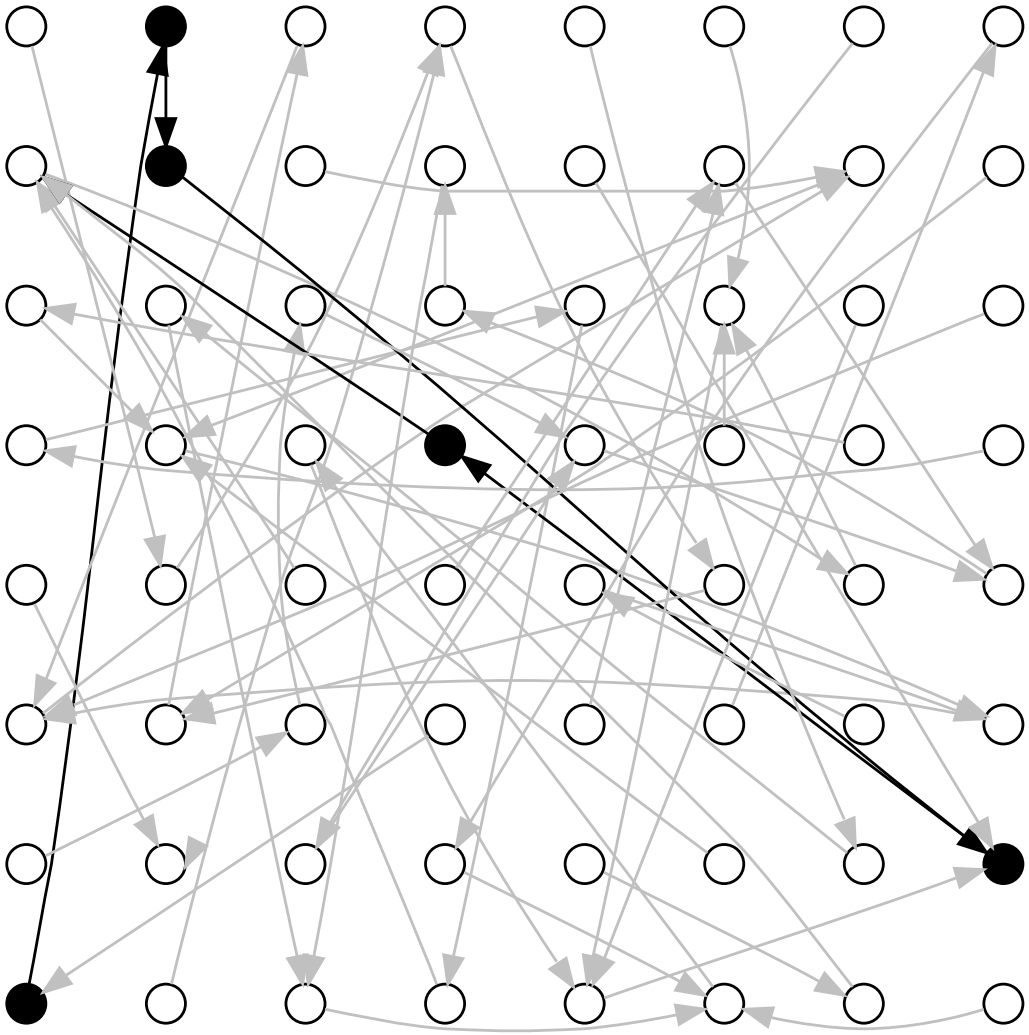
Random walks have collisions



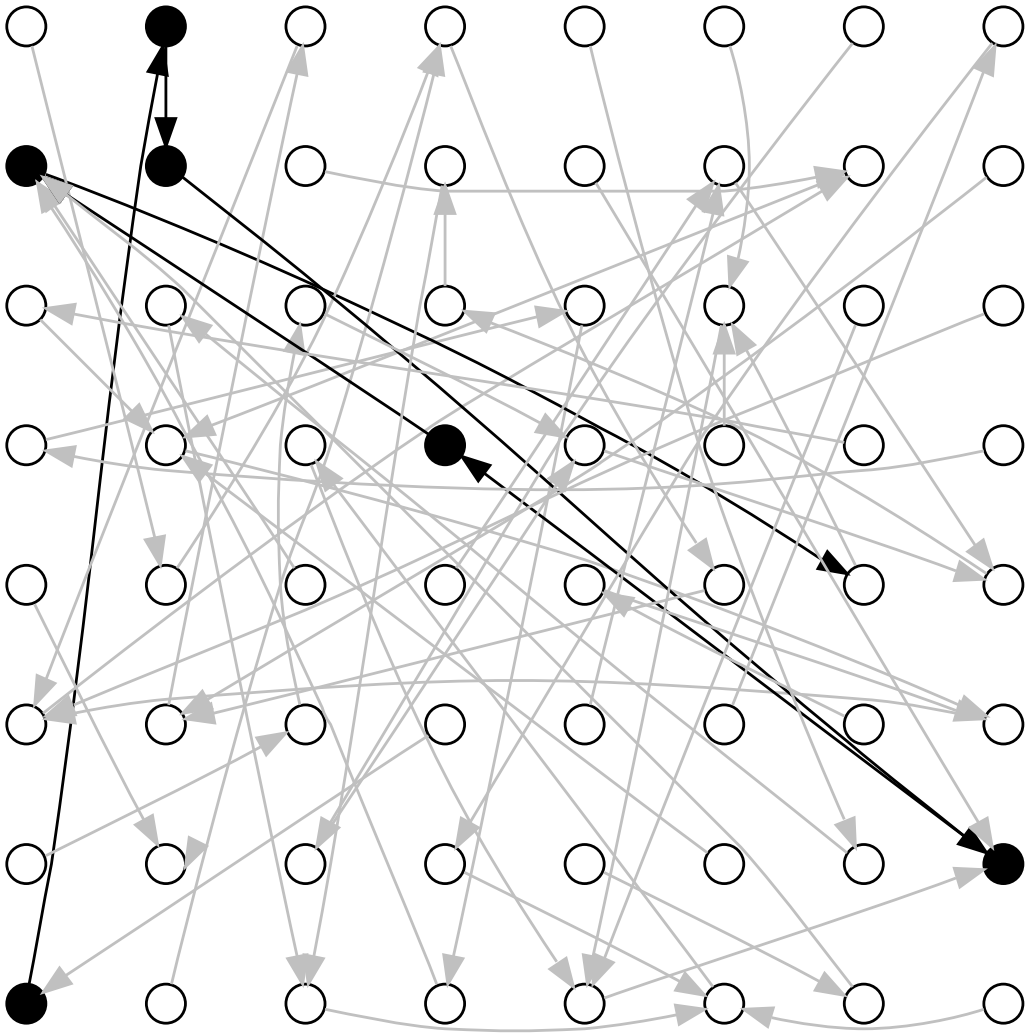
Random walks have collisions



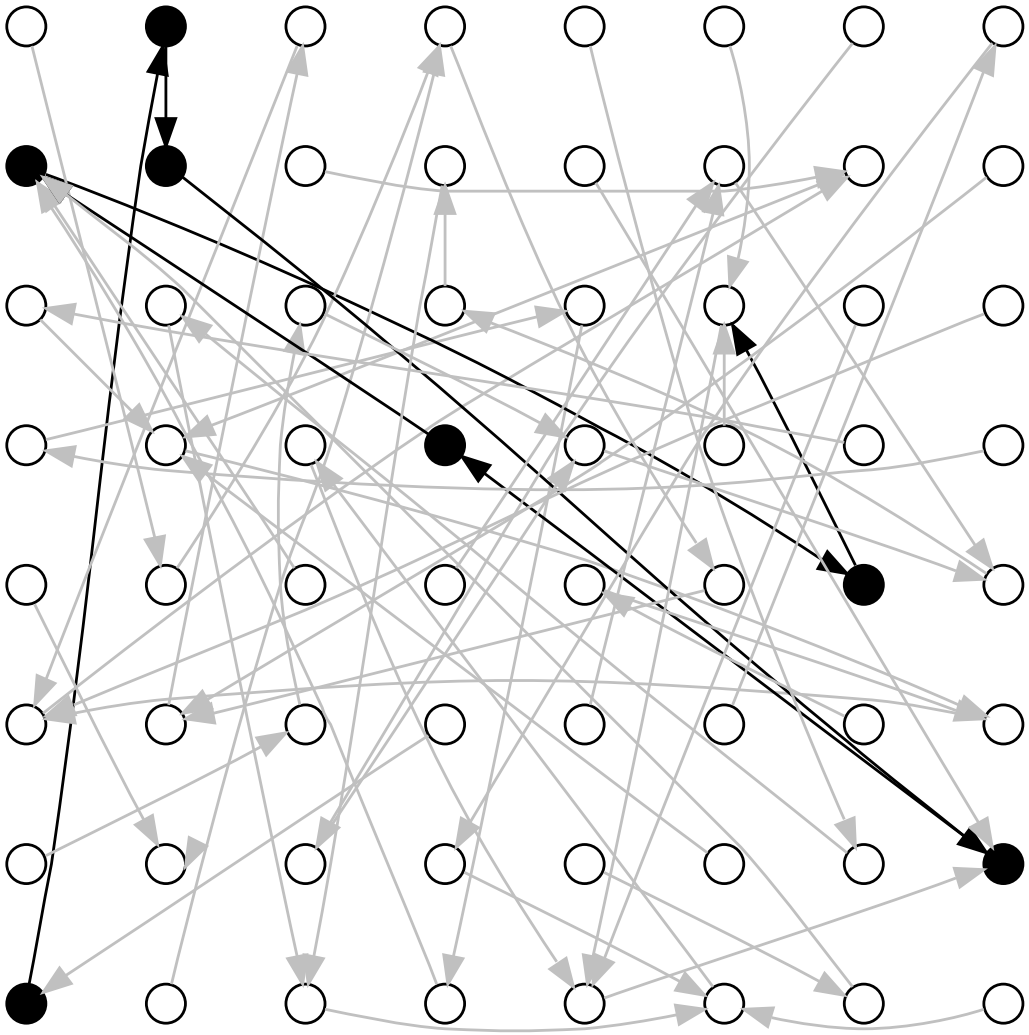
Random walks have collisions



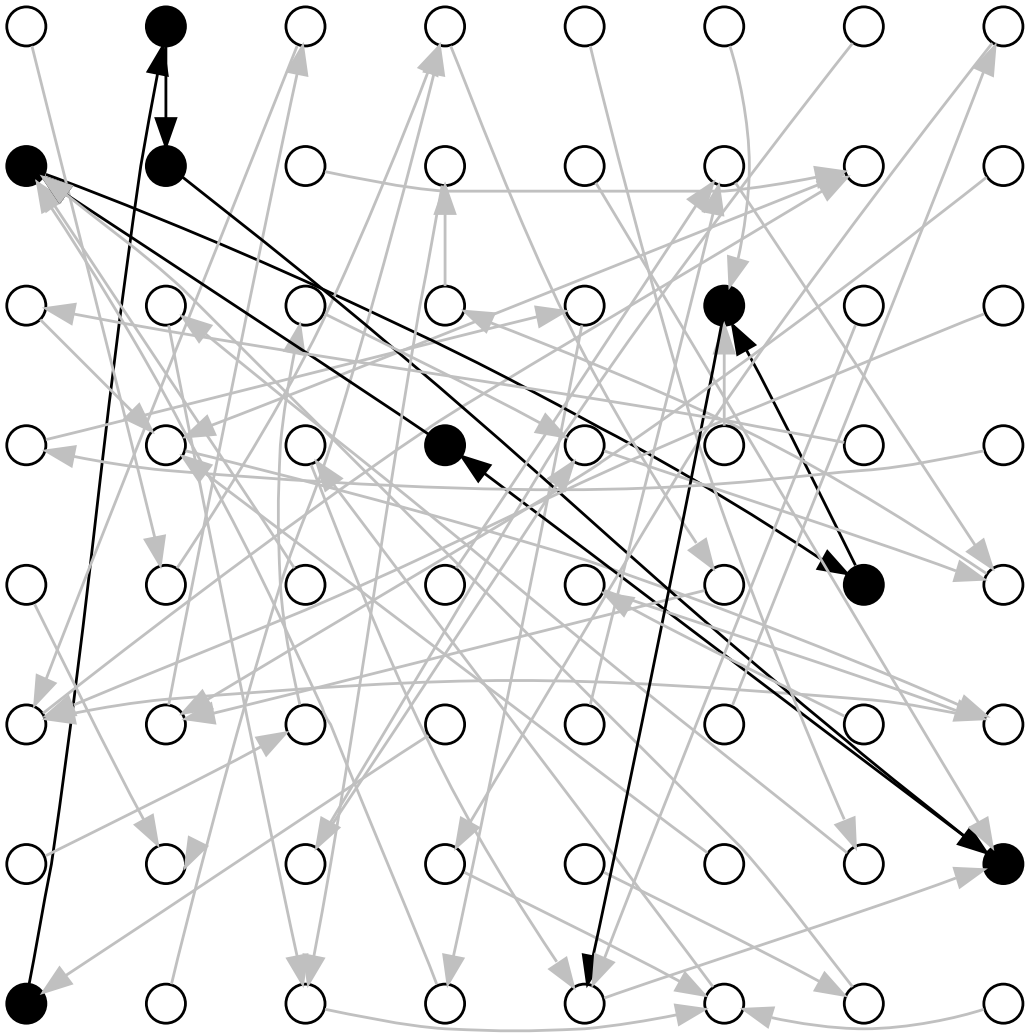
Random walks have collisions



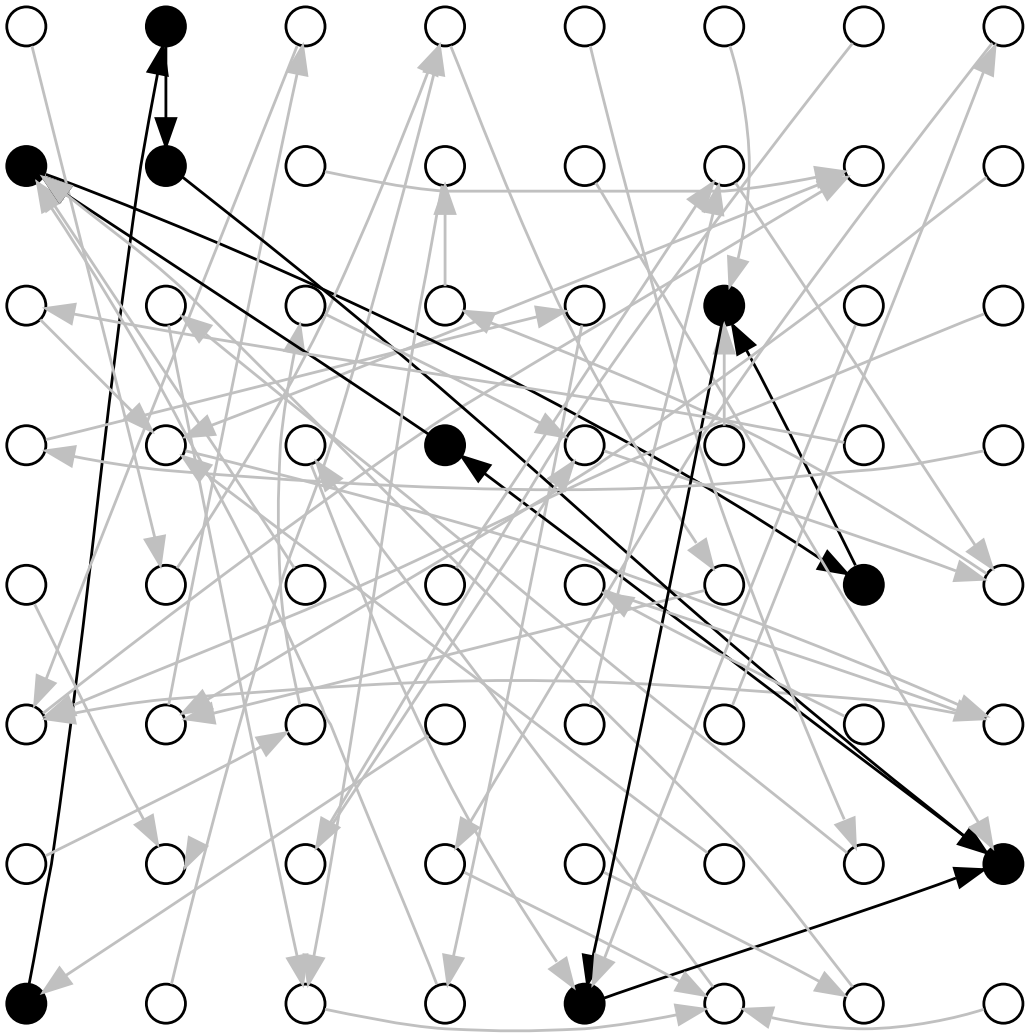
Random walks have collisions



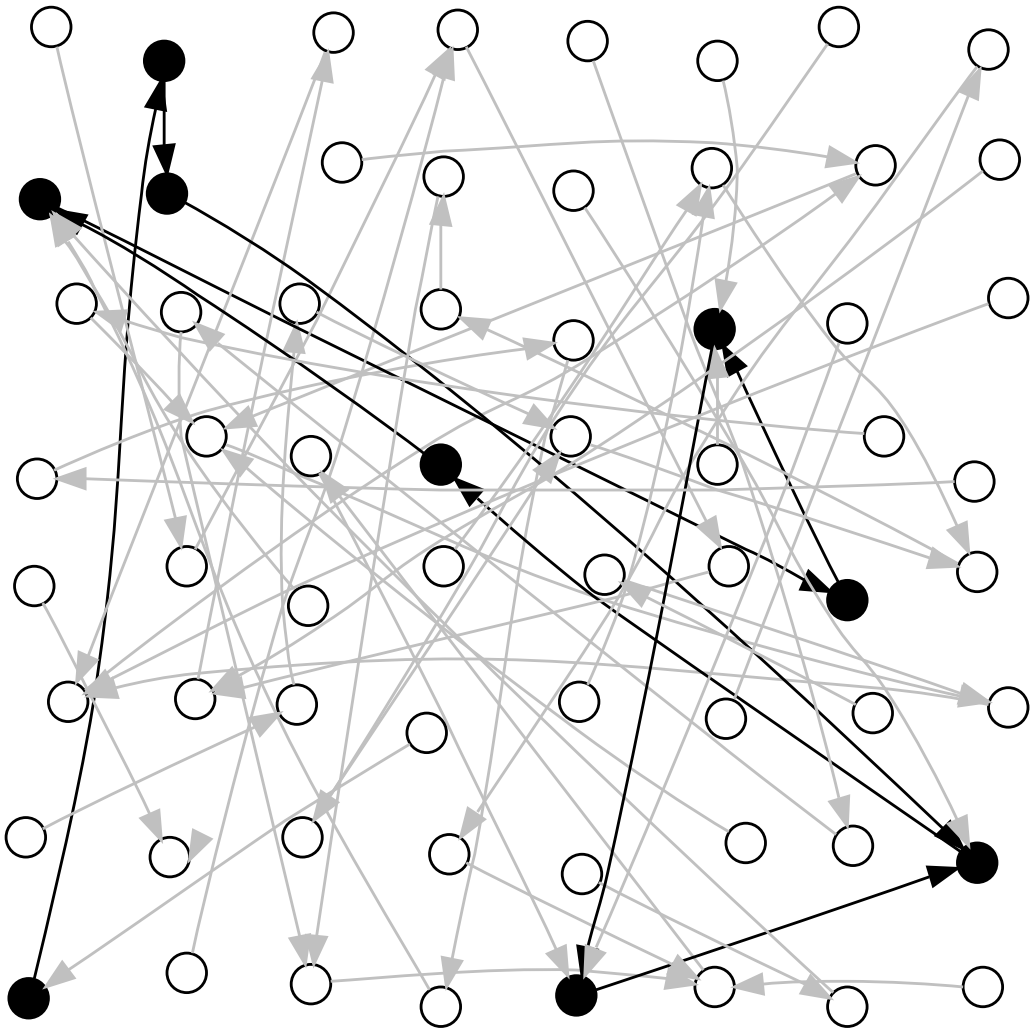
Random walks have collisions



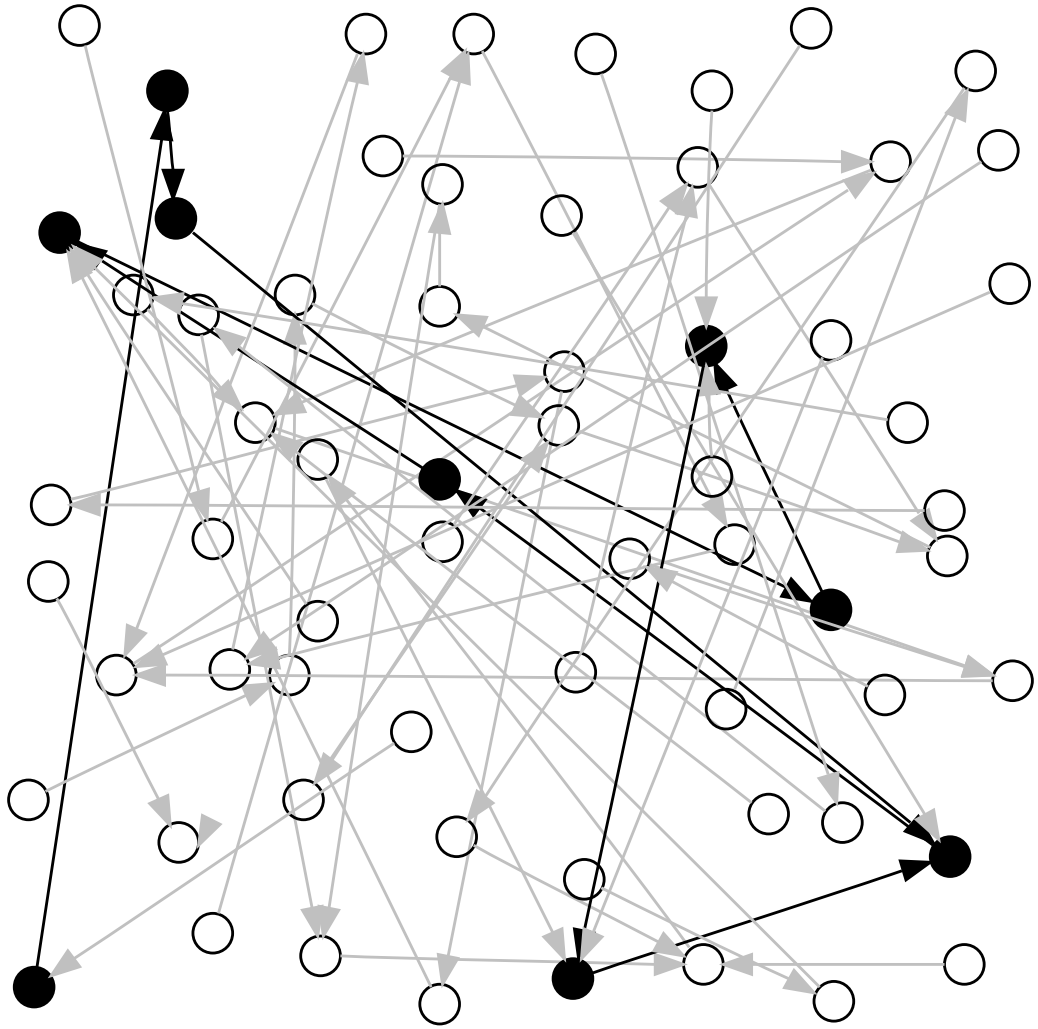
Random walks have collisions



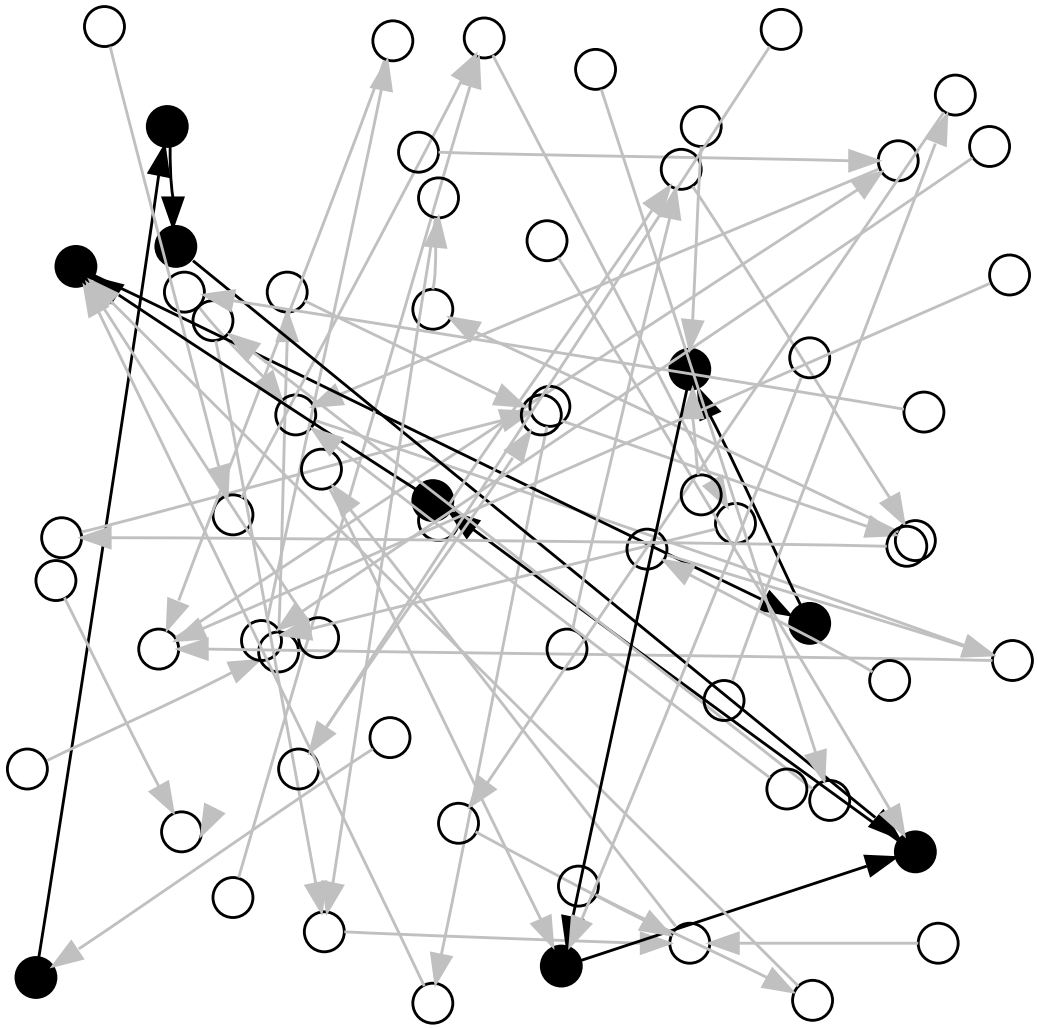
Random walks have collisions



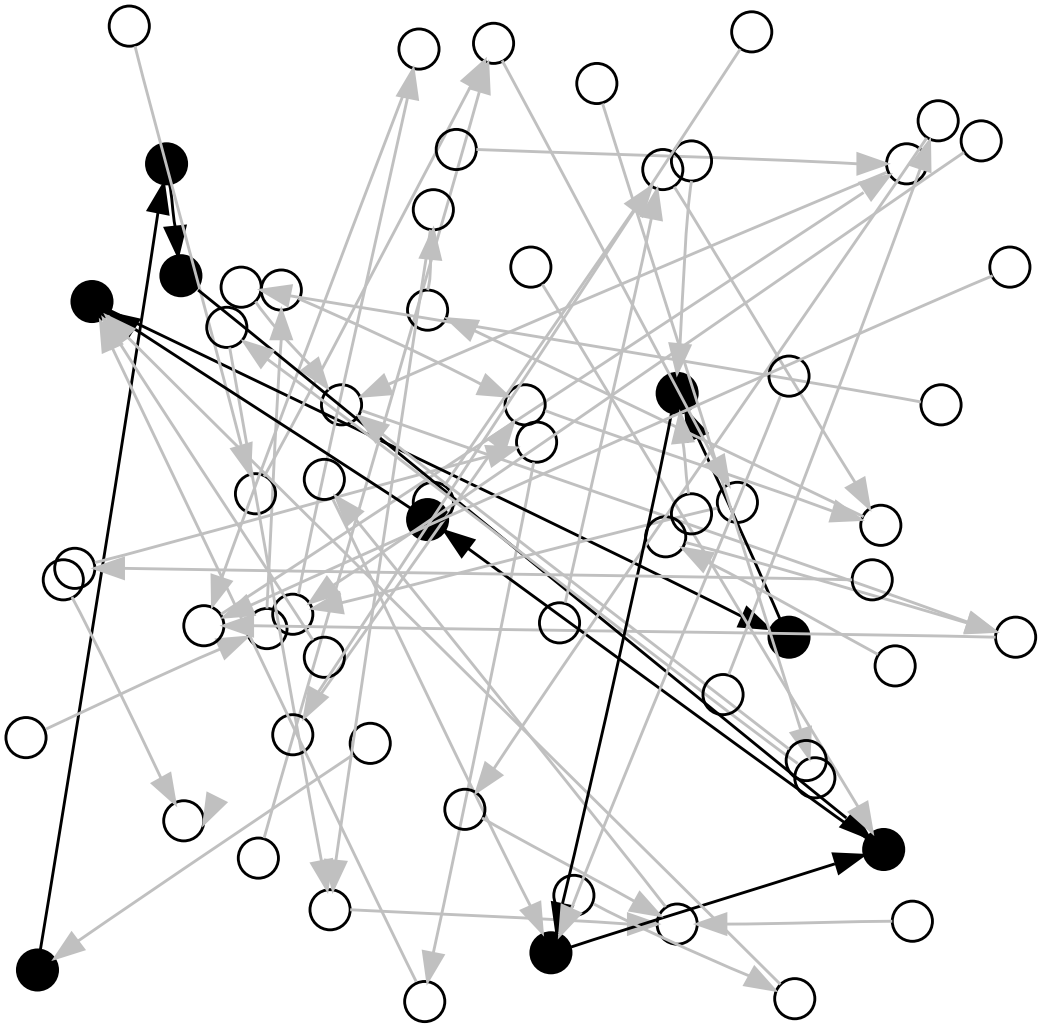
Random walks have collisions



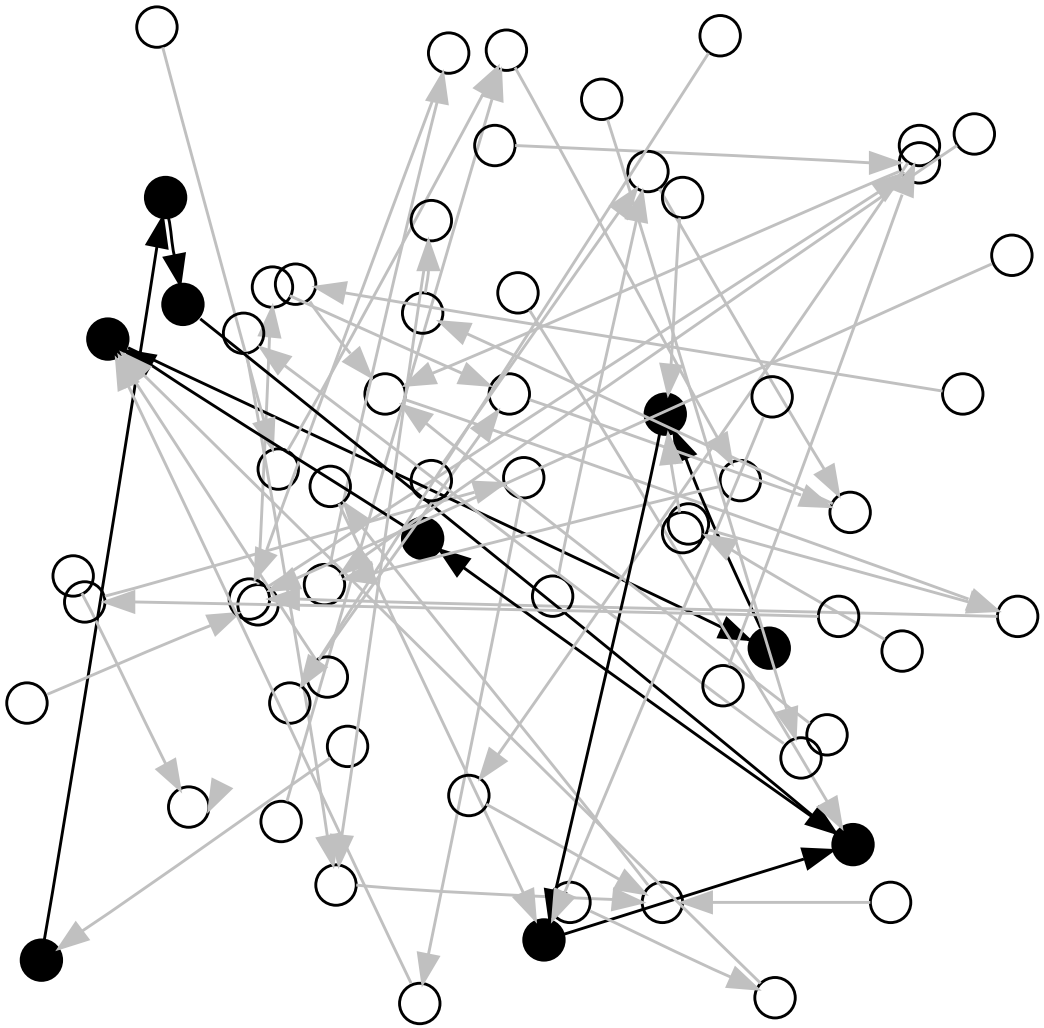
Random walks have collisions



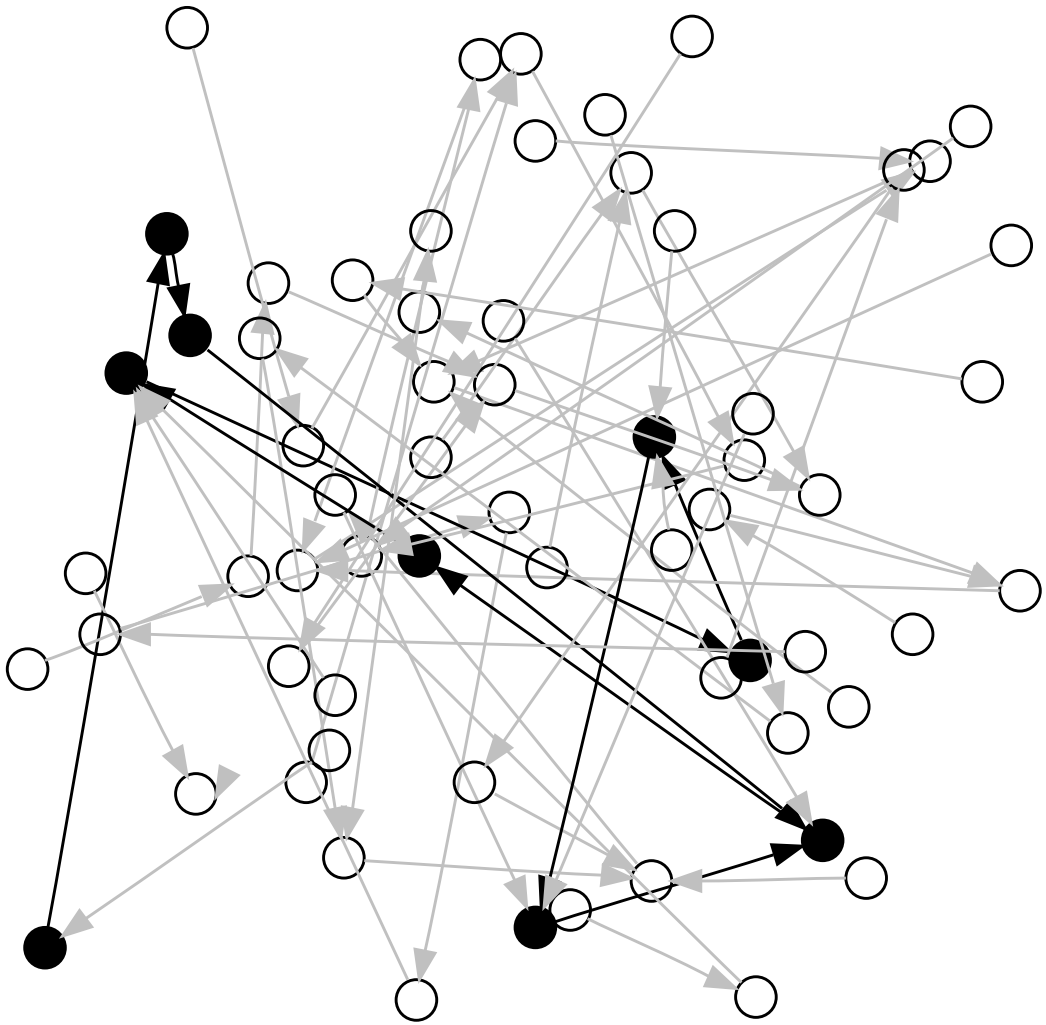
Random walks have collisions



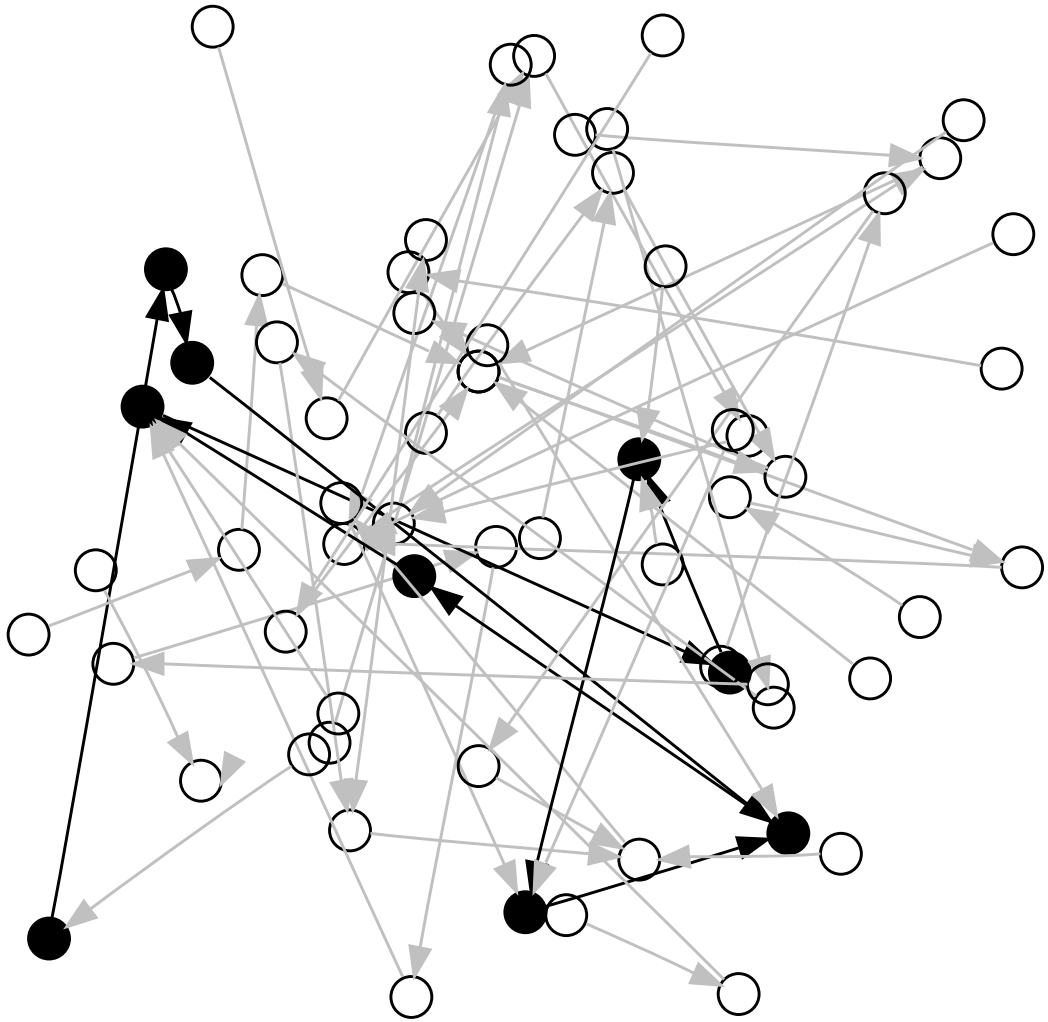
Random walks have collisions



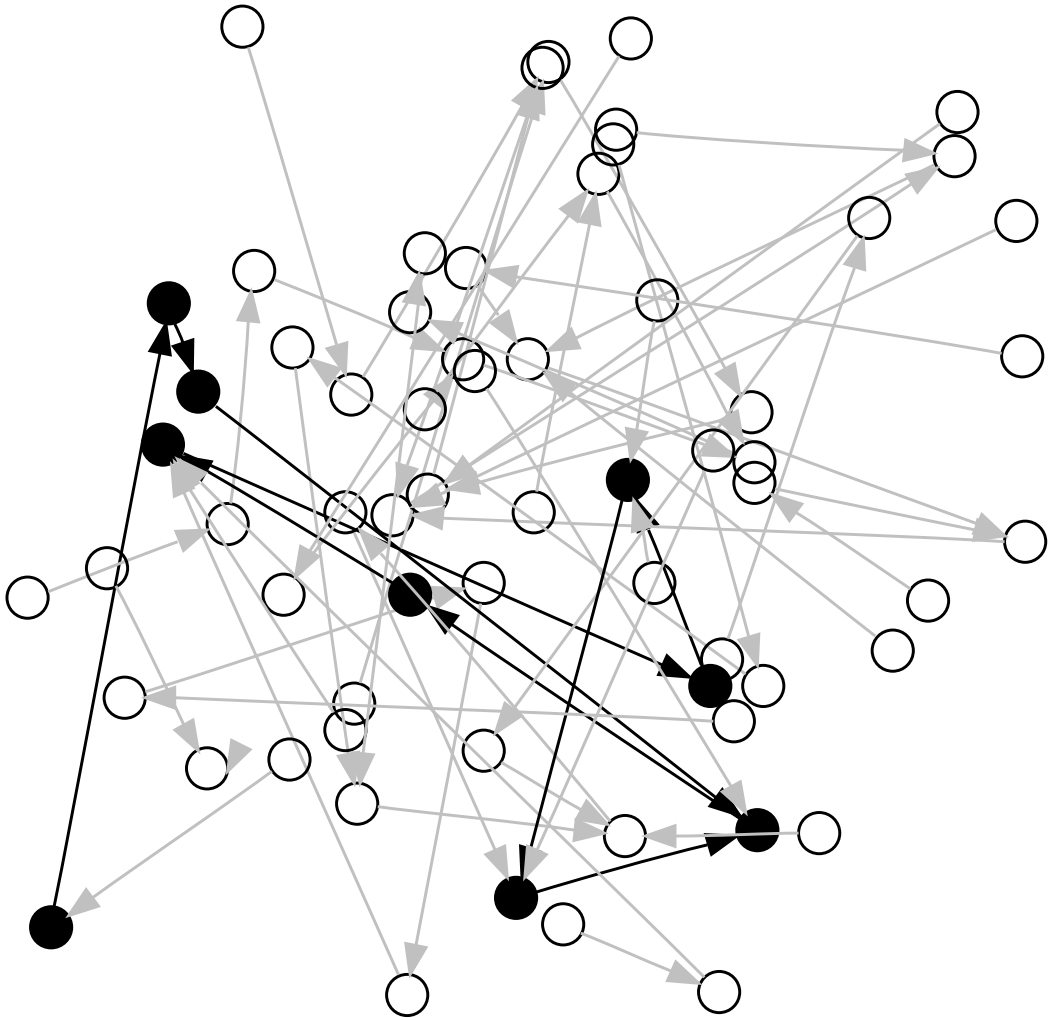
Random walks have collisions



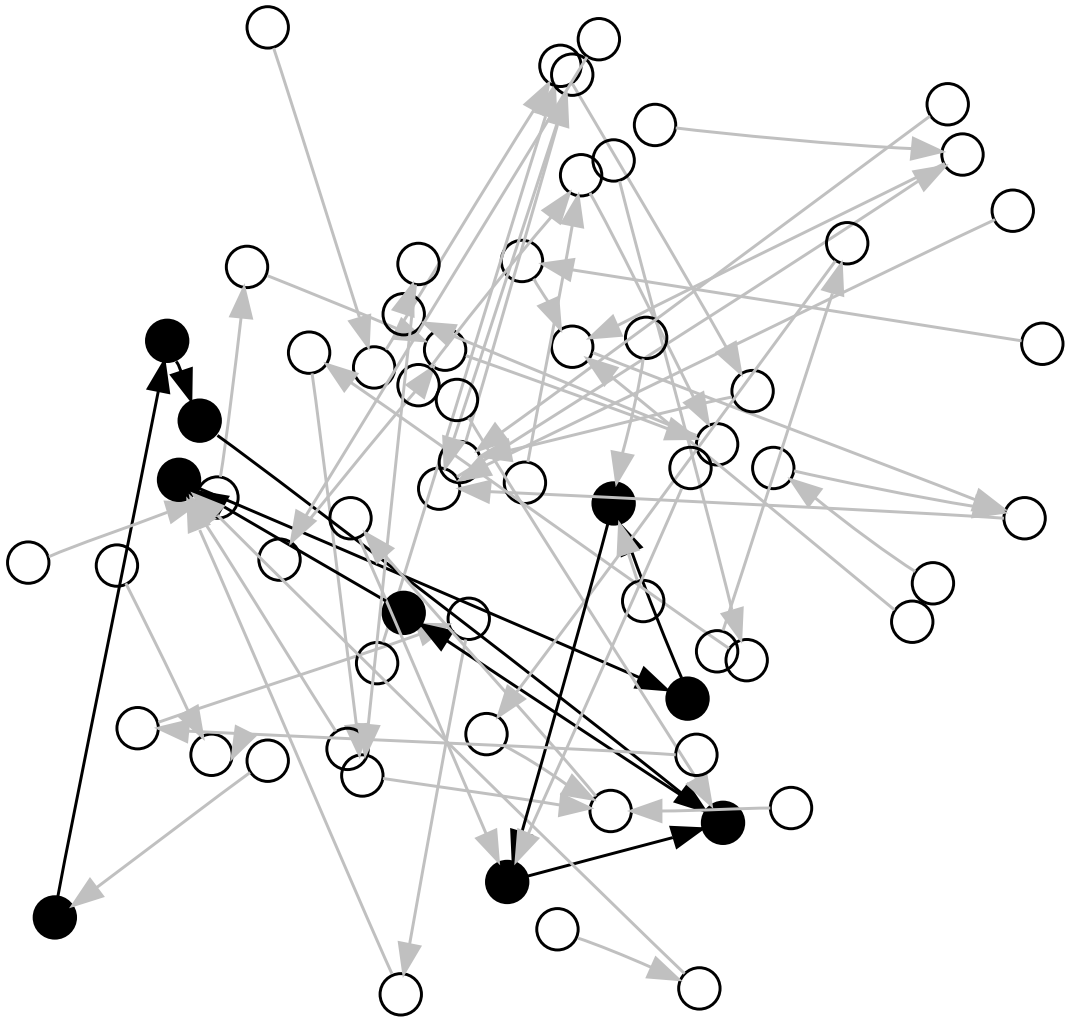
Random walks have collisions



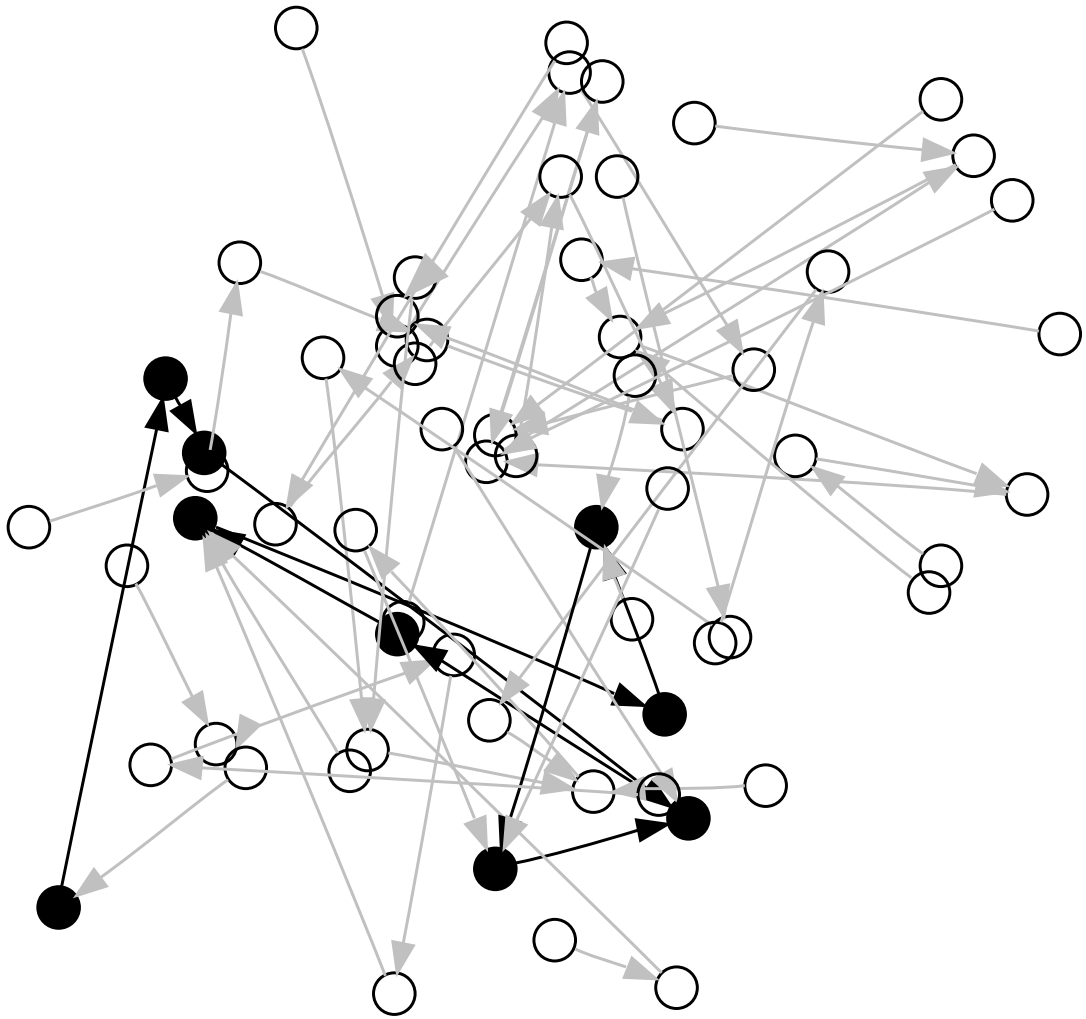
Random walks have collisions



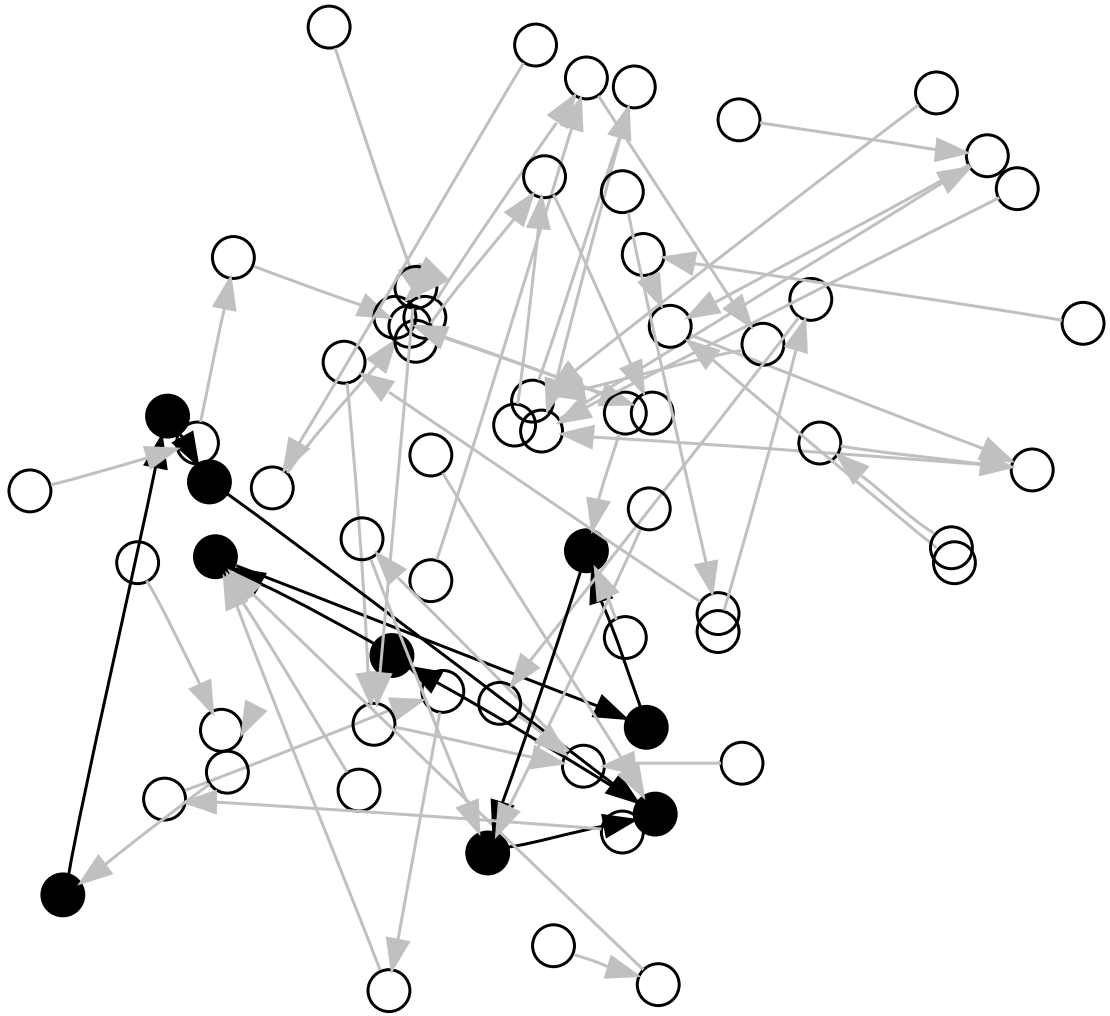
Random walks have collisions



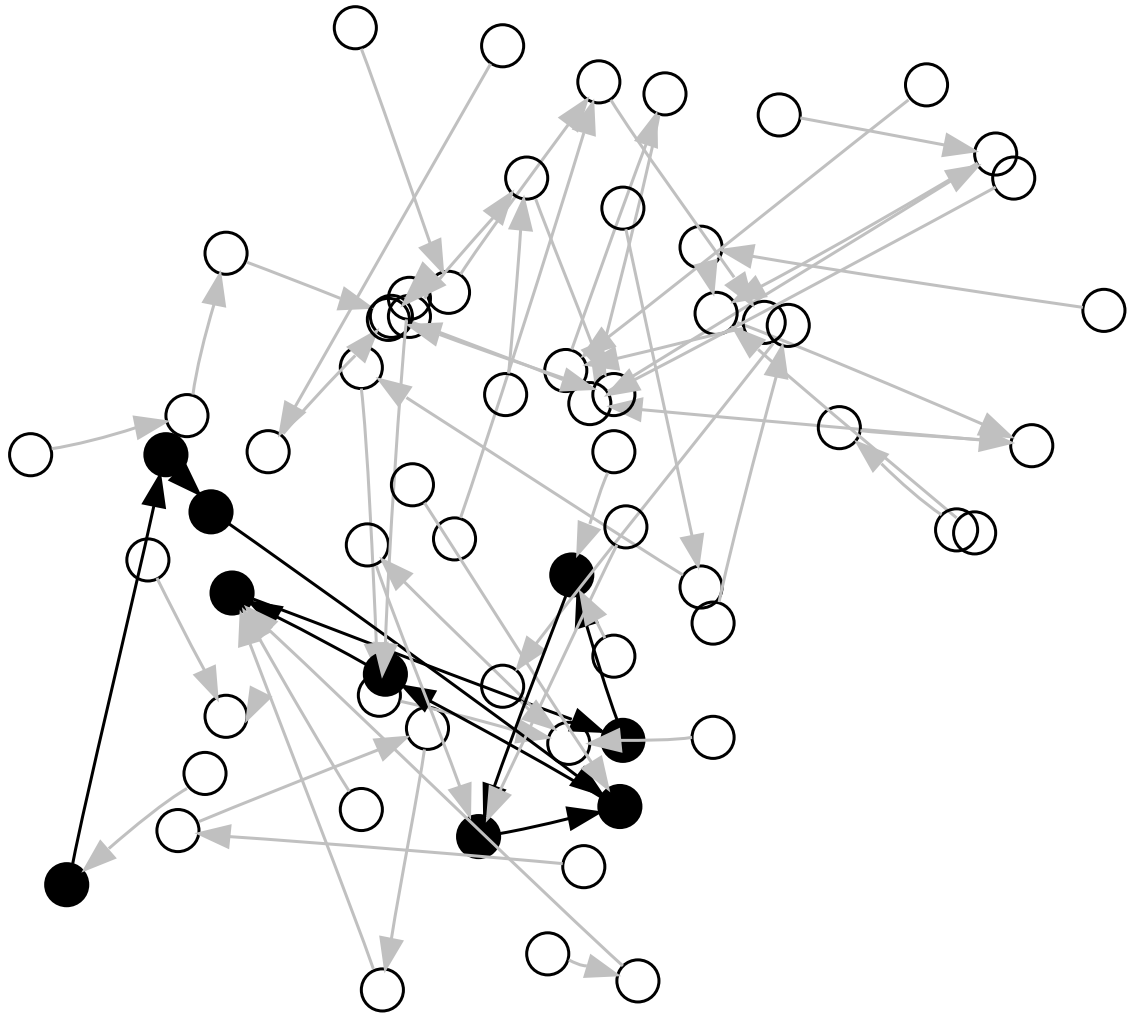
Random walks have collisions



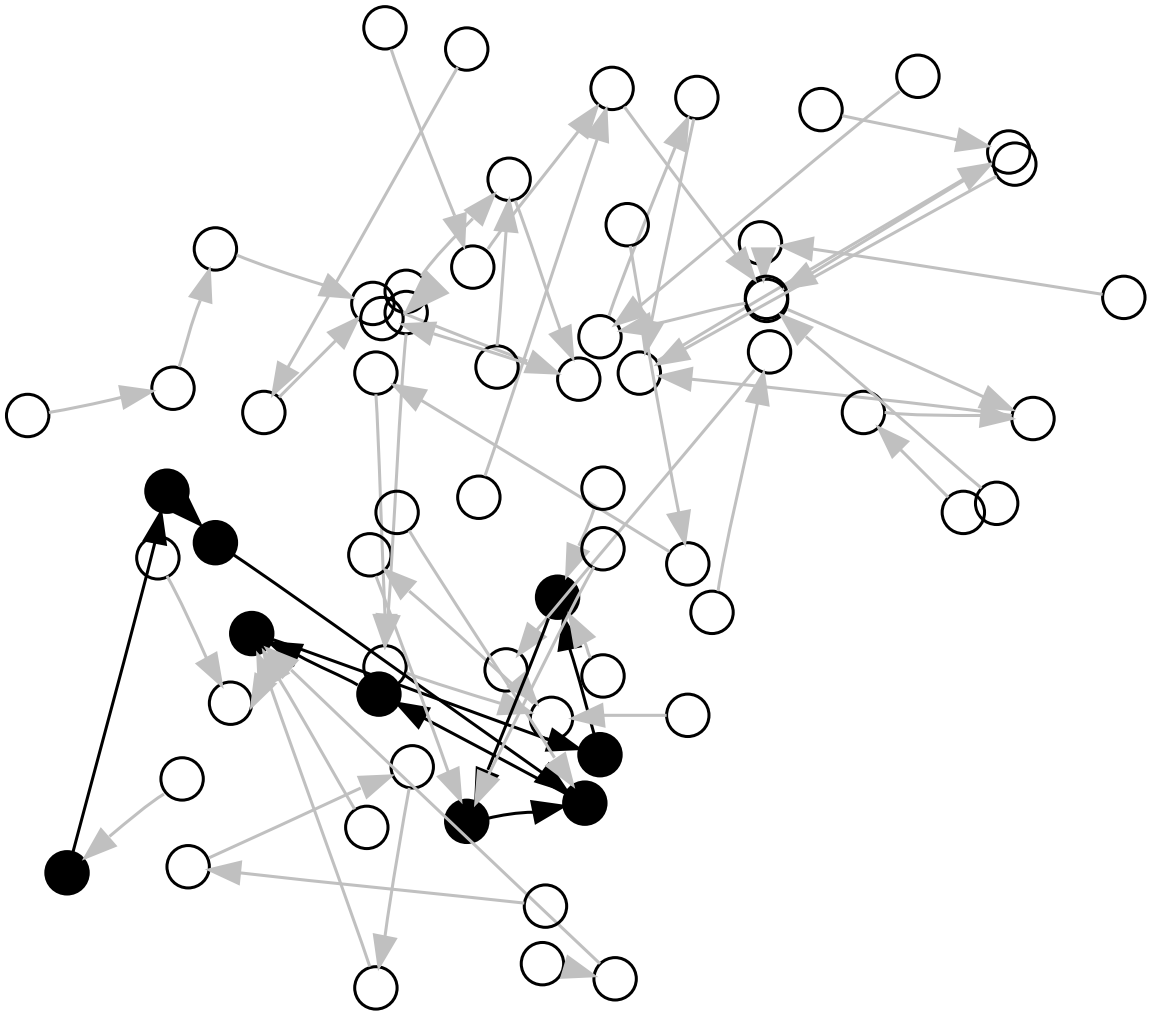
Random walks have collisions



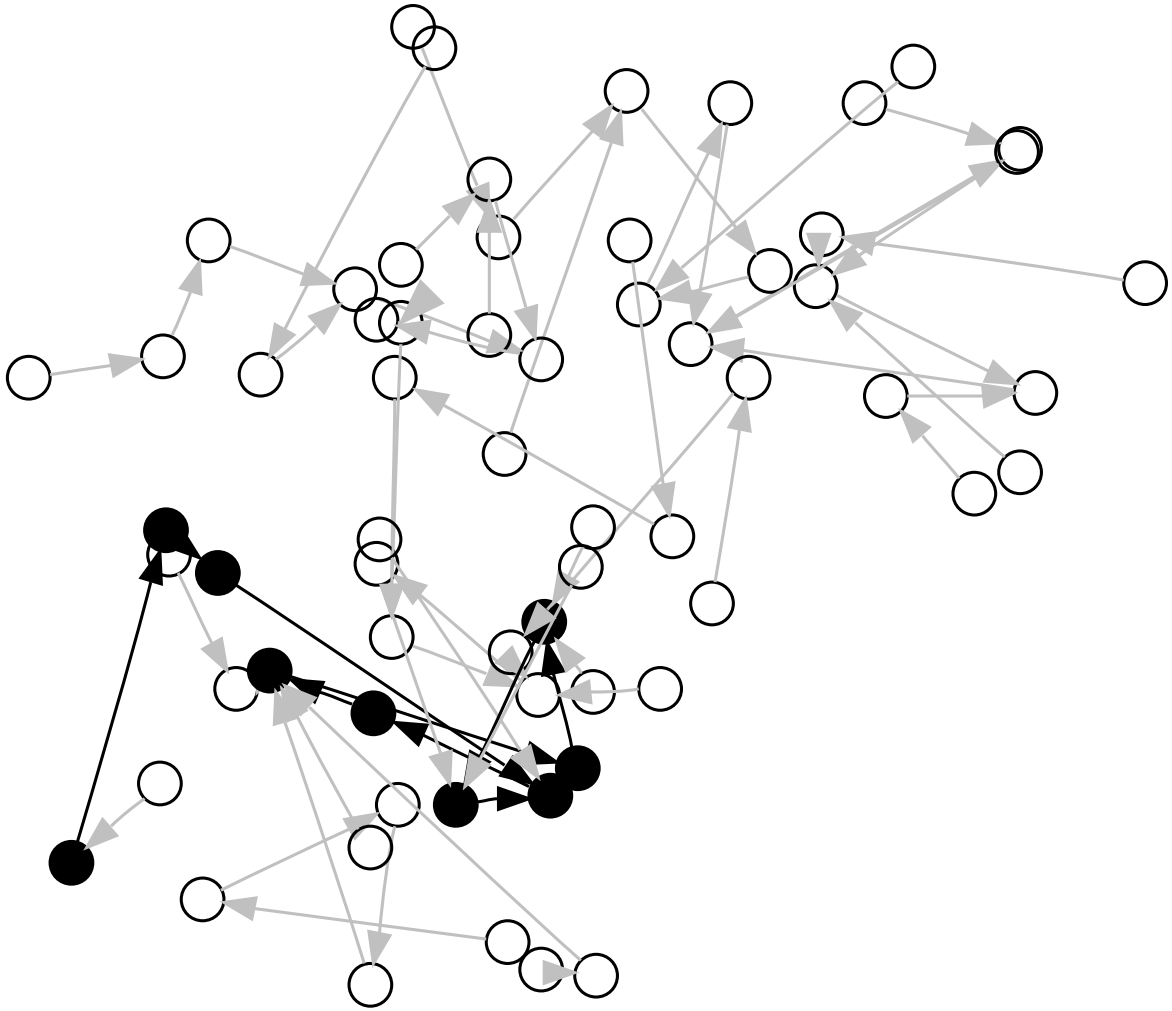
Random walks have collisions



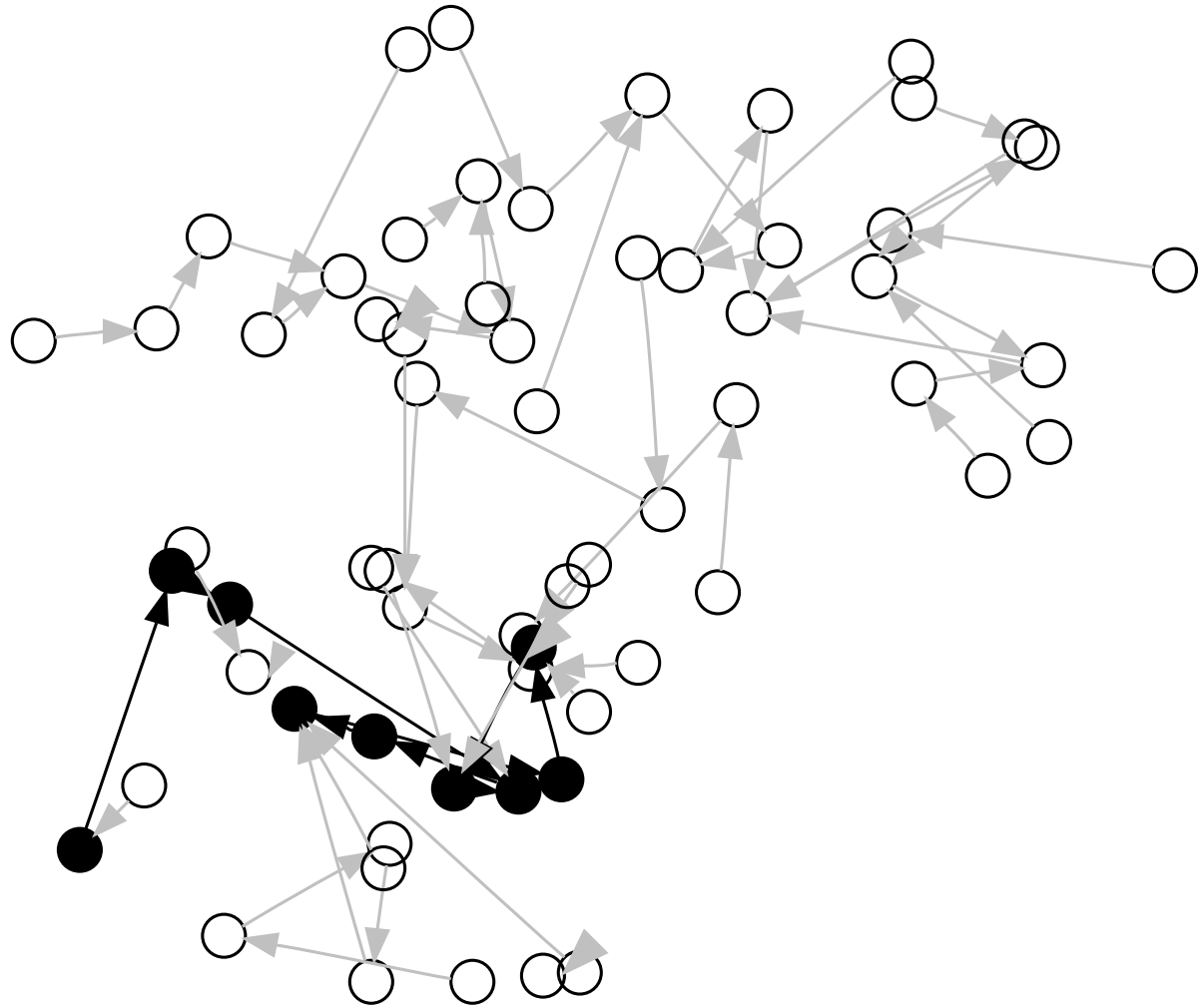
Random walks have collisions



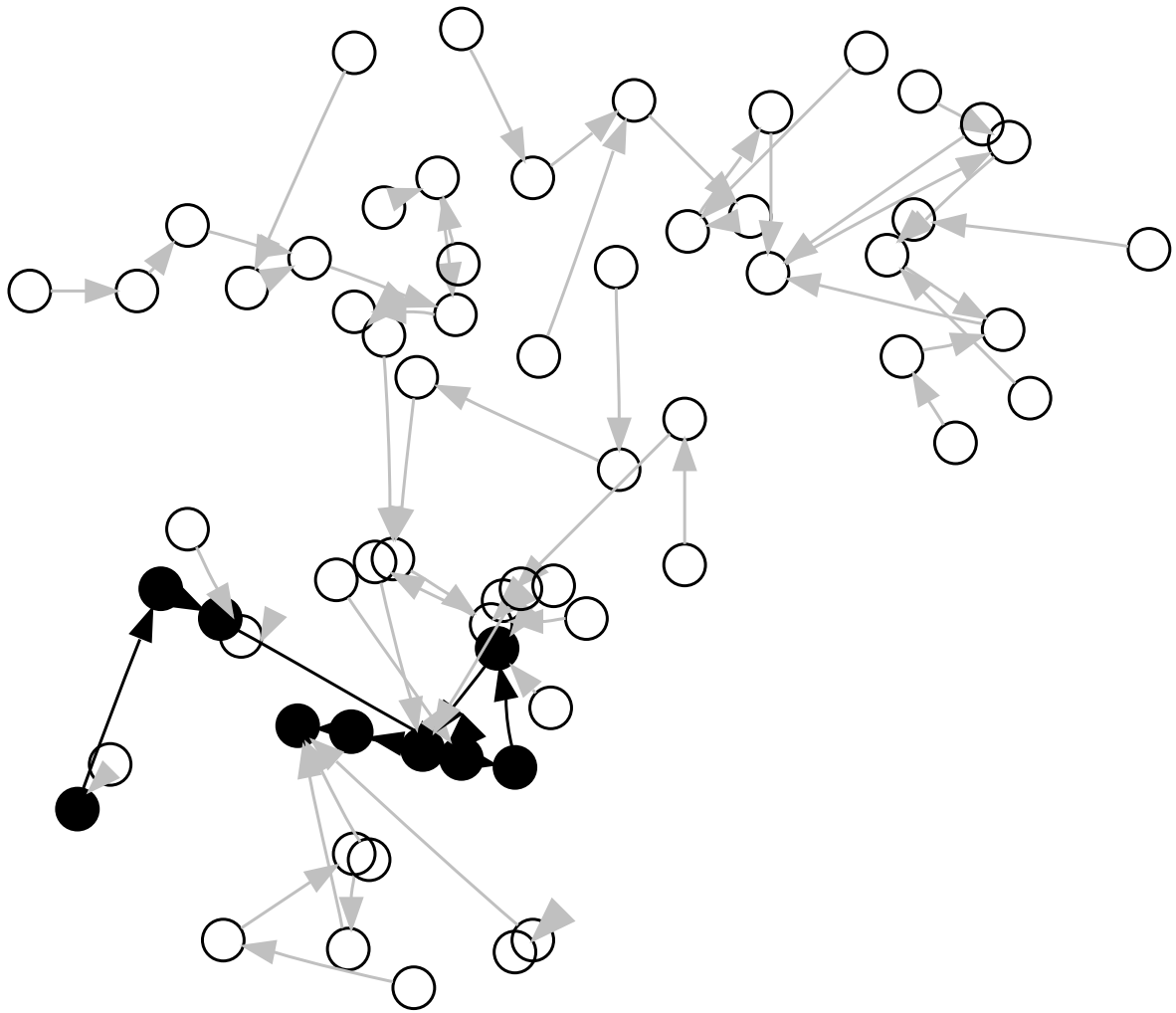
Random walks have collisions



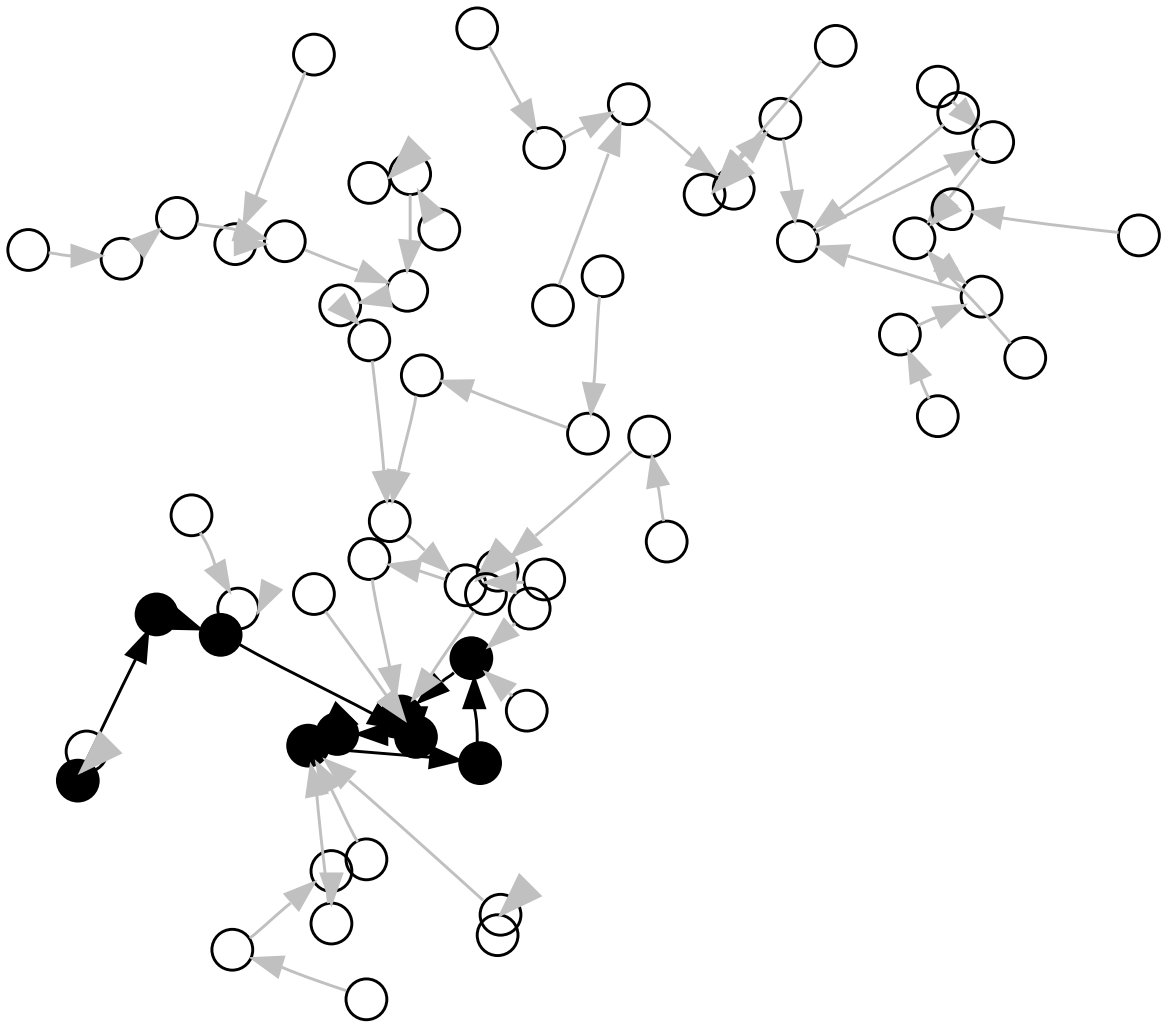
Random walks have collisions



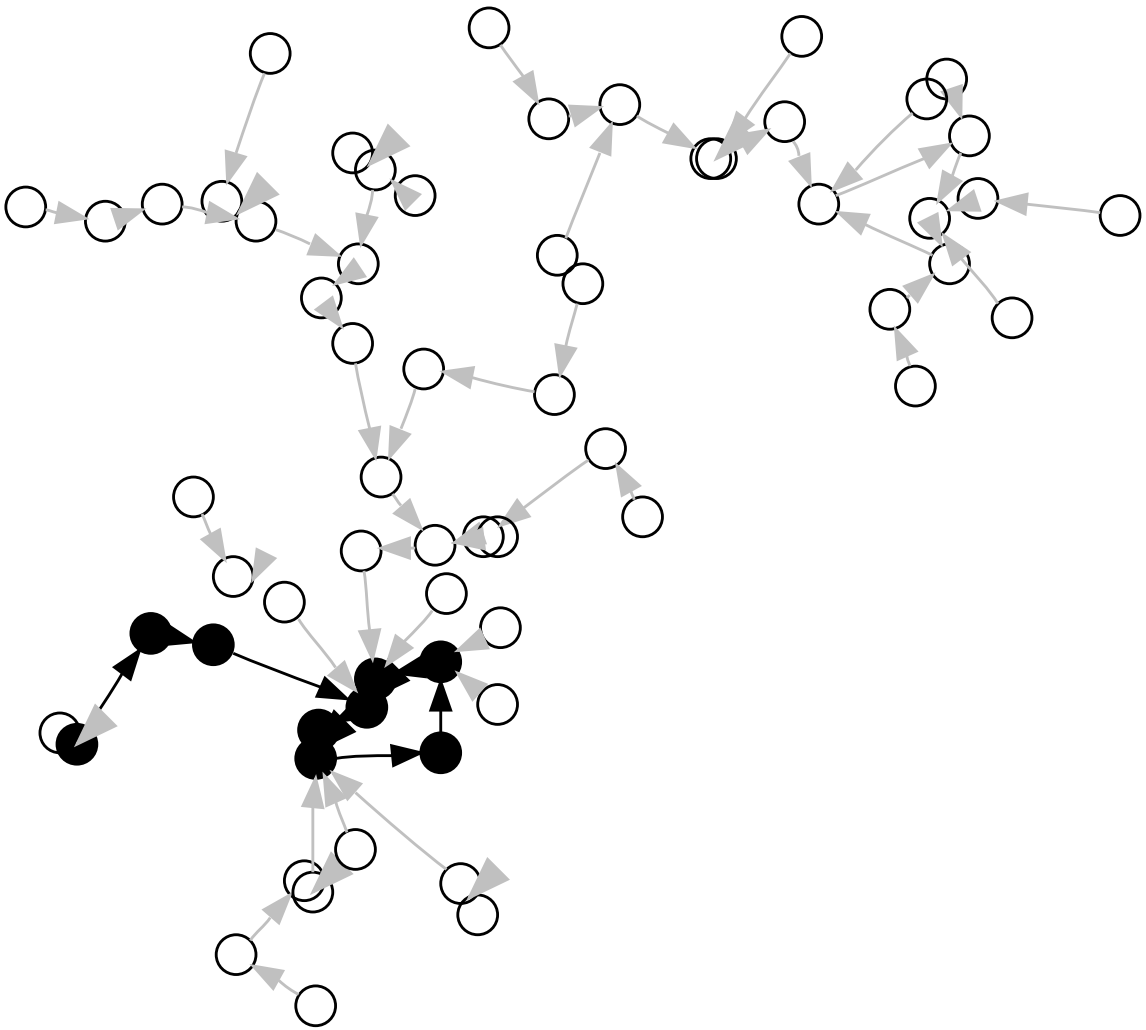
Random walks have collisions



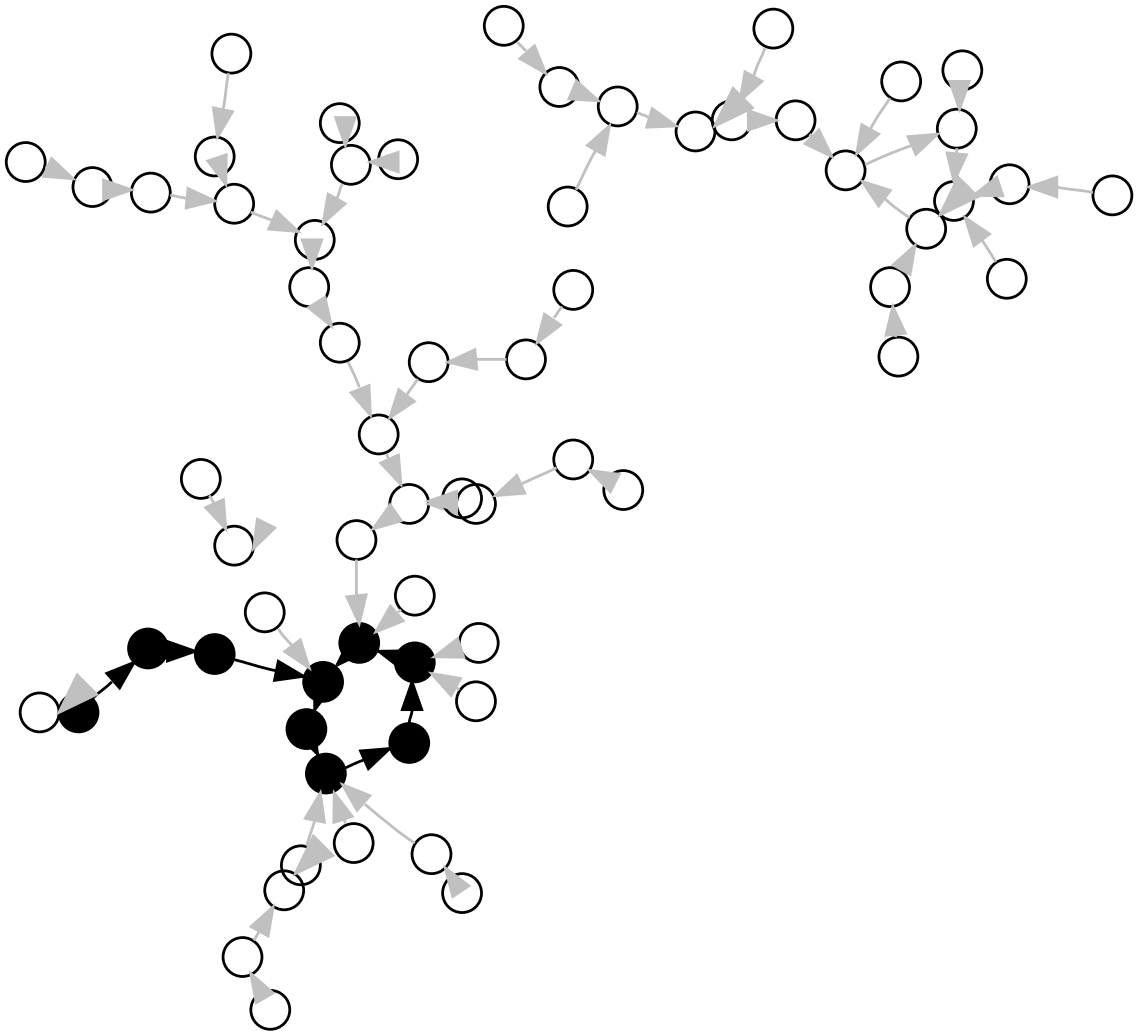
Random walks have collisions



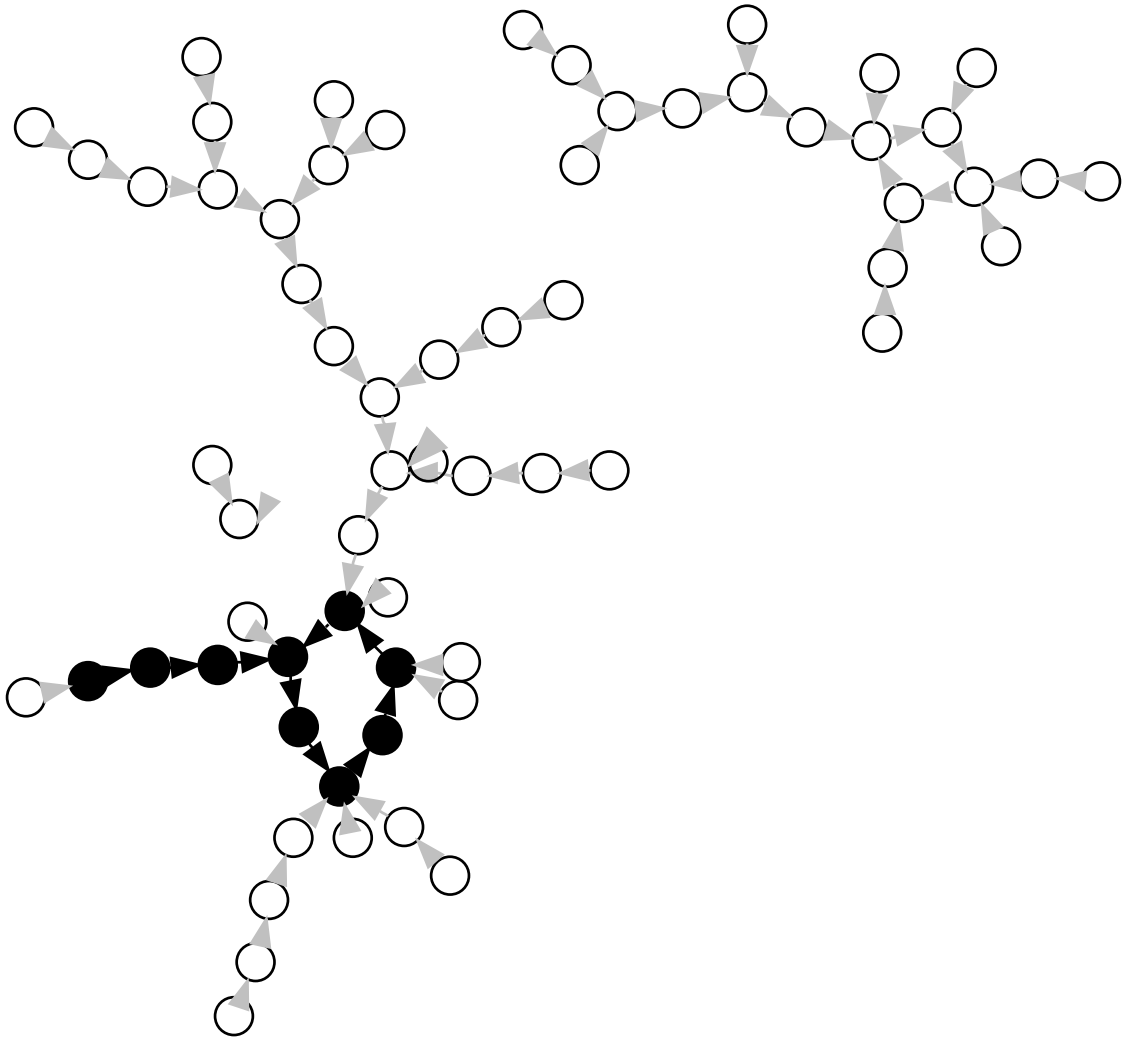
Random walks have collisions



Random walks have collisions



Random walks have collisions

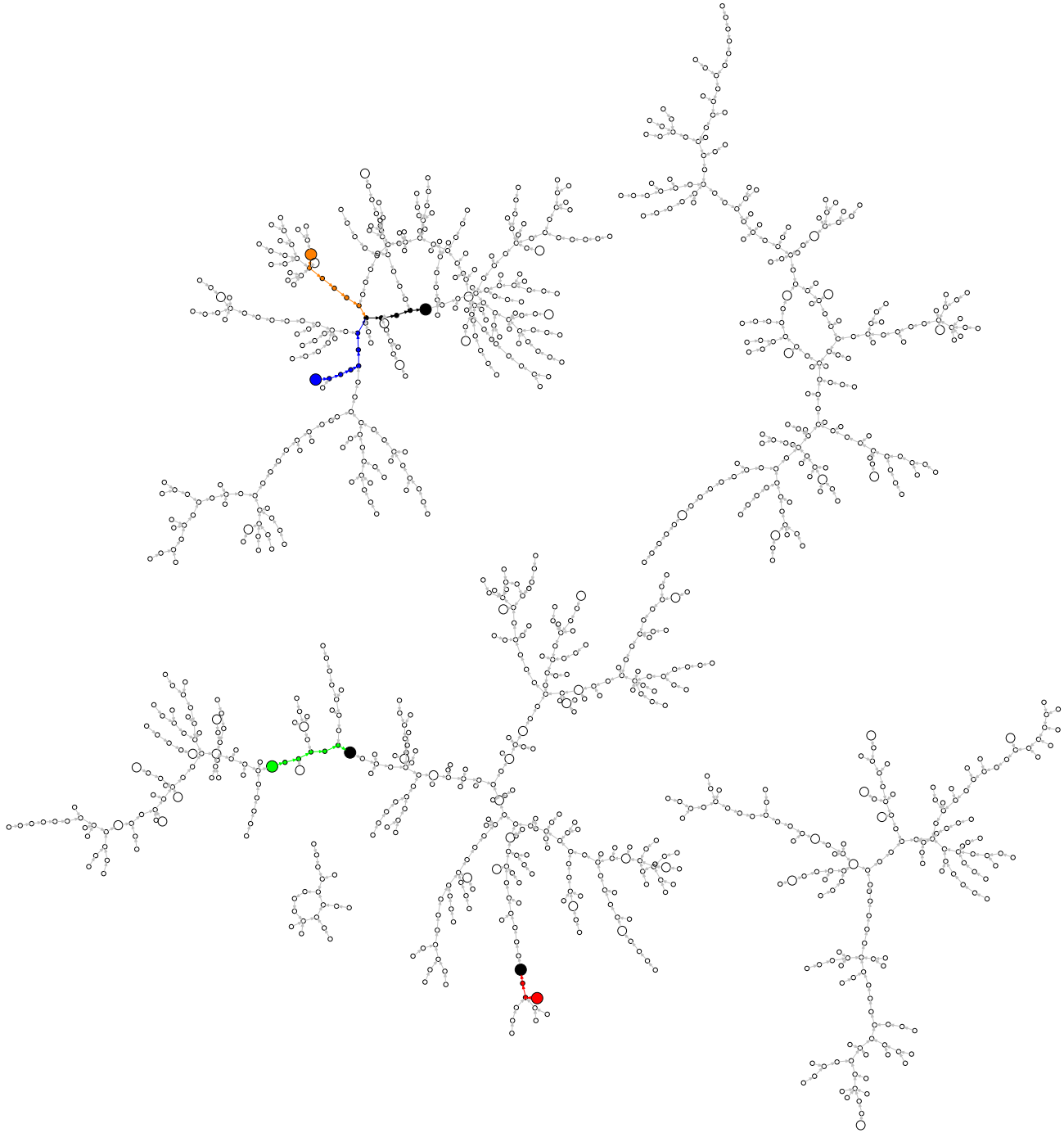


For random mappings:

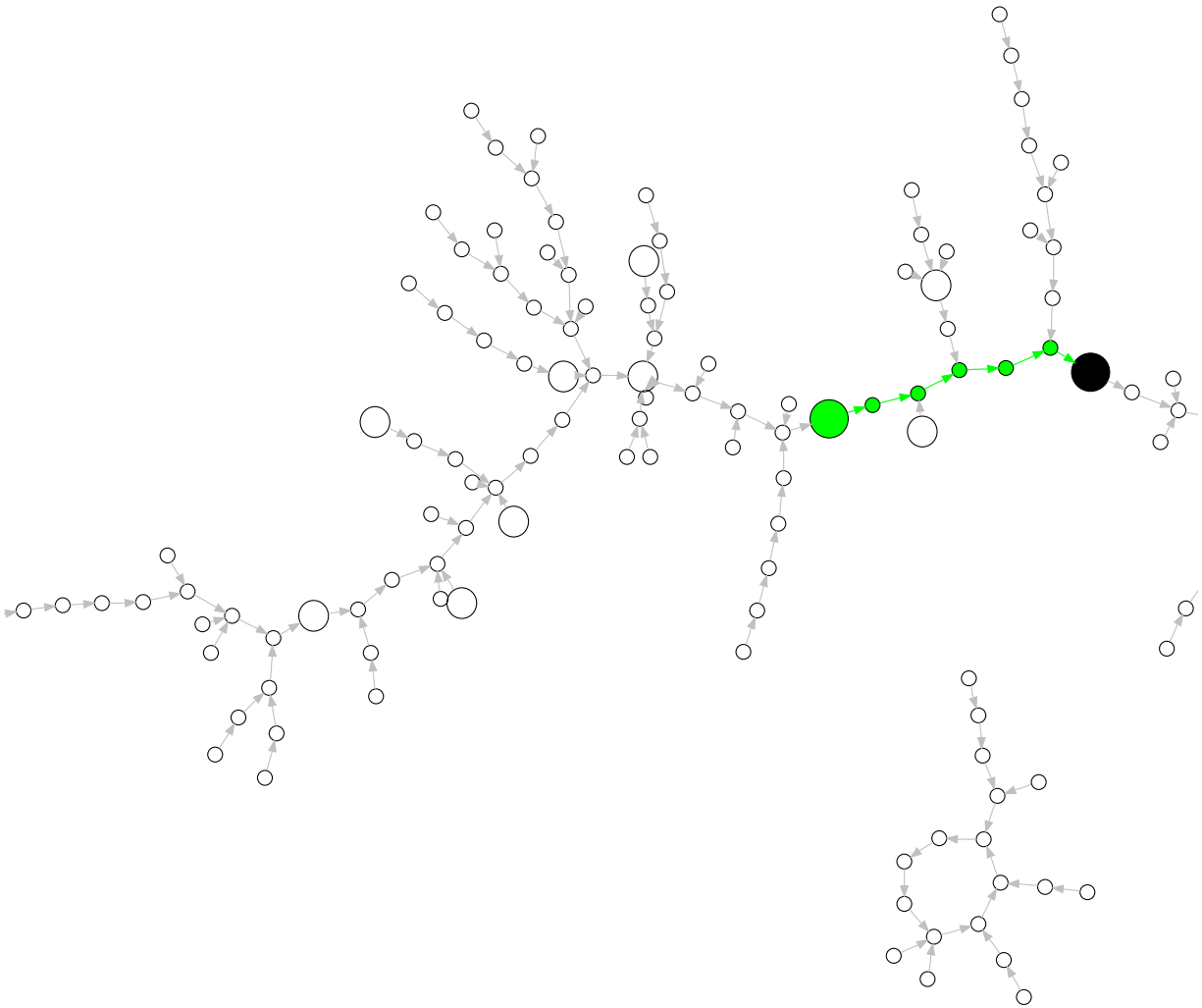
Tail length: $\sqrt{\pi n/8}$

Cycle length: $\sqrt{\pi n/8}$

See Flajolet & Odlyzko URL.



Walk to distinguished point, report to some server



Lucky case: two walks end in same distinguished point