How To Select its Parents in the Tangle

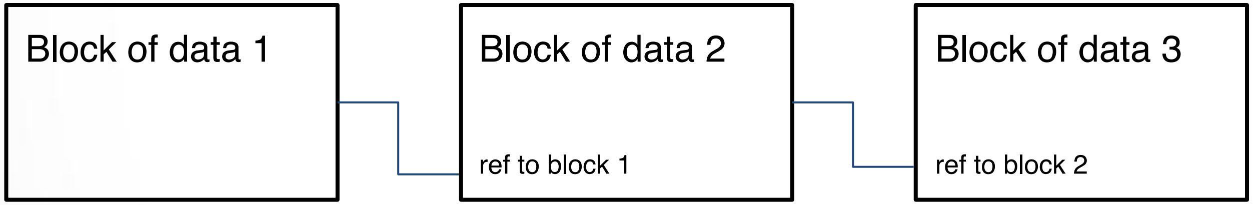
Vidal Attias, Quentin Bramas

bramas@unistra.fr

NETYS 2019, Marrakech, June, 21st

Introduction

Blockchain:



Block of data 1

Block of data 2

ref to block 1

Block of data 3

ref to block 2

The Tangle

The Tangle (IOTA)

The Tangle

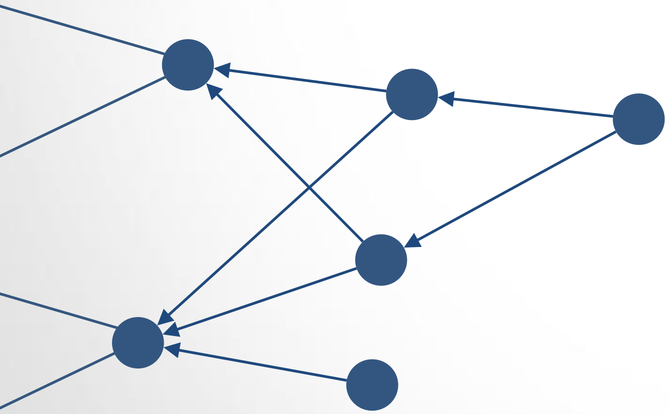
The Tangle (IOTA)

Each transaction is a small block that references two previous ones

The Tangle

The Tangle (IOTA)

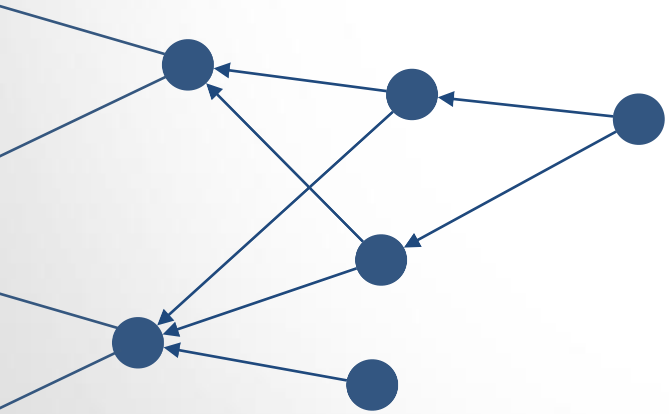
Each transaction is a small block that references two previous ones



The Tangle

The Tangle (IOTA)

Each transaction is a small block that references two previous ones

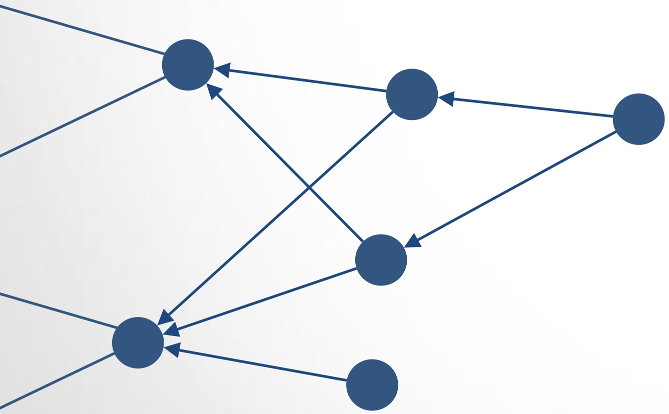


You come up with a DAG
(Directed Acyclic Graph)

The Tangle

The Tangle (IOTA)

Each transaction is a small block that references two previous ones



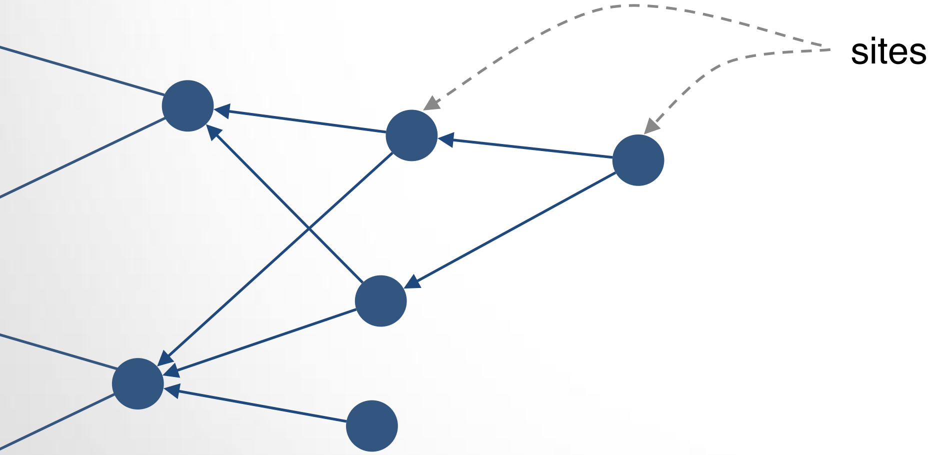
You come up with a DAG
(Directed Acyclic Graph)

You're only limited by bandwidth and storage

The Tangle

The Tangle (IOTA)

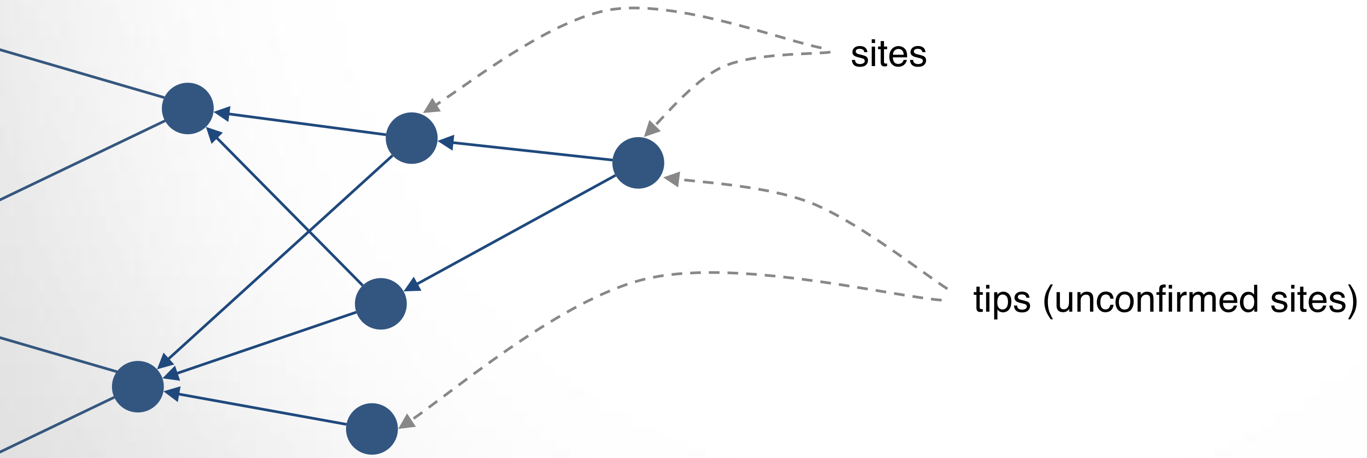
Each transaction is a small block that reference two previous ones



The Tangle

The Tangle (IOTA)

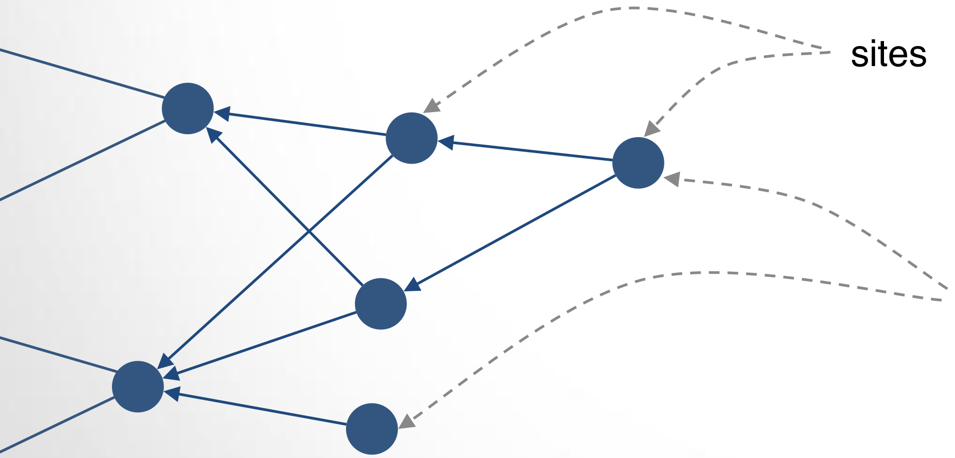
Each transaction is a small block that reference two previous ones



The Tangle

The Tangle (IOTA)

Each transaction is a small block that reference two previous ones



sites

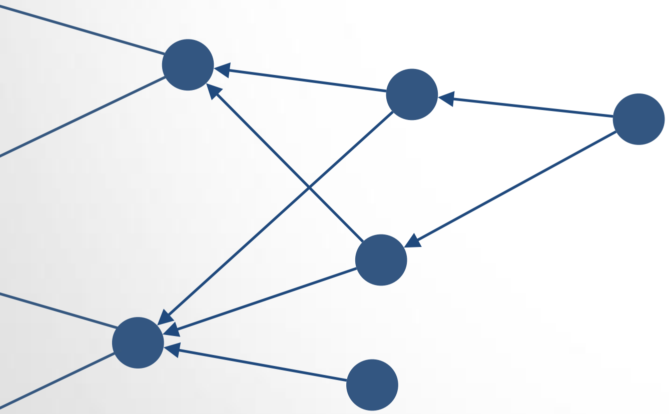
tips (unconfirmed sites)

A new site and its parents should not create conflicts.

The Tangle

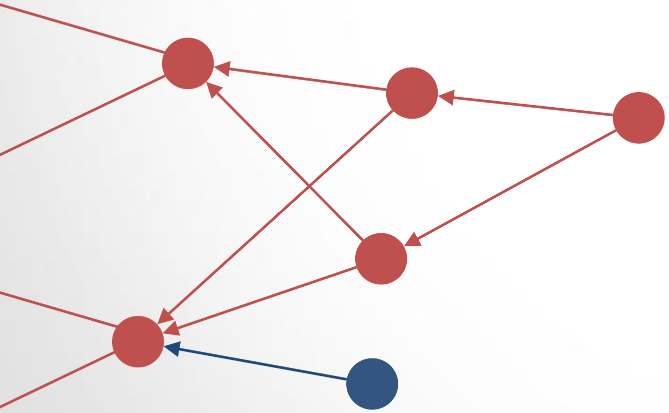
The Tangle (IOTA)

How to read a value?



The Tangle

The Tangle (IOTA)



How to read a value?

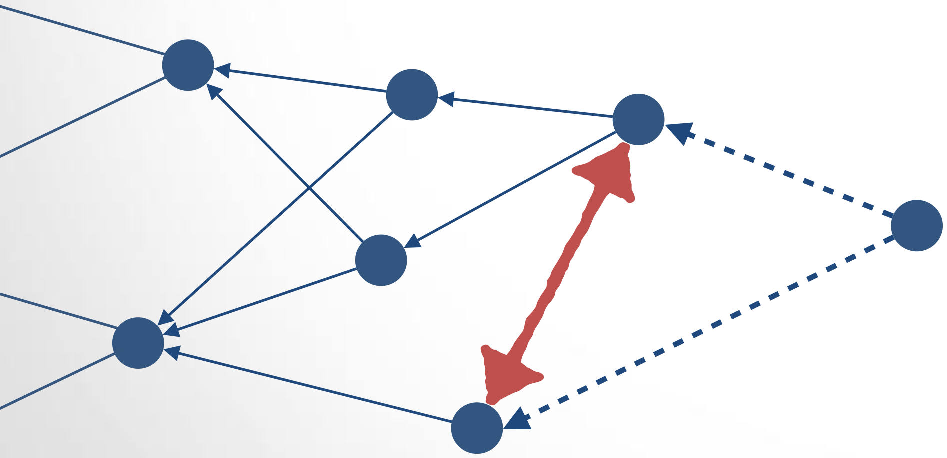
- If you take a tip, you can order transactions and do the same as in a blockchain

The Tangle

The Tangle (IOTA)

How to read a value?

What if tips are conflicting?



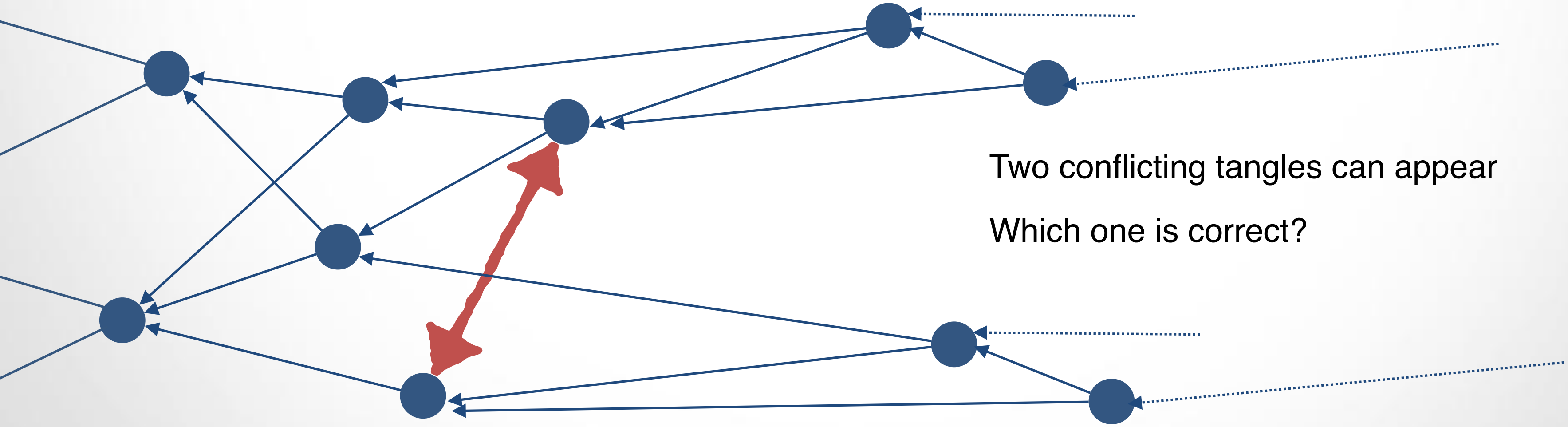
A new site cannot confirm conflicting sites

The Tangle

The Tangle (IOTA)

How to read a value?

What if tips are conflicting?

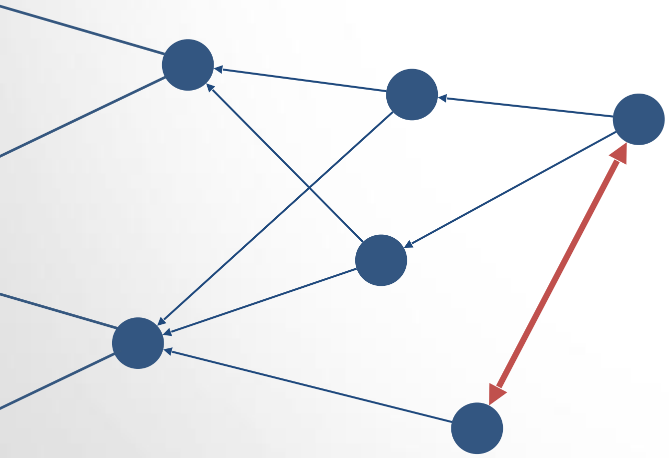


Two conflicting tangles can appear

Which one is correct?

The Tangle

The Tangle (IOTA)

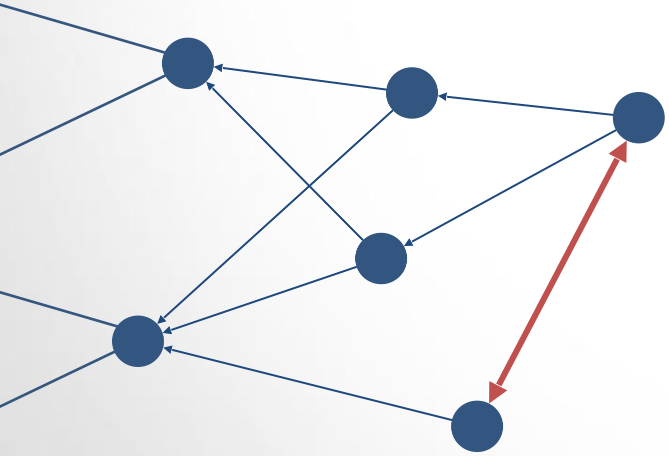


Tip Selection Algorithm (TSA):

- so we know how to read values
- so we know where to extend the Tangle

The Tangle

The Tangle (IOTA)



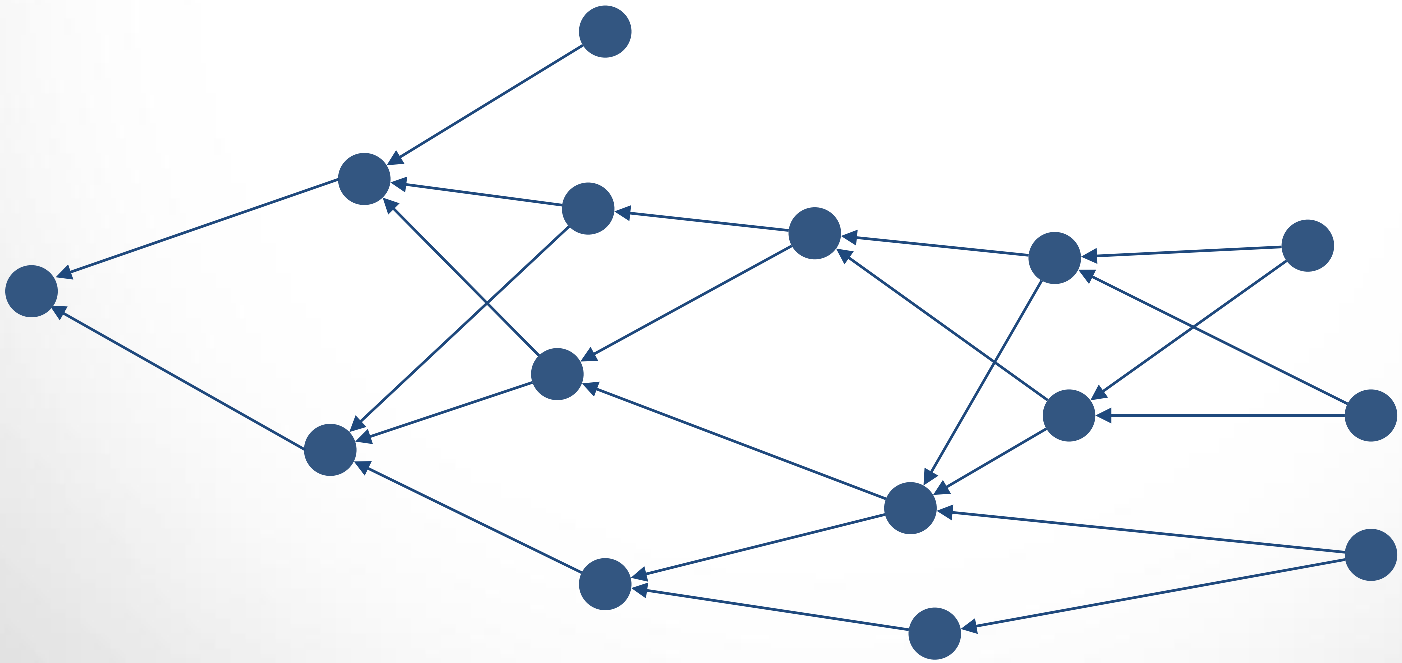
Tip Selection Algorithm (TSA):

- so we know how to read values
- so we know where to extend the Tangle

In Bitcoin, we read values from, and we try to extend, the longest chain. If you don't follow this, you'll lose money.

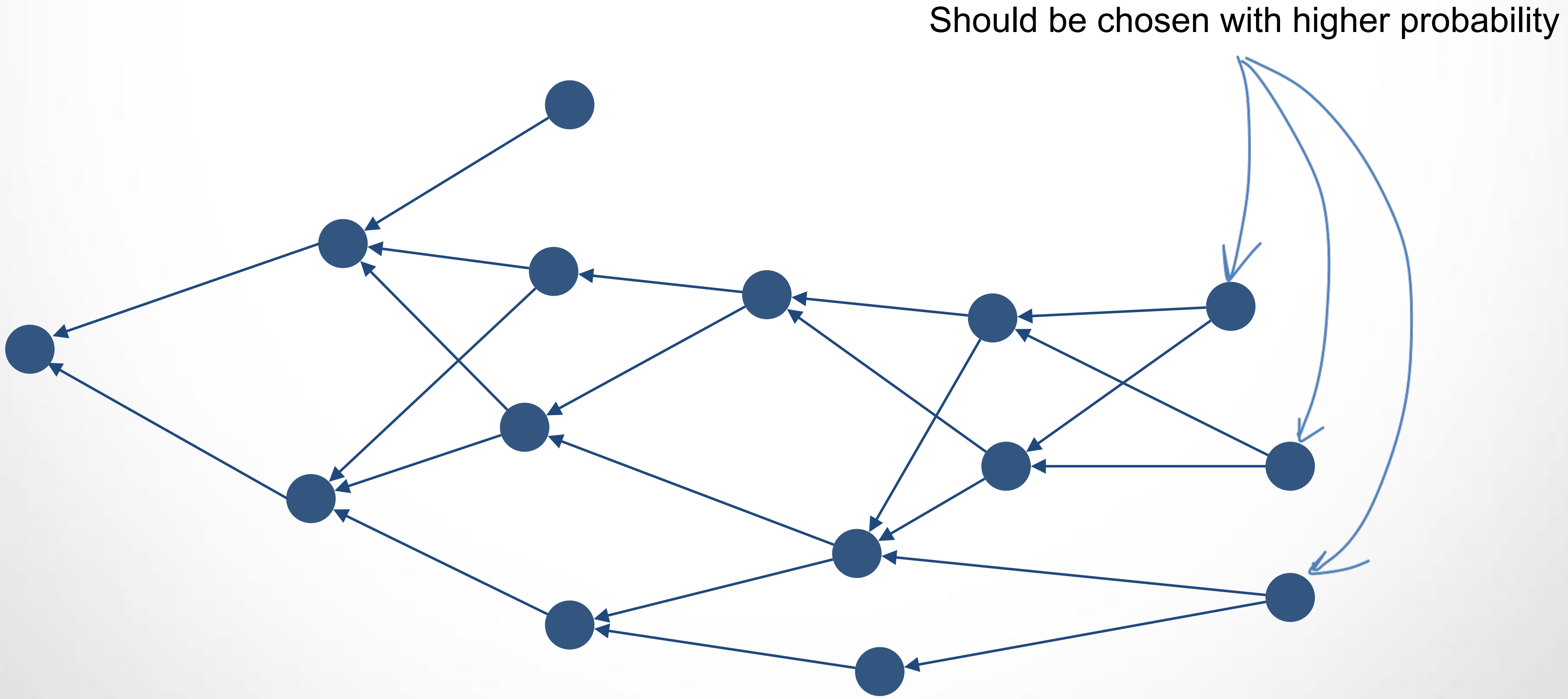
The Tangle

The Tangle (IOTA)



The Tangle

The Tangle (IOTA)



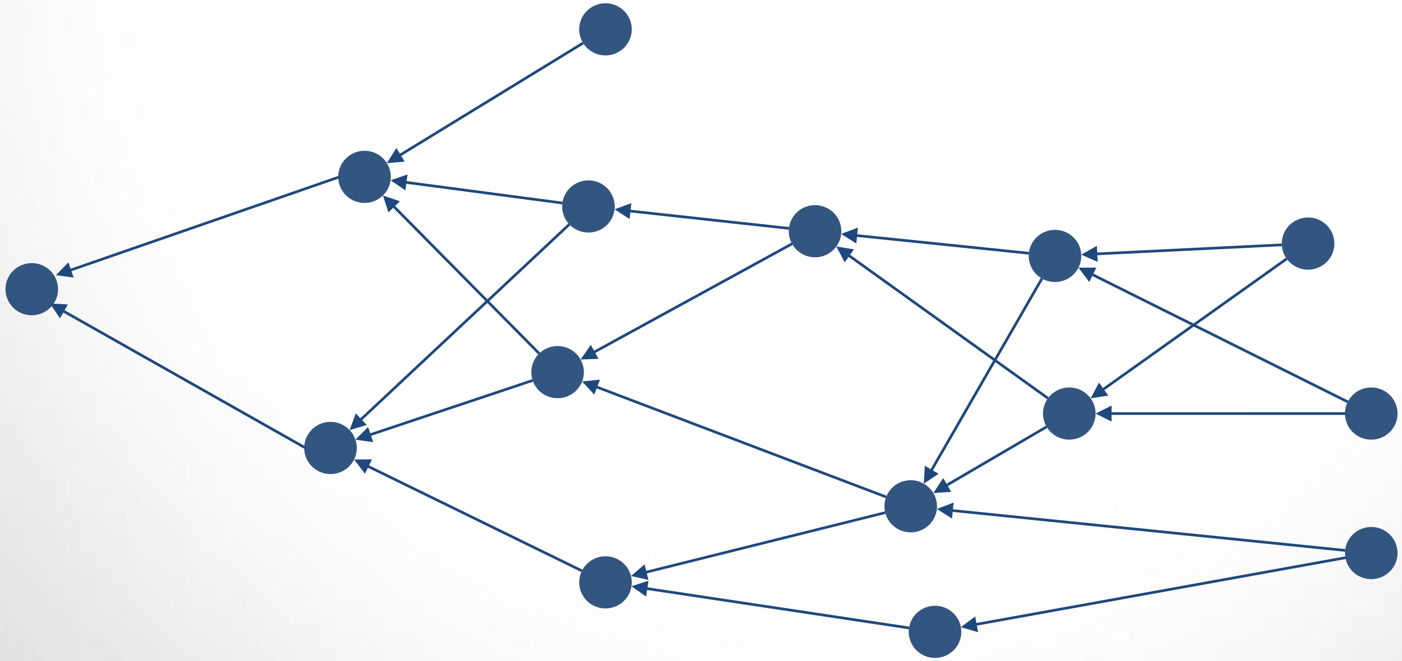
Should be chosen with higher probability

MCMC Tip selection algorithm

MCMC Tip selection algorithm

The Tangle (IOTA)

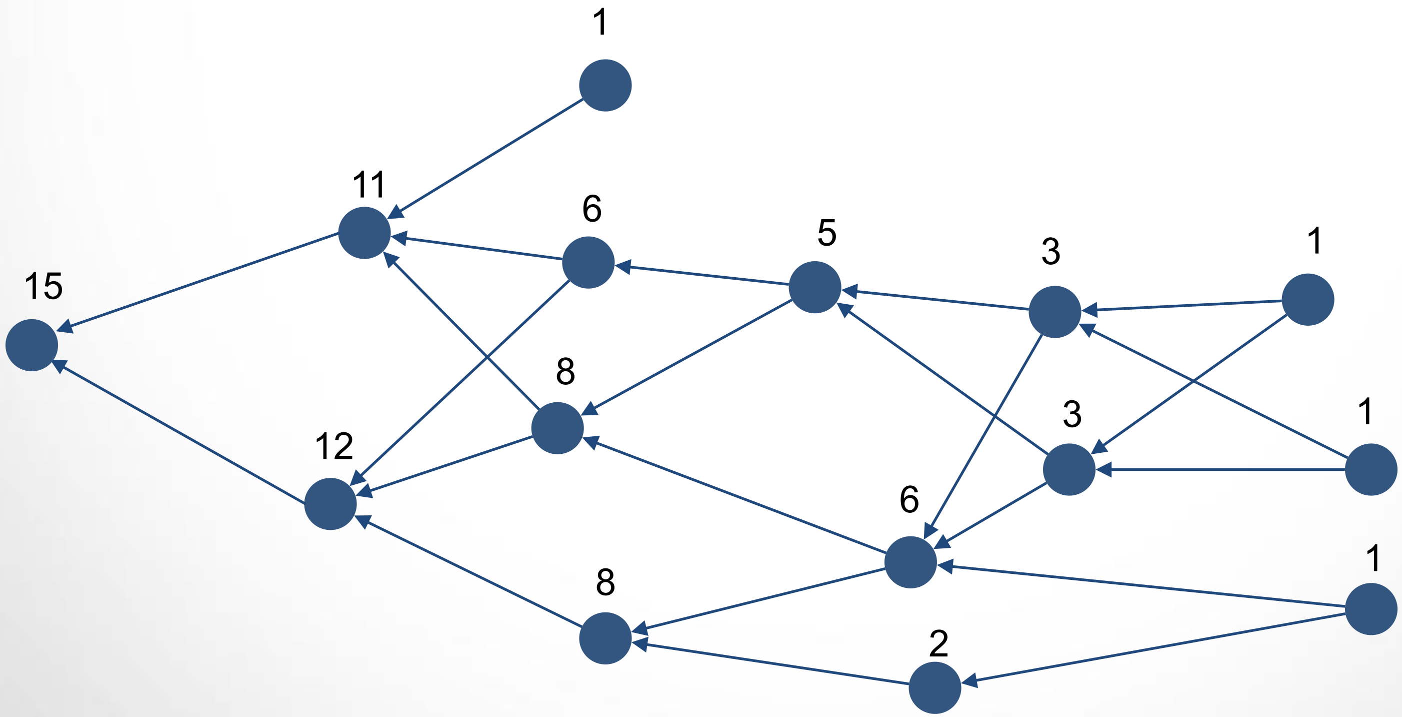
Compute cumulative weight to each site



MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

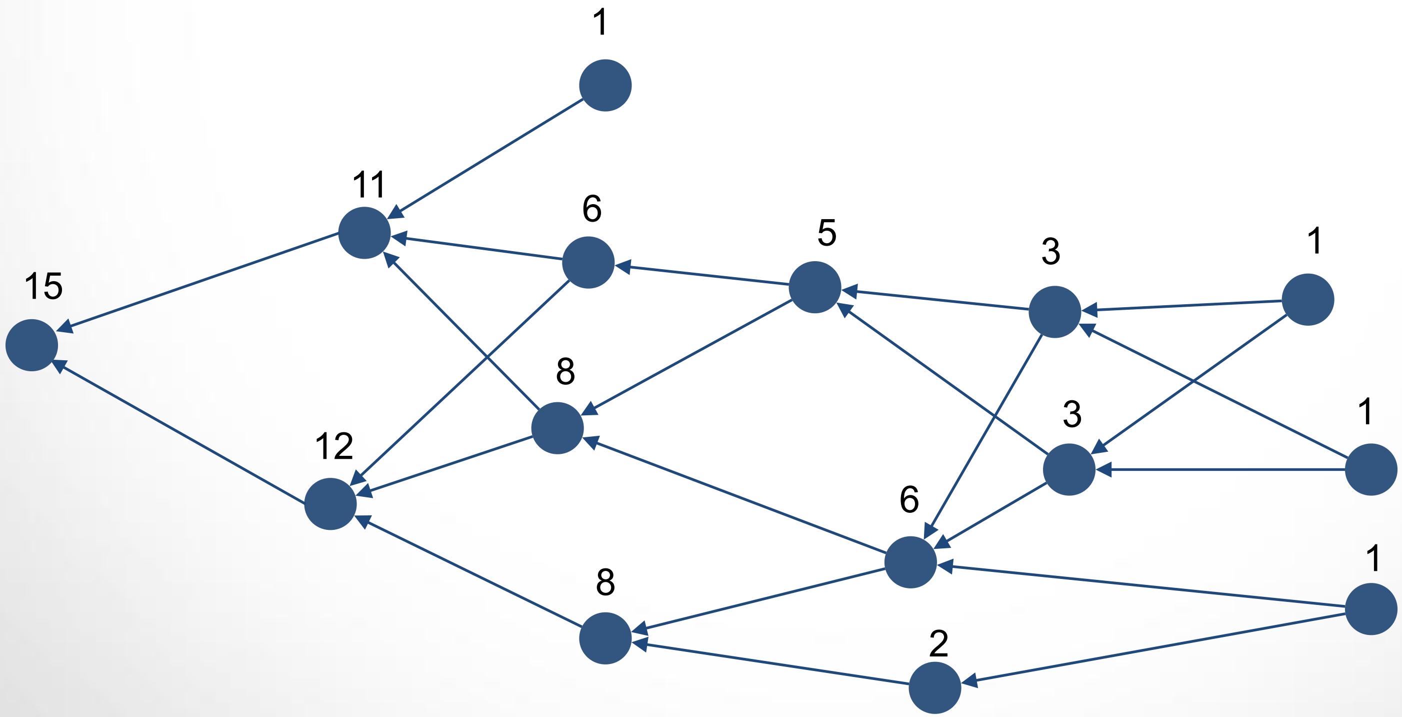


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk

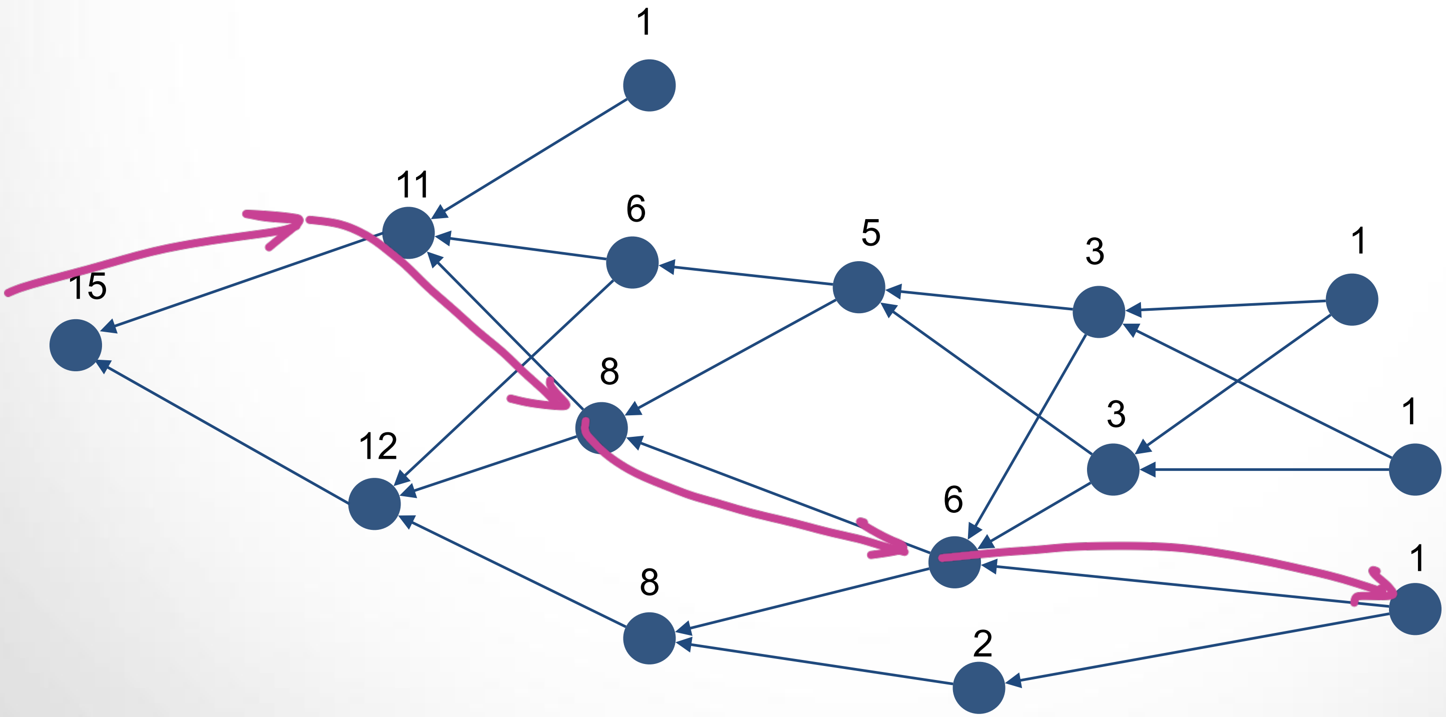


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk

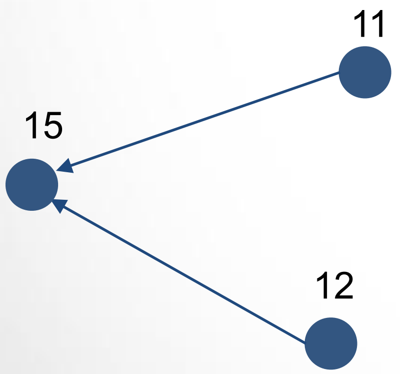


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk

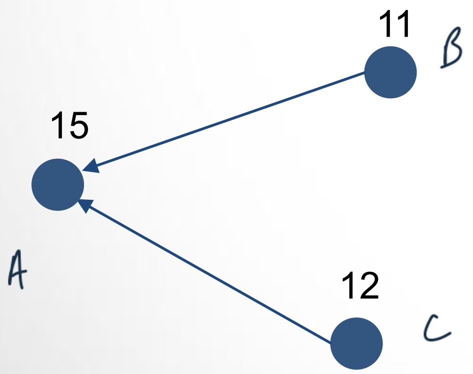


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk

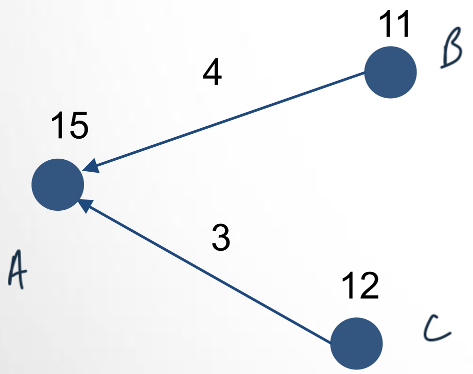


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk

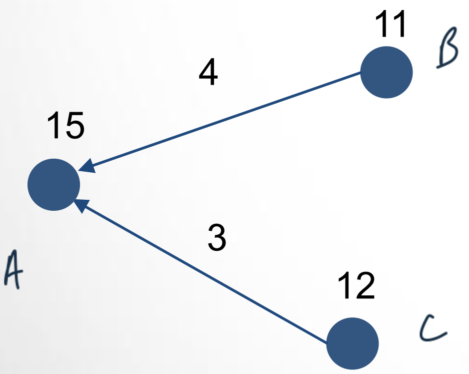


MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk



Transition function:

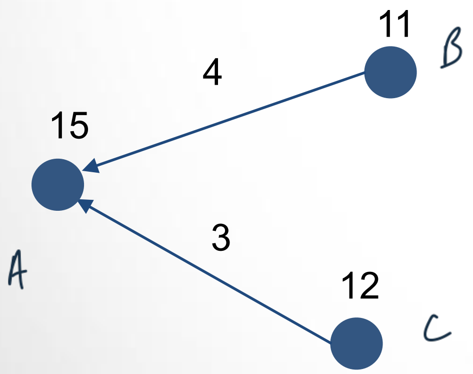
$$\mathbb{P}(A \rightsquigarrow B) = \frac{f(\Delta_{A,B})}{f(\Delta_{A,B}) + f(\Delta_{A,C})}$$

MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk



Transition function:

$$\mathbb{P}(A \rightsquigarrow B) = \frac{f(\Delta_{A,B})}{f(\Delta_{A,B}) + f(\Delta_{A,C})}$$

MCMC

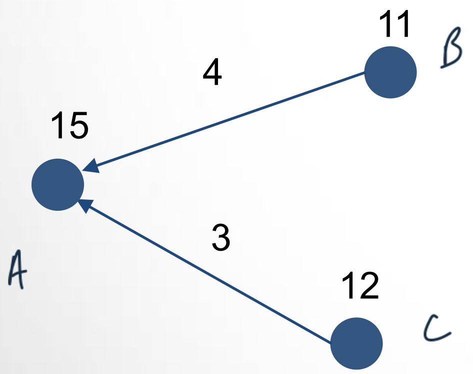
$$f(\Delta) = e^{-\alpha\Delta}$$

MCMC Tip selection algorithm

The Tangle (IOTA)

Compute cumulative weight to each site

Perform a random walk



Transition function:

$$\mathbb{P}(A \rightsquigarrow B) = \frac{f(\Delta_{A,B})}{f(\Delta_{A,B}) + f(\Delta_{A,C})}$$

MCMC

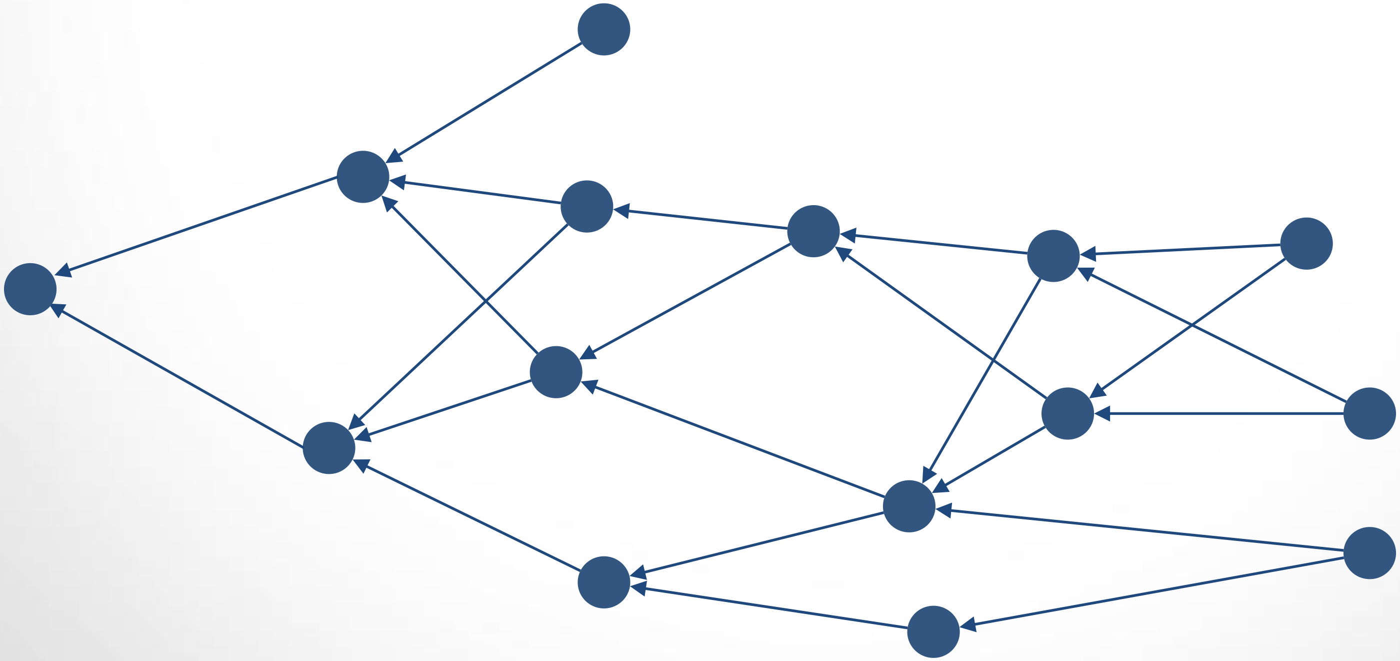
$$f(\Delta) = e^{-\alpha\Delta}$$

LMCMC

$$f(\Delta) = \Delta^{-\alpha}$$

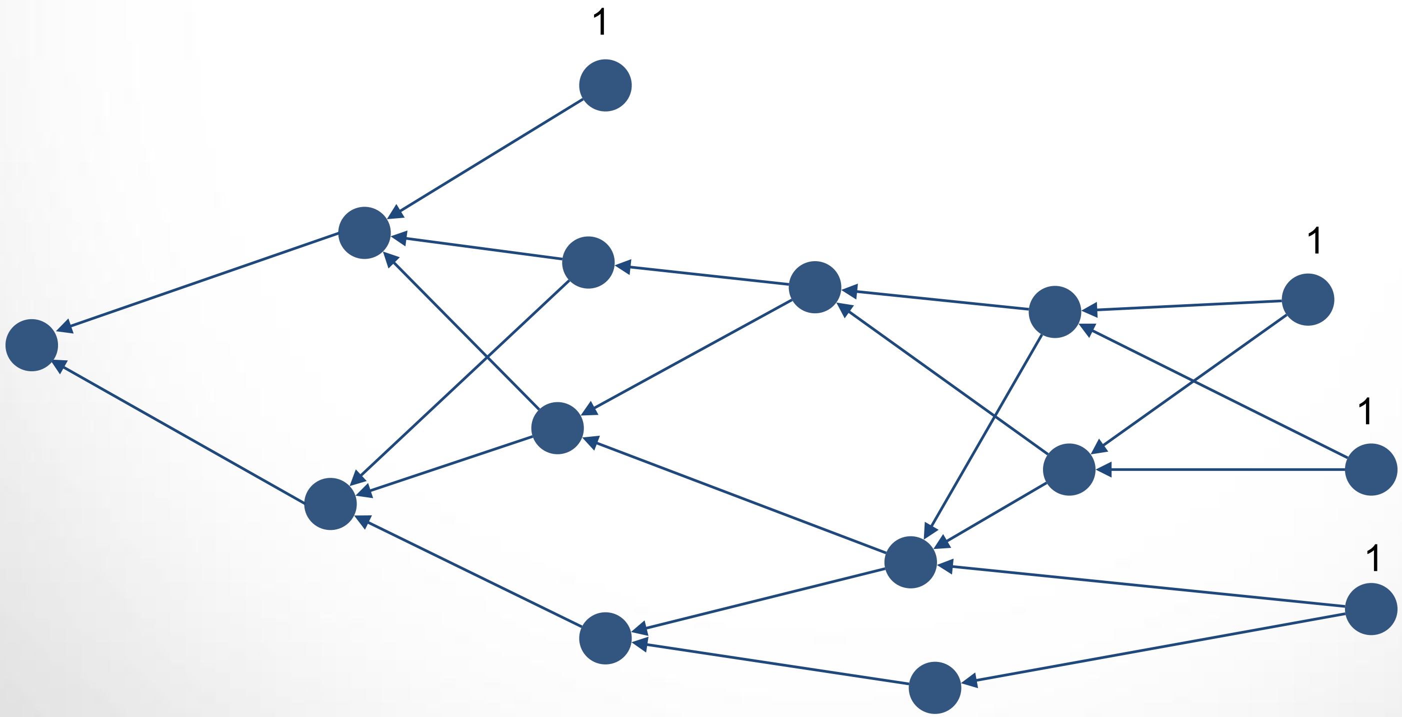
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



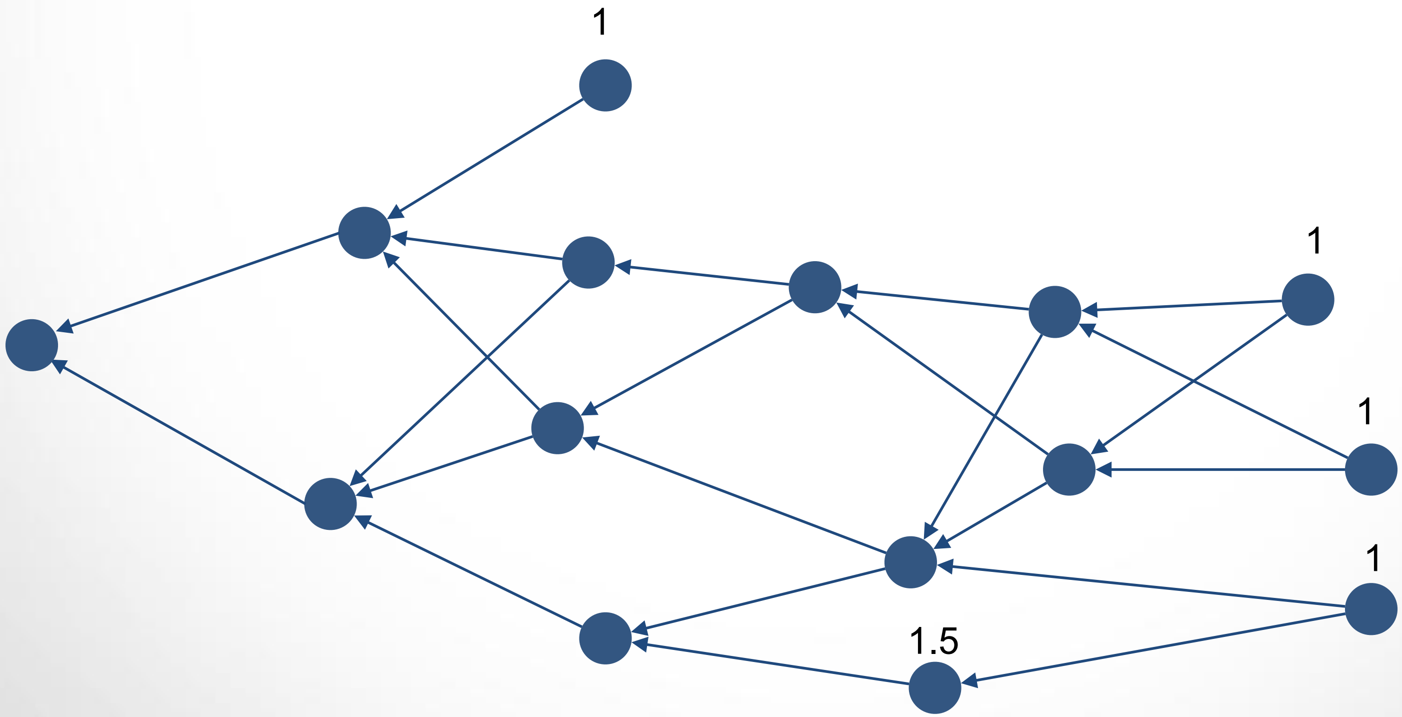
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



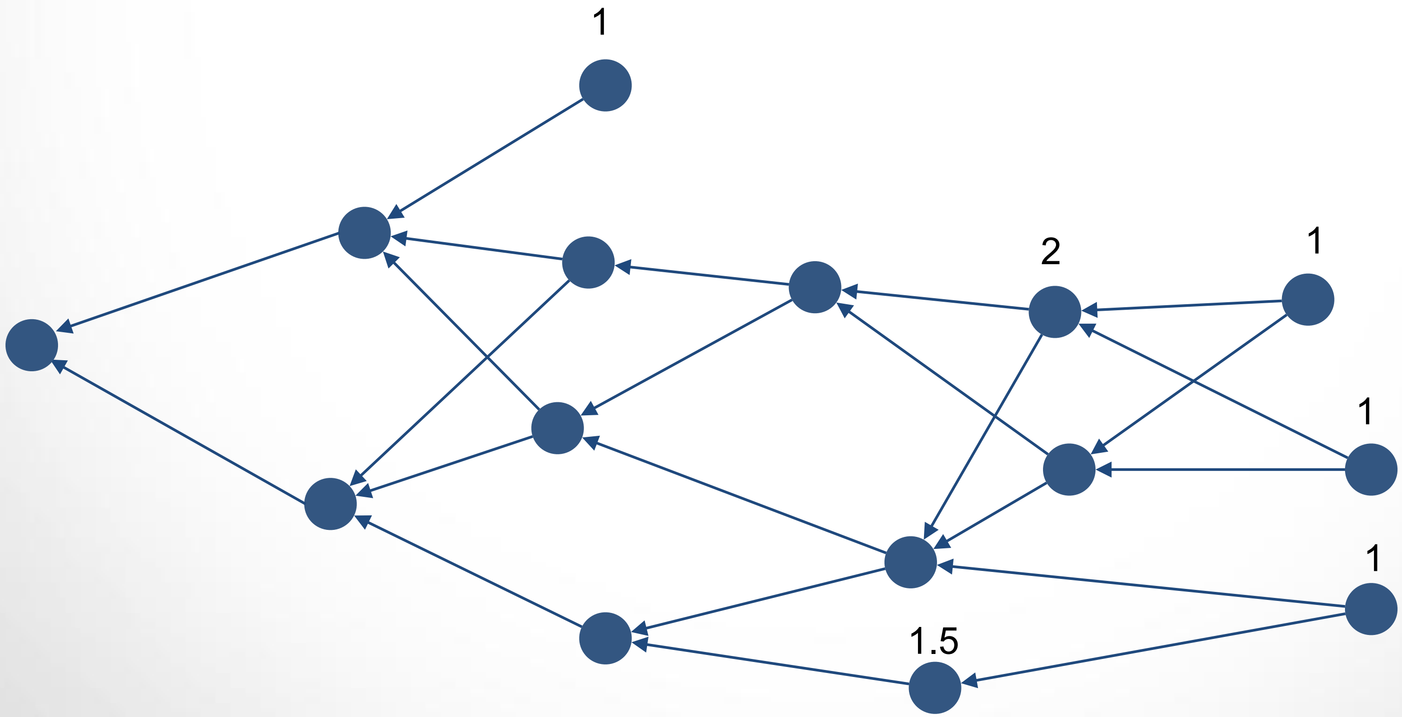
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



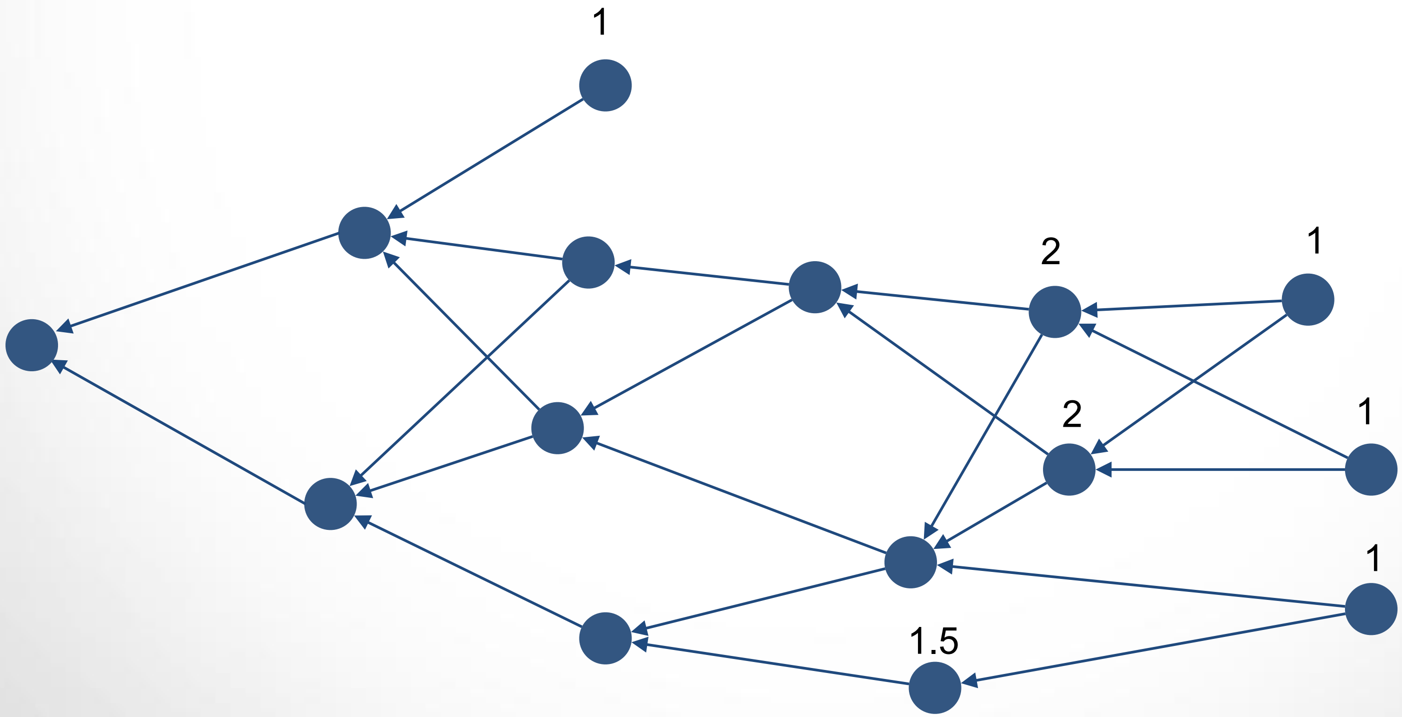
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



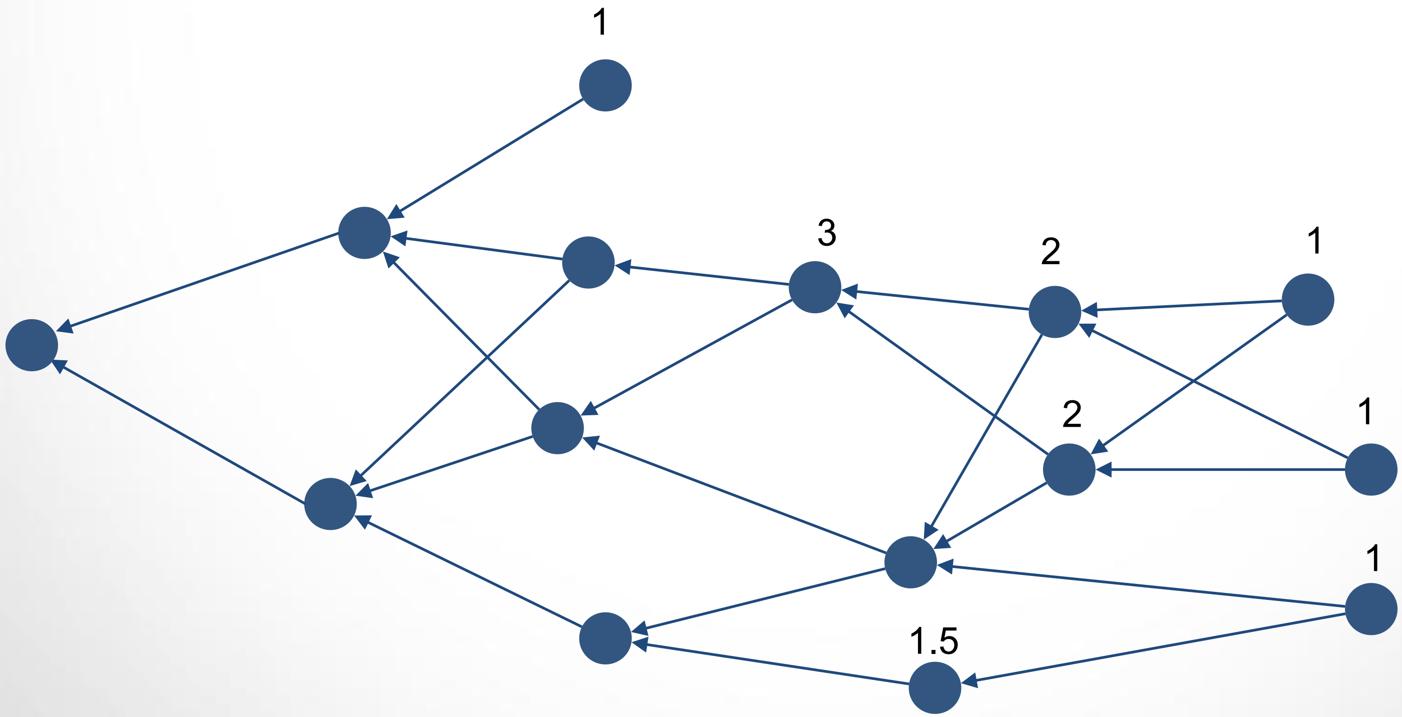
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



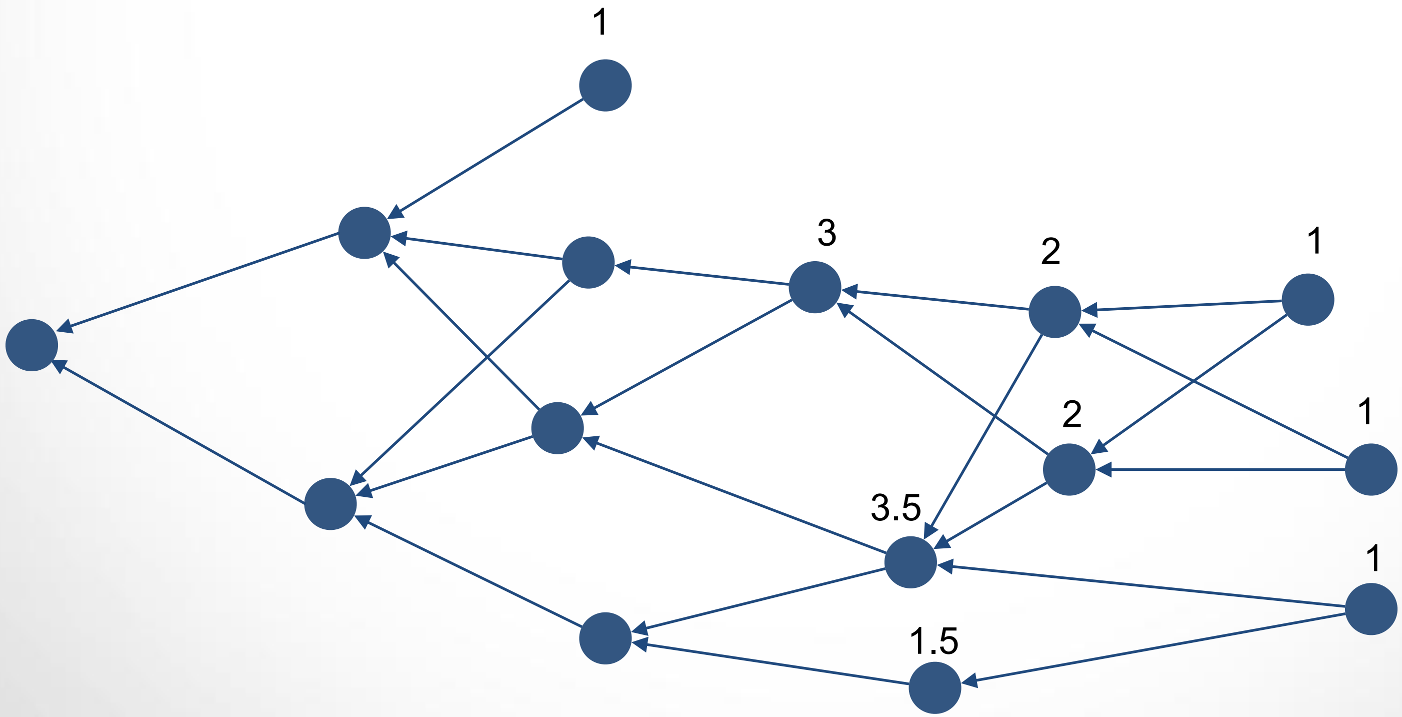
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



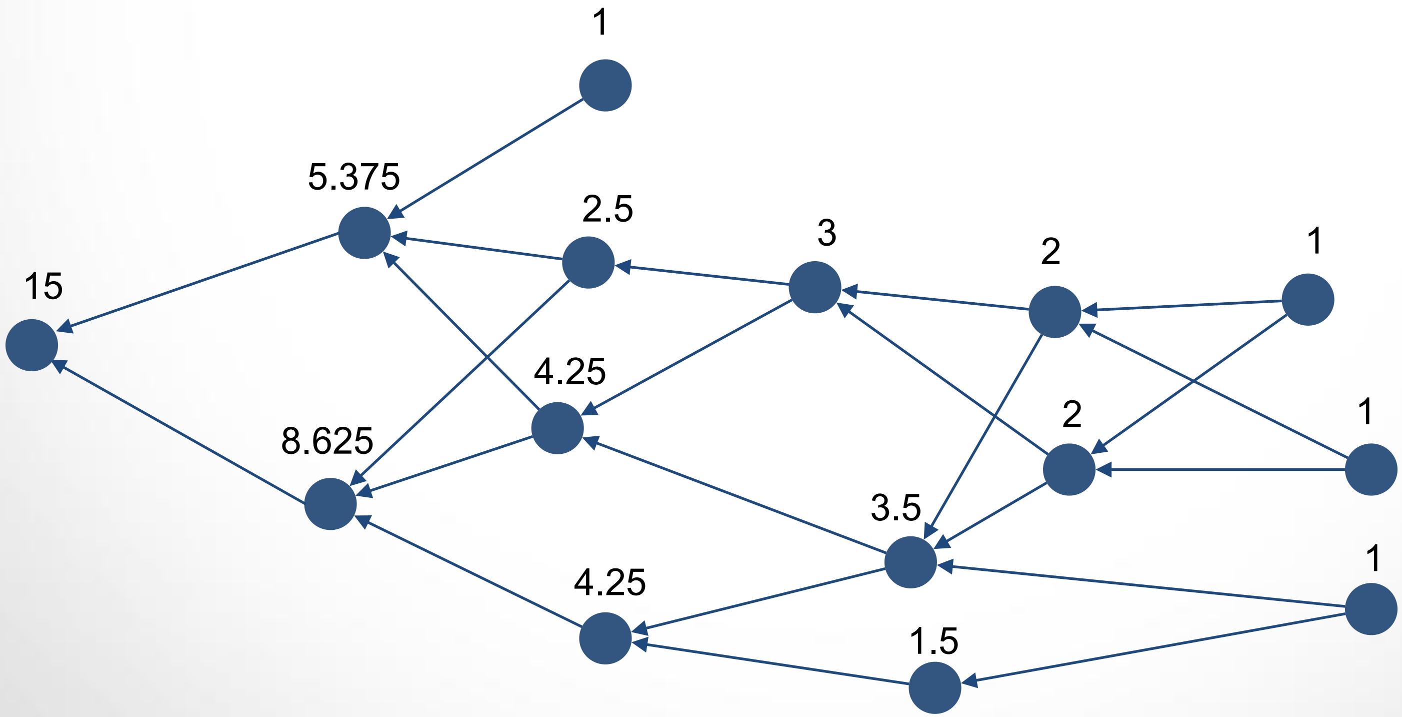
Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$

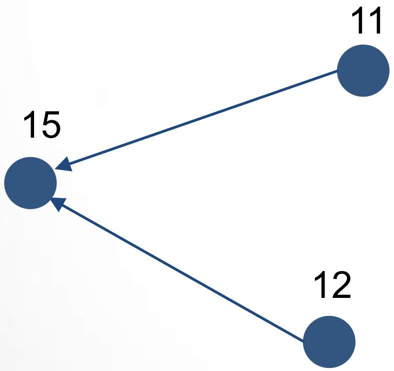


Real cumulative weight

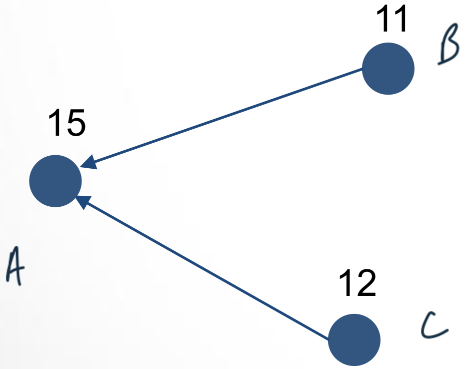
$$w(u) = 1 + \sum_{c \in \text{children}} w(c)$$



Random Walk

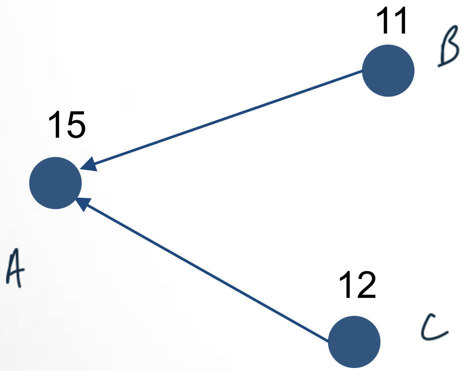


Random Walk



$$\mathbb{P}_{A\to B} = \frac{11}{11+12}.$$

Random Walk



Transition function:

$$\mathbb{P}_{A\to B} = \frac{11}{11+12}.$$

Parasite Chain Attack

Parasite Chain Attack

Double Spending Attack

Parasite Chain Attack

Double Spending Attack

- Alice sends 10 IOTA to Bob for a sandwich

Parasite Chain Attack

Double Spending Attack

- Alice sends 10 IOTA to Bob for a sandwich
- Bob waits to see the transaction in the Tangle

Parasite Chain Attack

Double Spending Attack

- Alice sends 10 IOTA to Bob for a sandwich
- Bob waits to see the transaction in the Tangle
- Bob gives Alice the sandwich

Parasite Chain Attack

Double Spending Attack

- Alice sends 10 IOTA to Bob for a sandwich
- Bob waits to see the transaction in the Tangle
- Bob gives Alice the sandwich
- Alice generates a lots of transactions so that her first transaction is discarded

Parasite Chain Attack

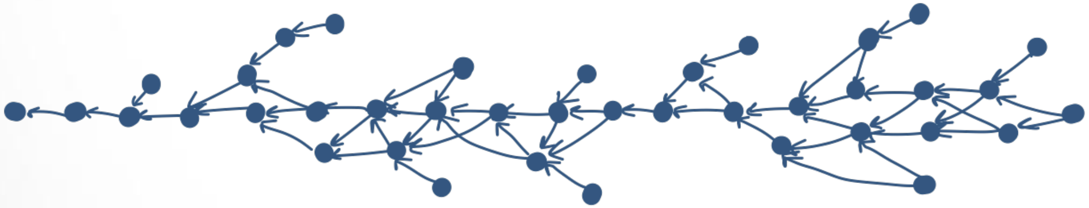
Double Spending Attack

- Alice sends 10 IOTA to Bob for a sandwich
- Bob waits to see the transaction in the Tangle
- Bob gives Alice the sandwich
- Alice generates a lots of transactions so that her first transaction is discarded
- Alice eats the sandwich

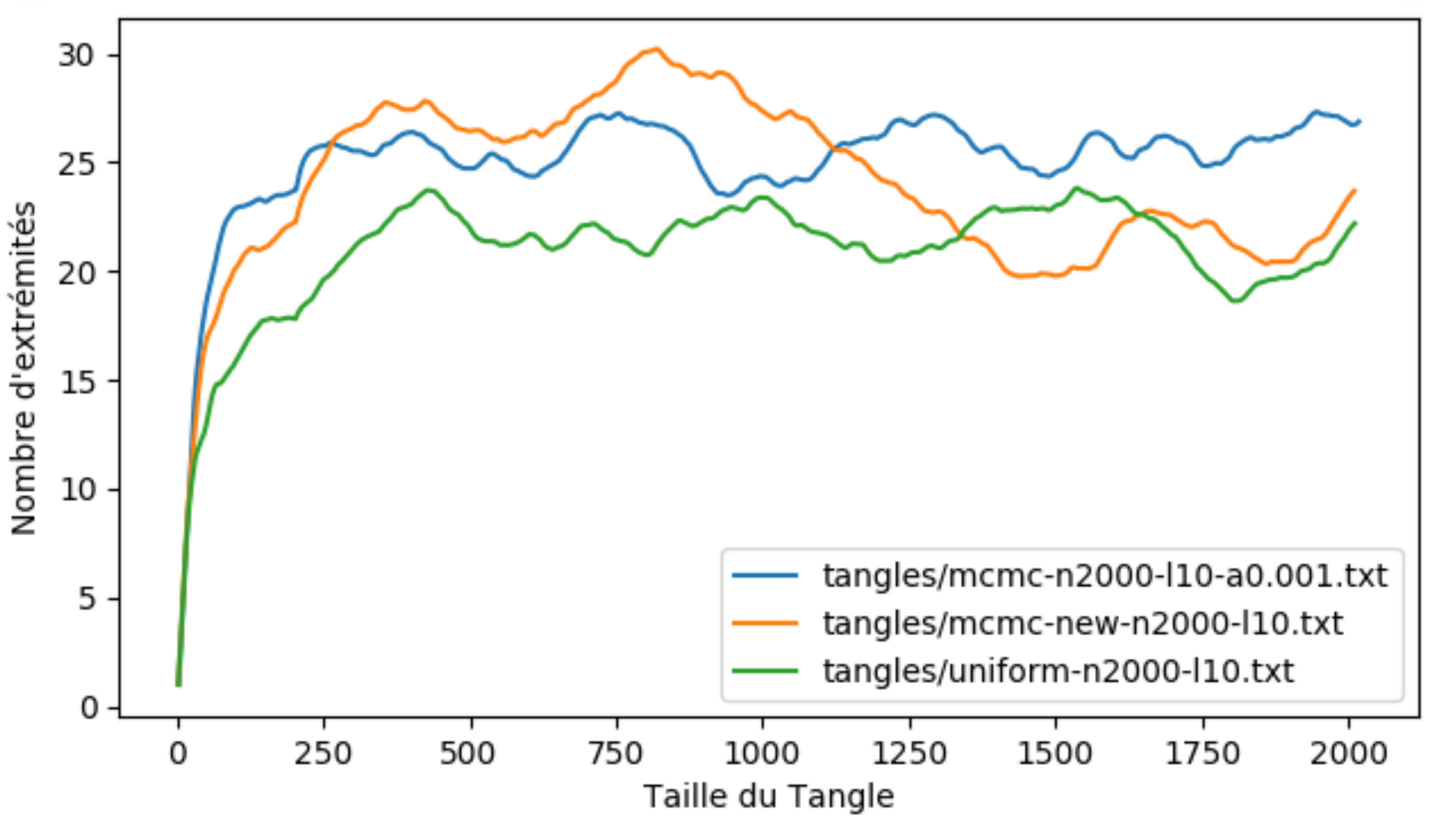
Number of tips

How many tips are left behind ?

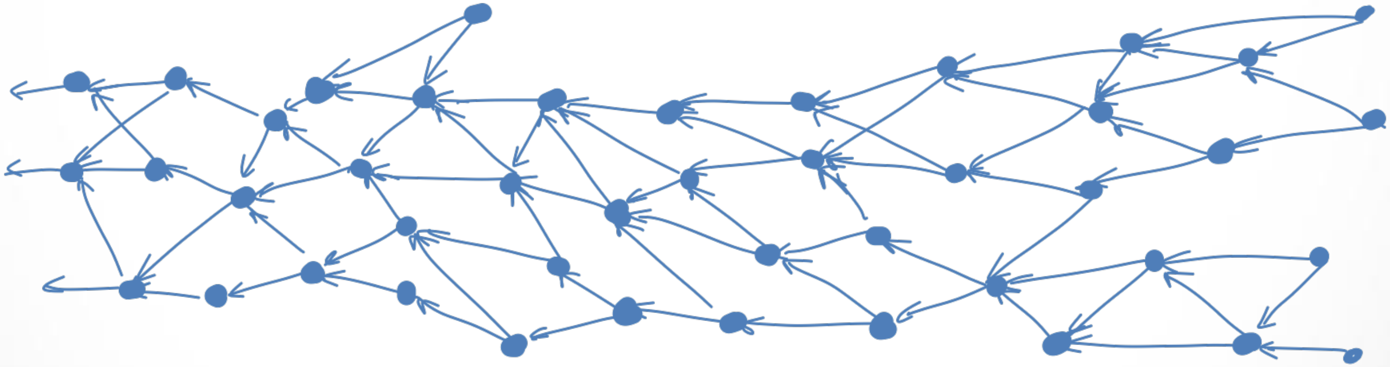
How many tips over the time ?



Tips over time

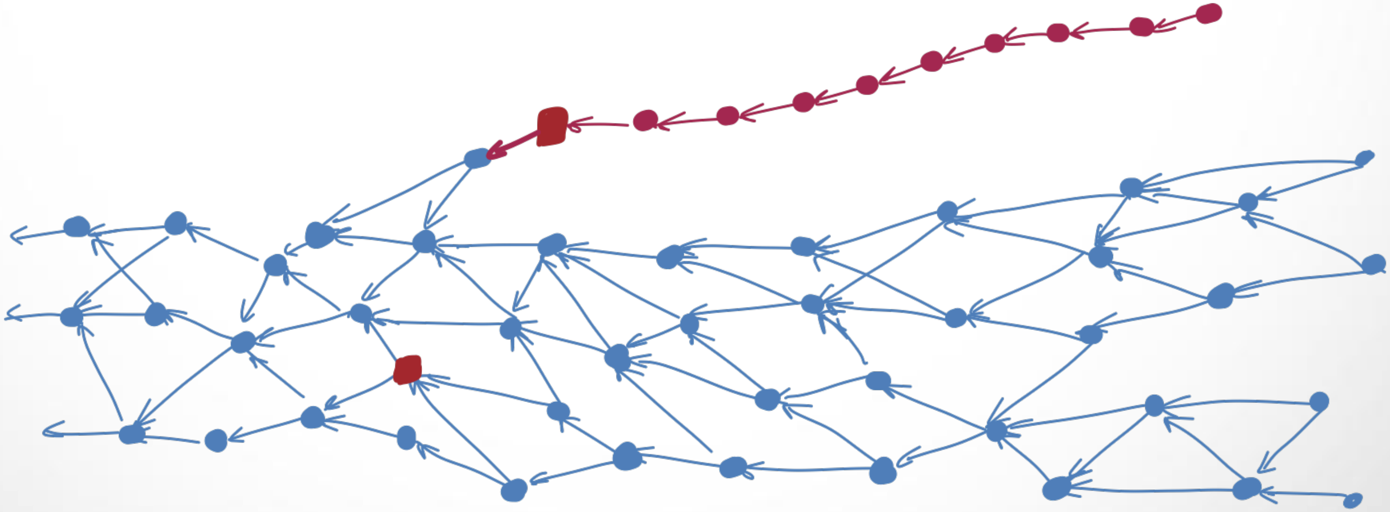


Tips over time



Parasite Chain Attack

The parasite chain attack

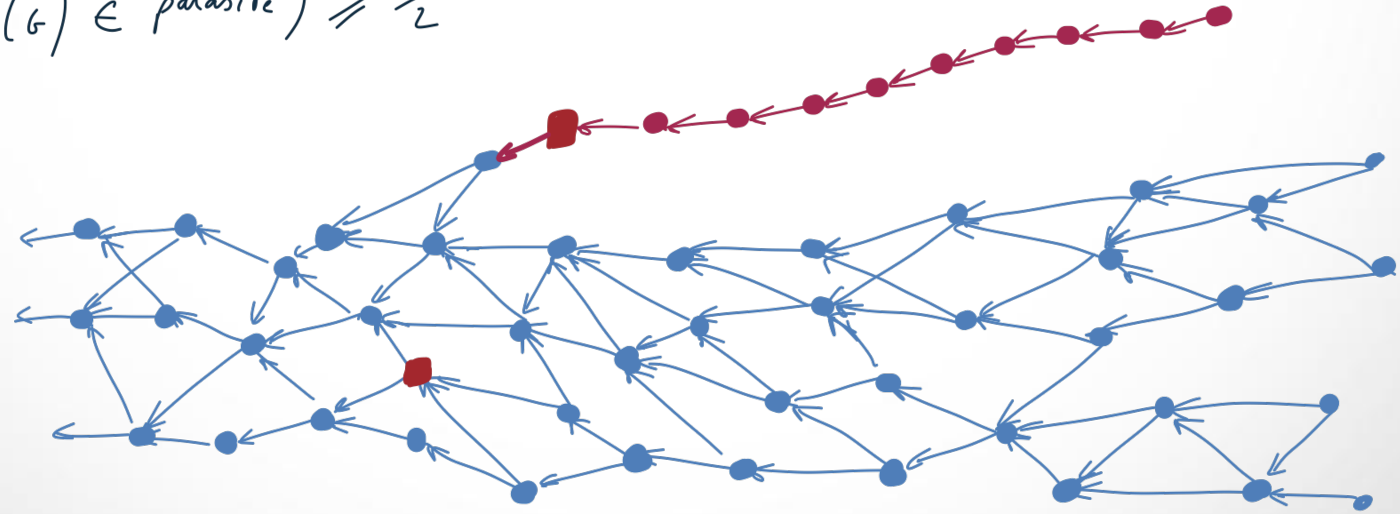


Parasite Chain Attack

The parasite chain attack

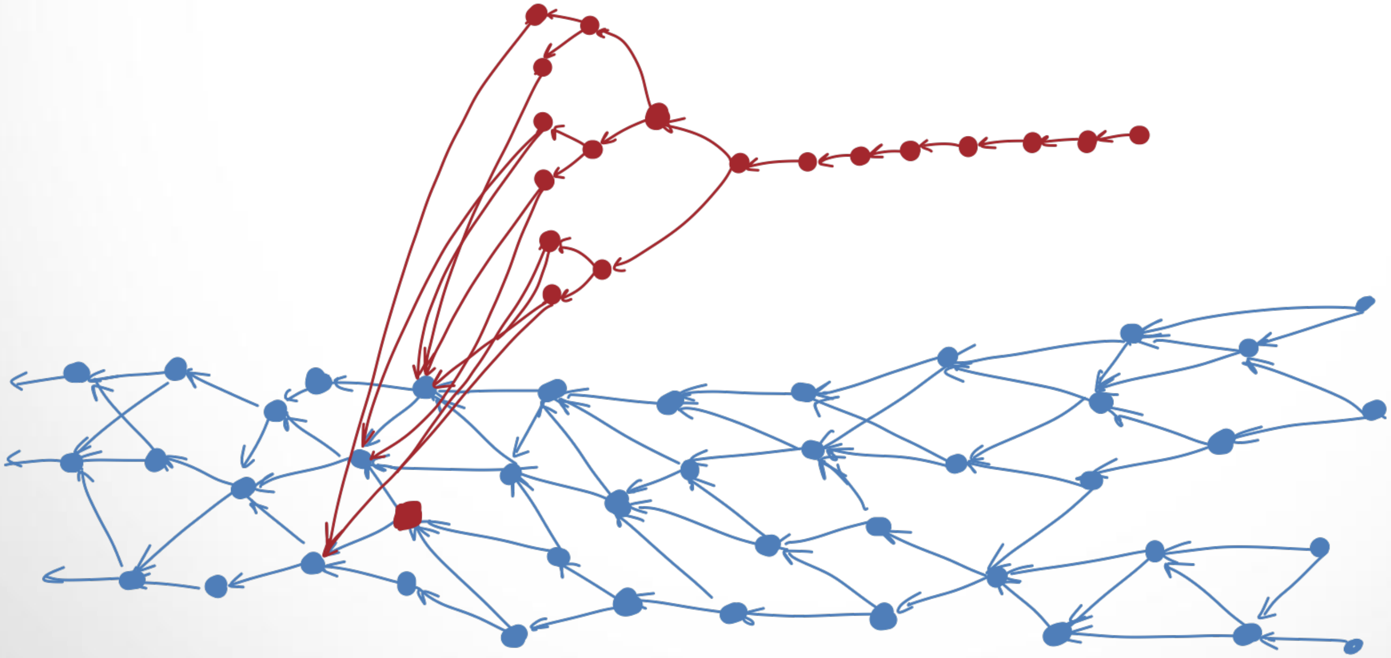
How many red site so that:

$$P(TSA(G) \in \text{parasite}) \geq 1/2$$



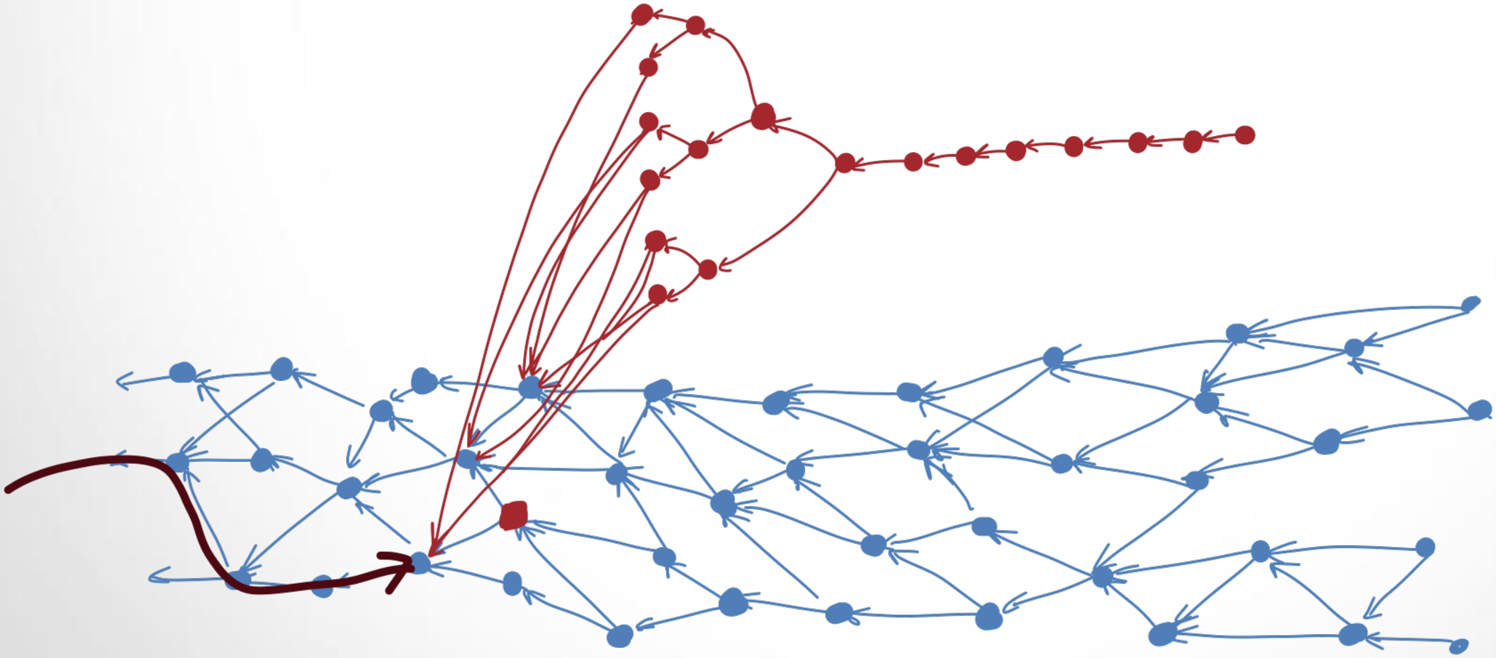
Parasite Chain Attack

Against MCMC



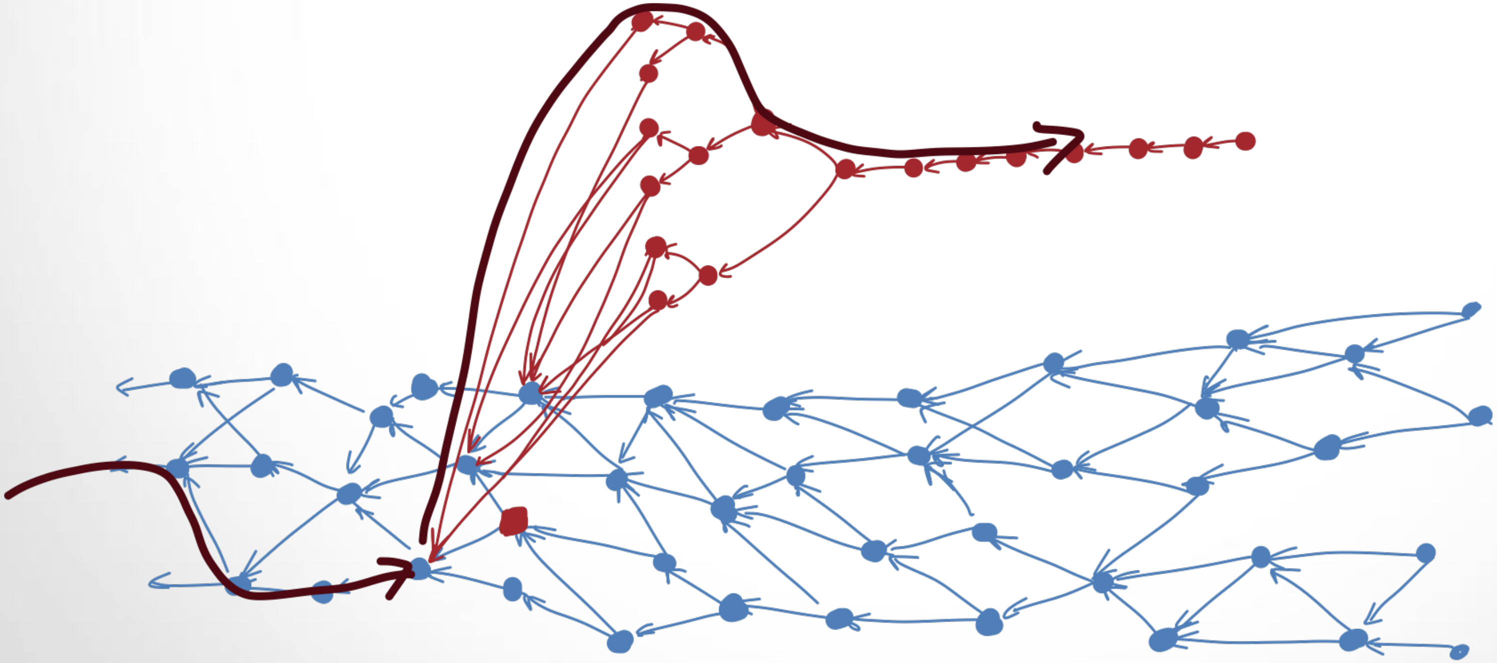
Parasite Chain Attack

Against MCMC

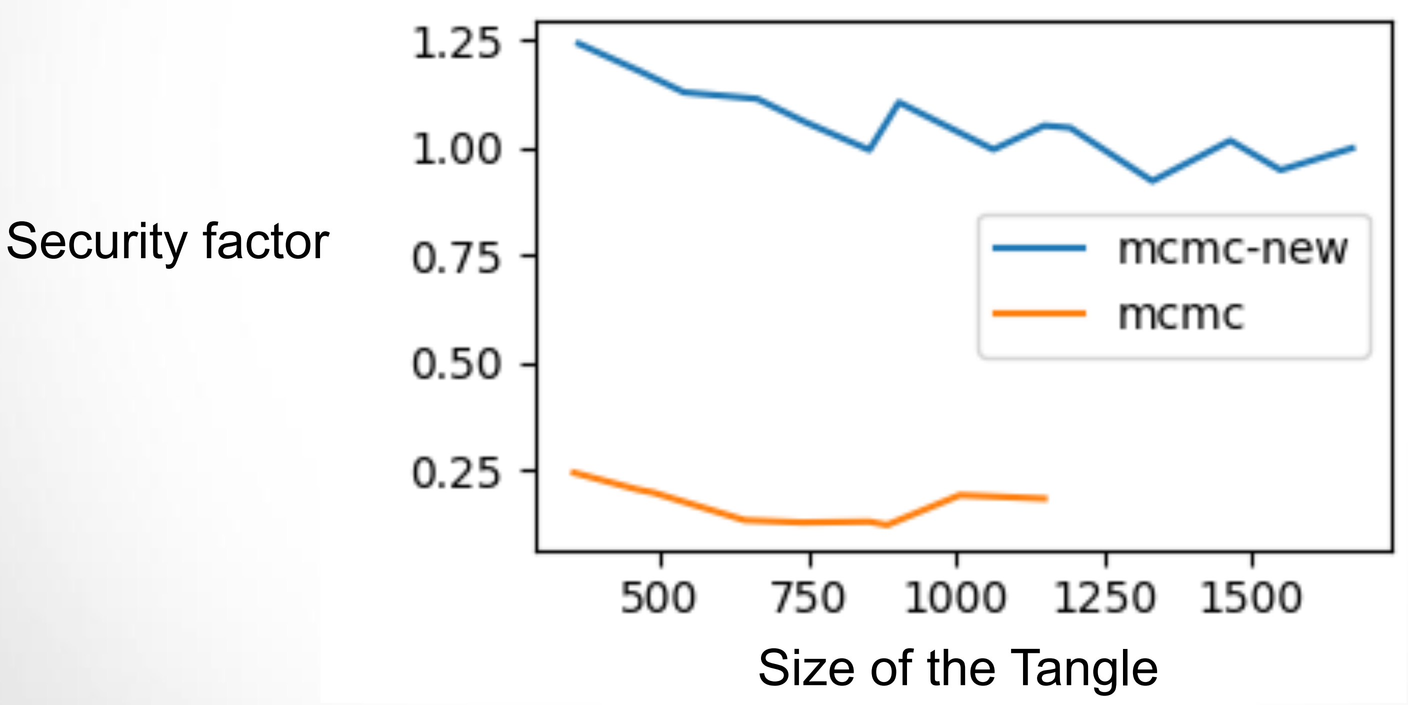


Parasite Chain Attack

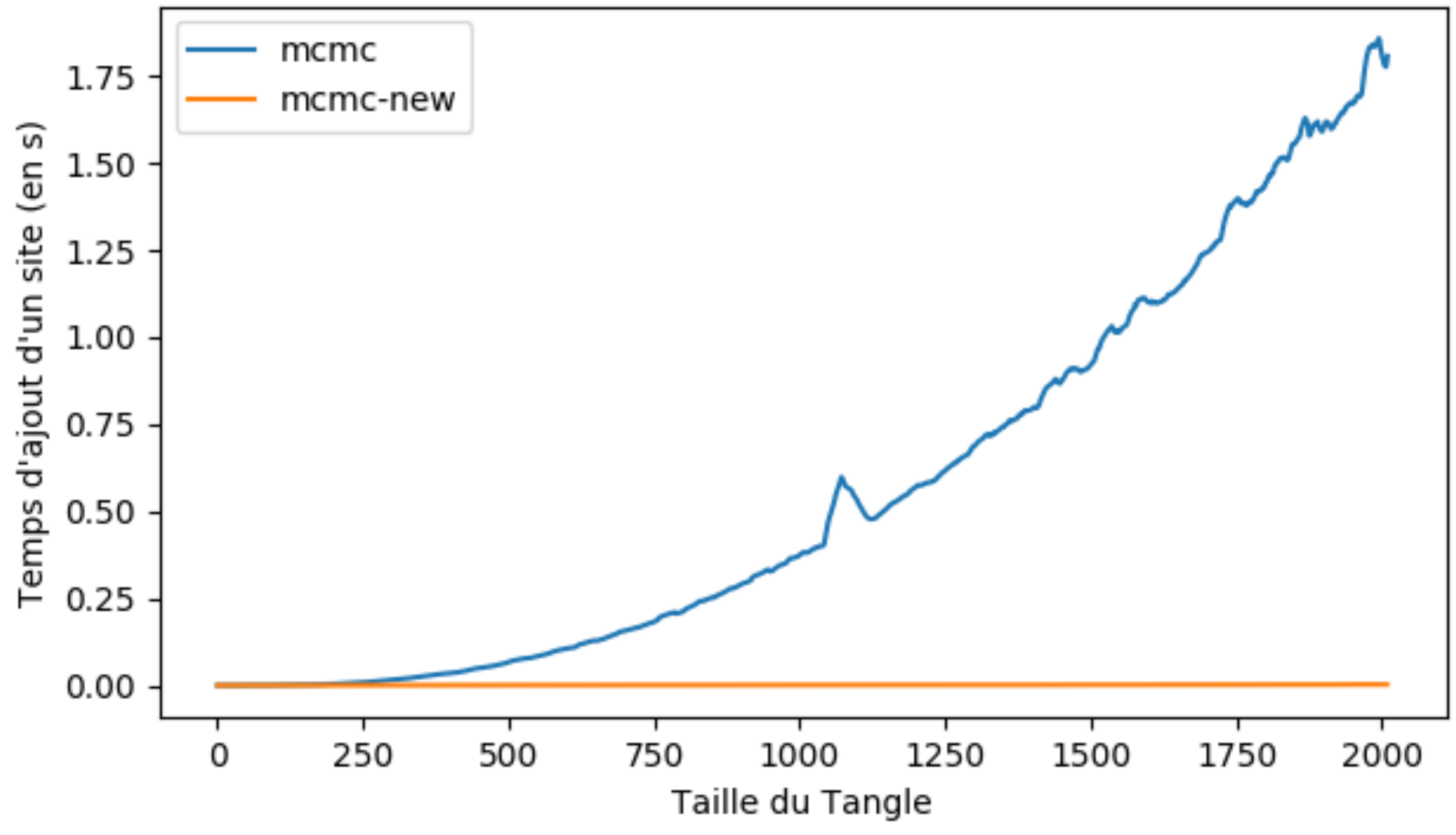
Against MCMC



Resistance to parasite chain



Complexity



mcmc
mcmc-new
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
Temps d'ajout d'un site (en s)
0
250
500
750
1000
1250
1500
1750
2000
Taille du Tangle

Conclusion

Future Work

Conclusion

We defined a good tip selection algorithms

Future Work

Conclusion

We defined a good tip selection algorithms

Future Work

Even better tip selection algorithms

Conclusion

We defined a good tip selection algorithms

Future Work

Even better tip selection algorithms

Thank you for your attention!