IOTA and the Tangle

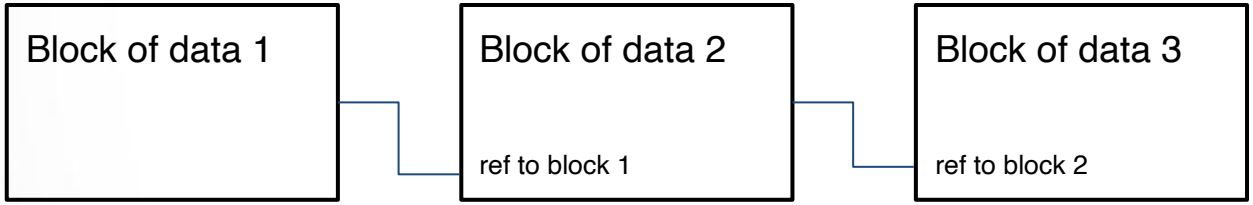
Quentin Bramas bramas@unistra.fr

Tokyo, March, 5th, 2020

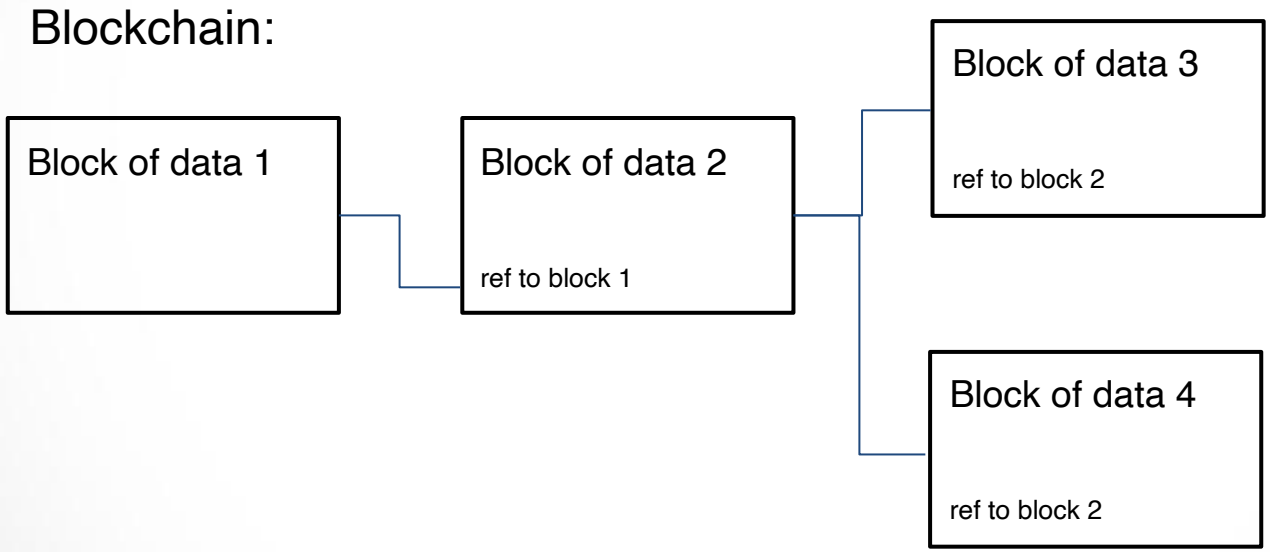
Slides available at http://bramas.fr

Introduction

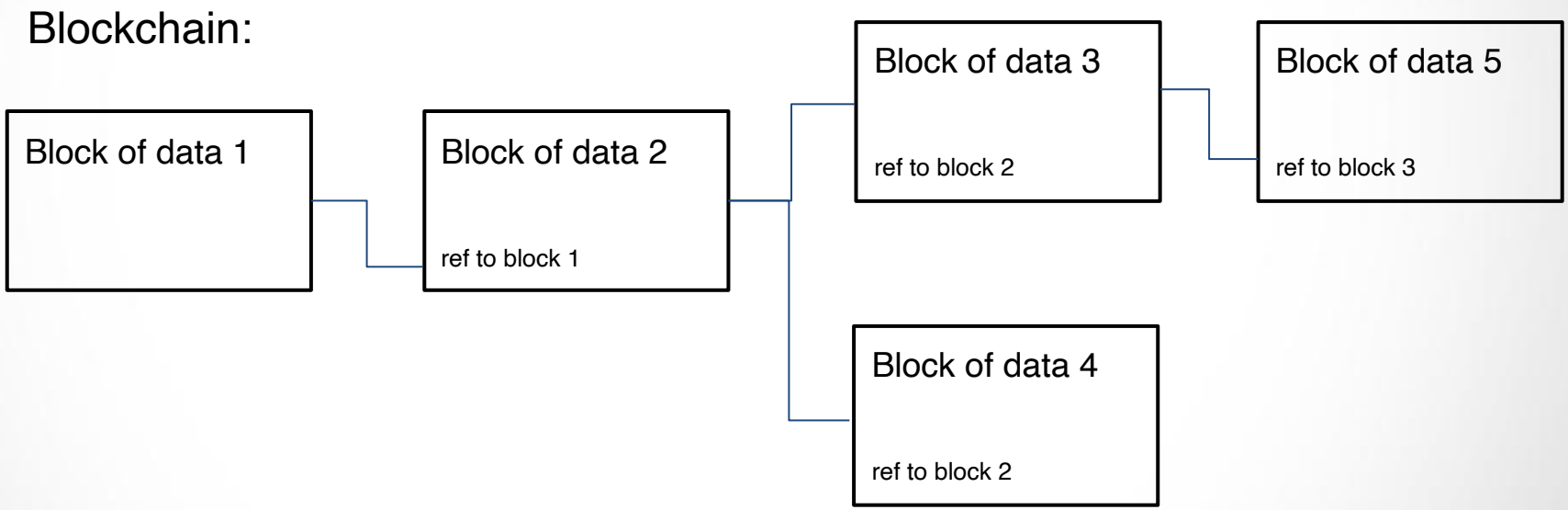
Blockchain:



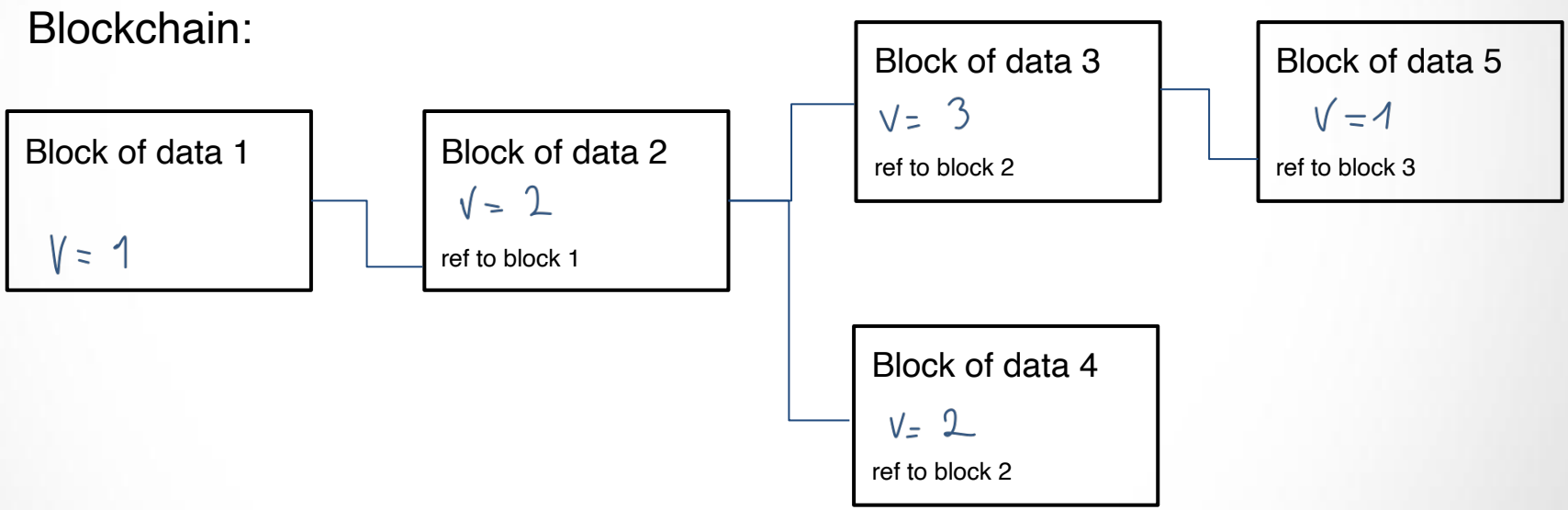
Introduction



Introduction



Introduction



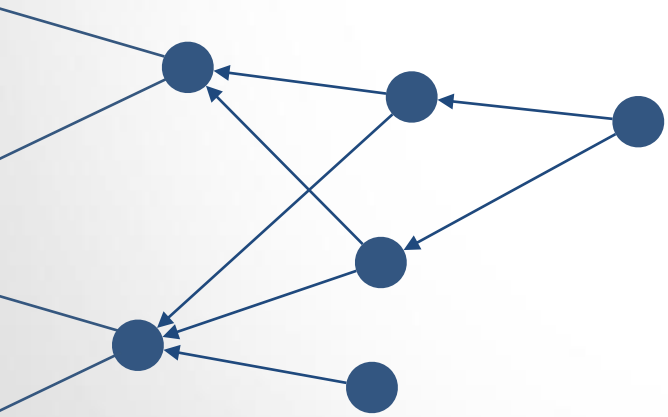
How to read Data: read the longest chain.

How to append Data: chain your block to the longest chain (and mine).

The Tangle

The Tangle (IOTA)

Each transaction is a small block that references two previous ones



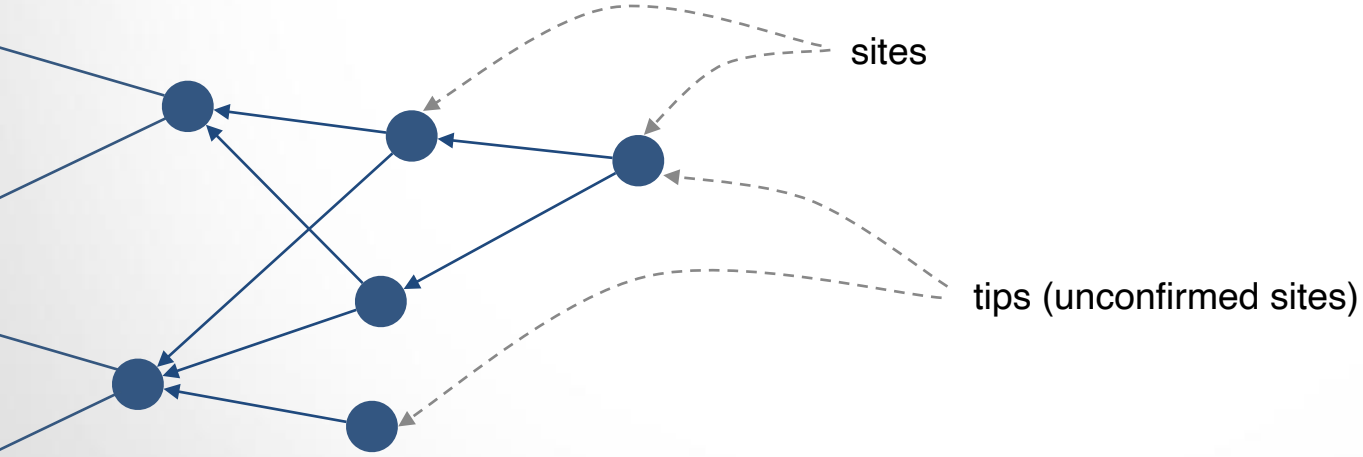
You come up with a DAG
(Directed Acyclic Graph)

You're only limited by bandwidth and storage

The Tangle

The Tangle (IOTA)

Each transaction is a small block that reference two previous ones

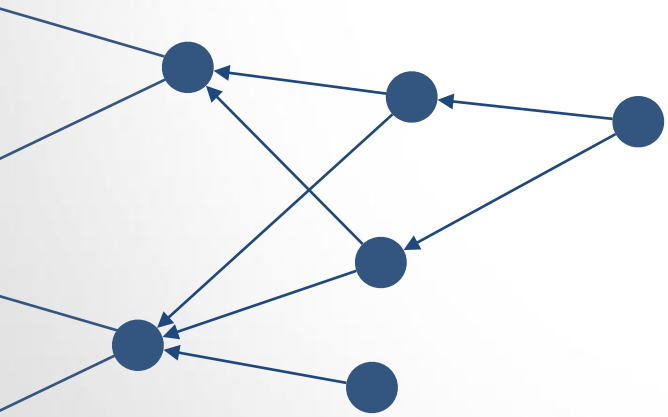


A new site and its parents should not create conflicts.

The Tangle

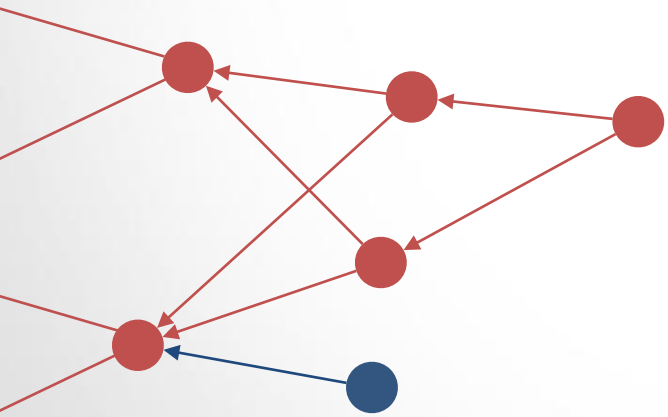
The Tangle (IOTA)

How to read a value?



The Tangle

The Tangle (IOTA)

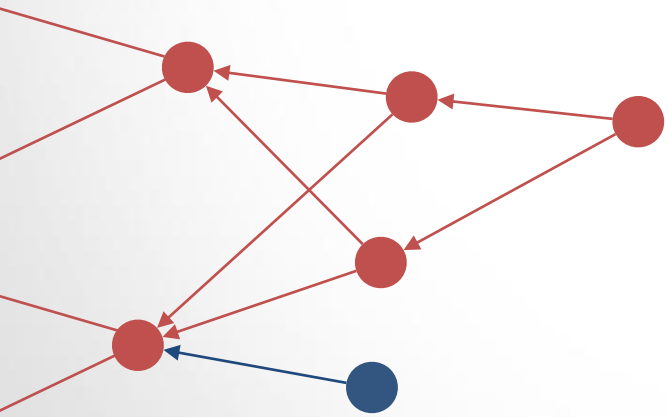


How to read a value?

You first select a tip, you can then order transactions and do the same as in a blockchain

The Tangle

The Tangle (IOTA)



How to read a value?

You first select a tip, you can then order transactions and do the same as in a blockchain

How to append a transaction?

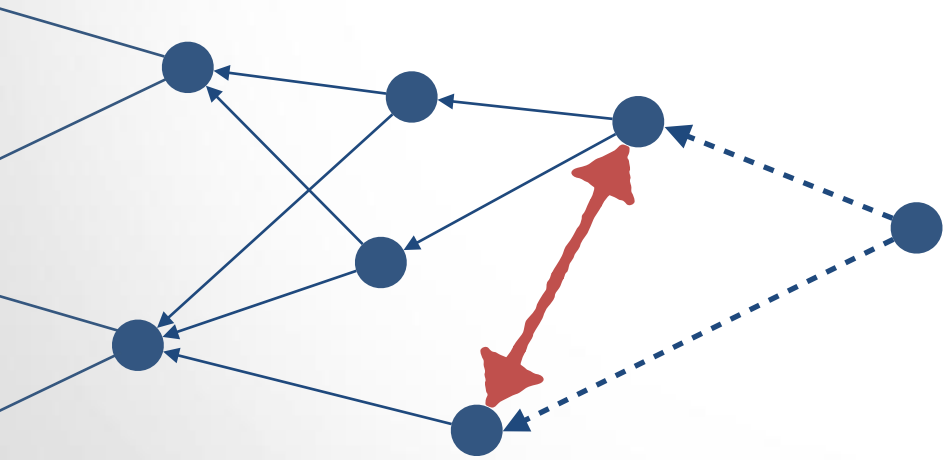
You first select two tips, then add a site that confirms those parents.

The Tangle

The Tangle (IOTA)

How to read a value?

What if tips are conflicting?



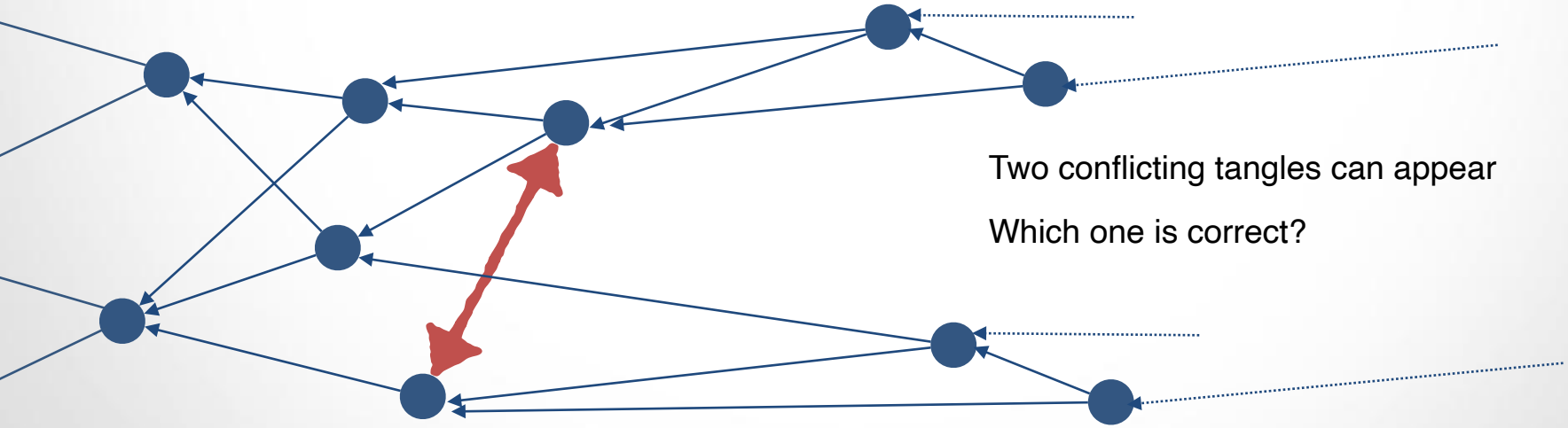
A new site cannot confirm conflicting sites

The Tangle

The Tangle (IOTA)

How to read a value?

What if tips are conflicting?

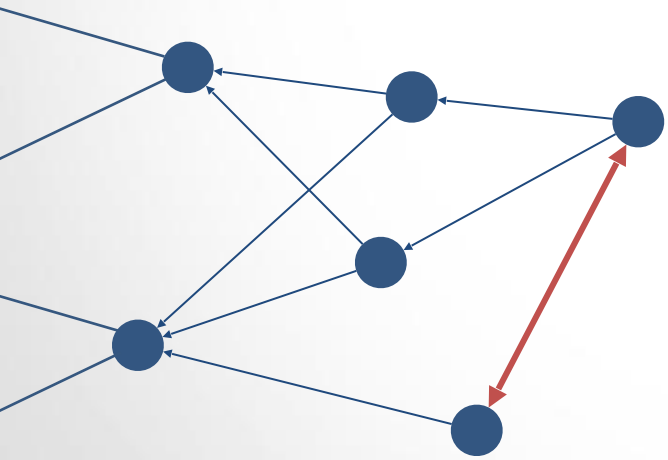


Two conflicting tangles can appear

Which one is correct?

The Tangle

The Tangle (IOTA)



Tip Selection Algorithm (TSA):

- To know how to read values
- To 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)

In the Tangle, forks are ok if not conflicting

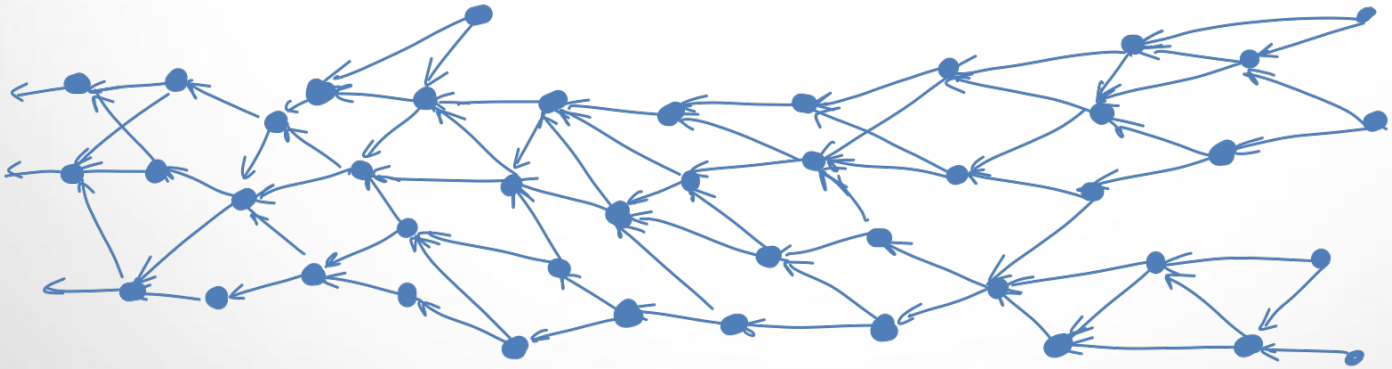
But conflicting forks are worst in this case

The Tangle

The Tangle (IOTA)

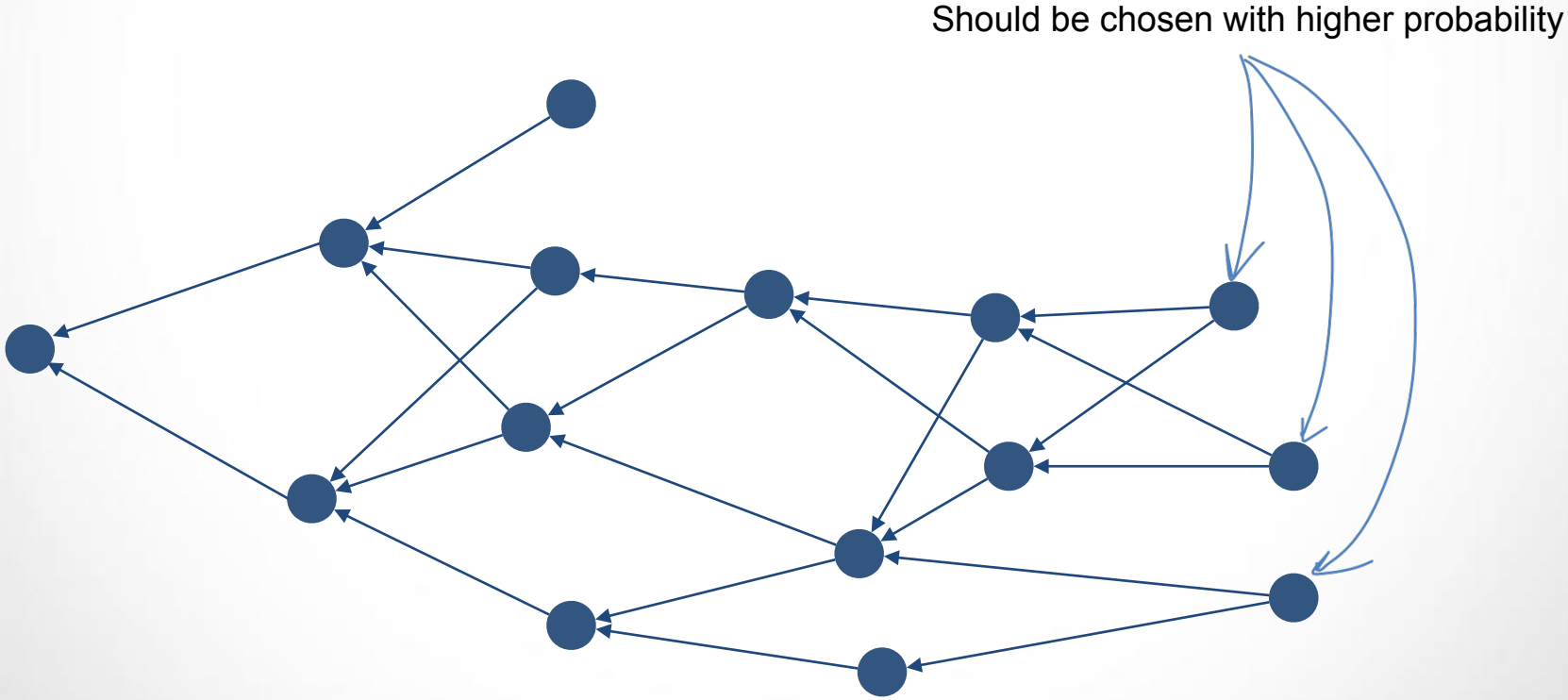
In the Tangle, forks are ok if not conflicting

So its better to have something like this



The Tangle

The Tangle (IOTA)



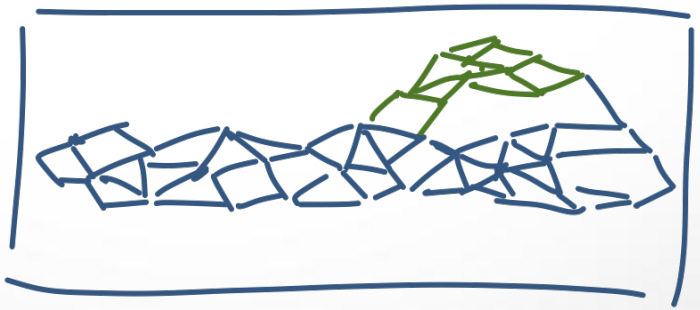
How is it done? We will come back to this

The Tangle

Some advantages of IOTA:

There are no transaction fees

A disconnected network can publish transactions locally, that get merged after a reconnection.



The Tangle

Some advantages of IOTA:

- There are no transaction fees
- A disconnected network can publish transactions locally, that get merged after a reconnection.
- It is Quantum-resistant
- It is maintained by a non-profit Foundation

Some questionnable things about IOTA:

- There is a central coordinator
- It uses ternary arithmetics

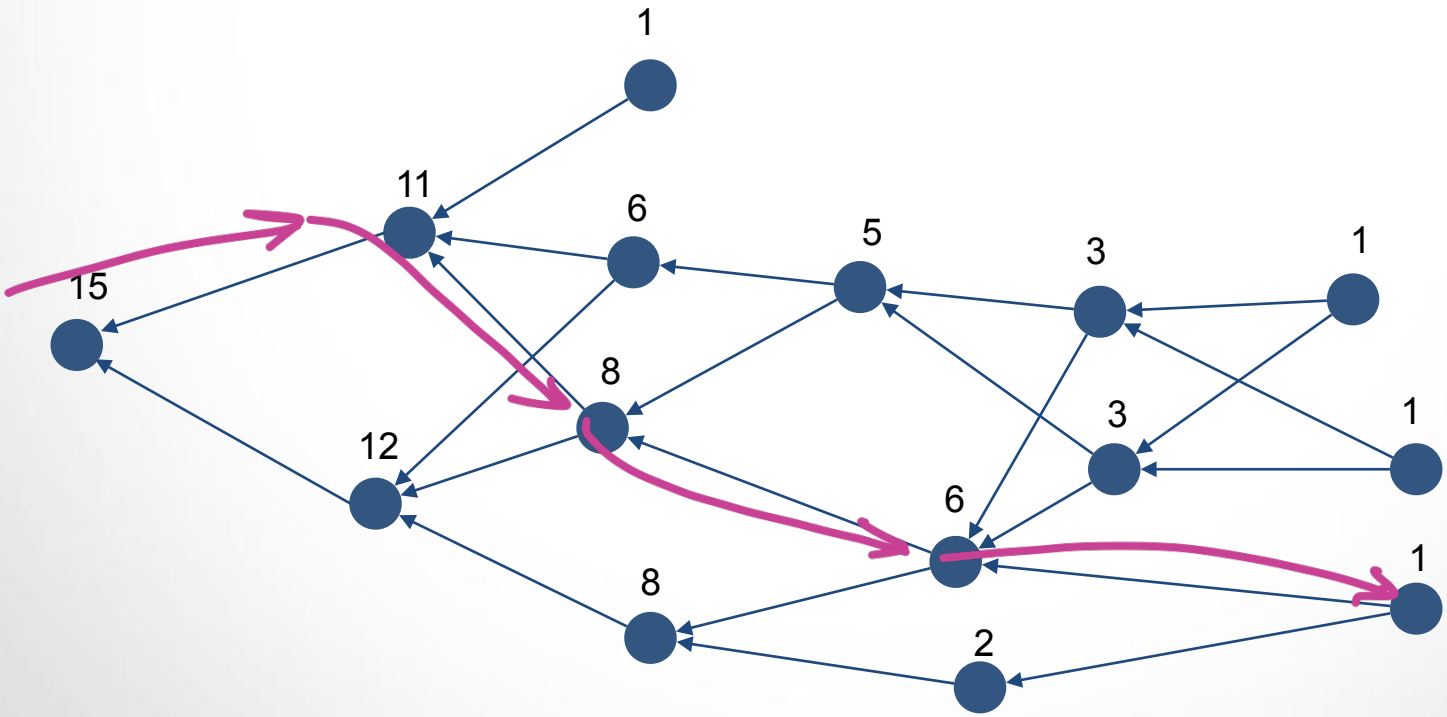
MCMC Tip selection algorithm

MCMC Tip selection algorithm

The Tangle (IOTA)

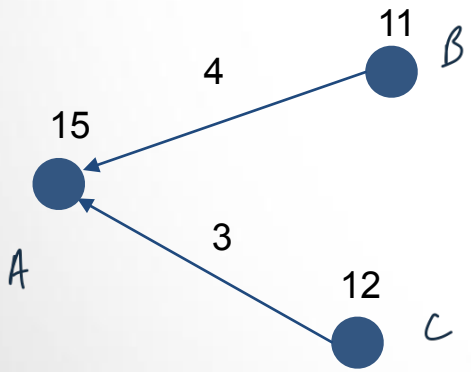
Compute cumulative weight to each site

Perform a random walk



MCMC Tip selection algorithm

The Tangle (IOTA)



Compute cumulative weight to each site

Perform a random walk

Transition function:

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

MCMC

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

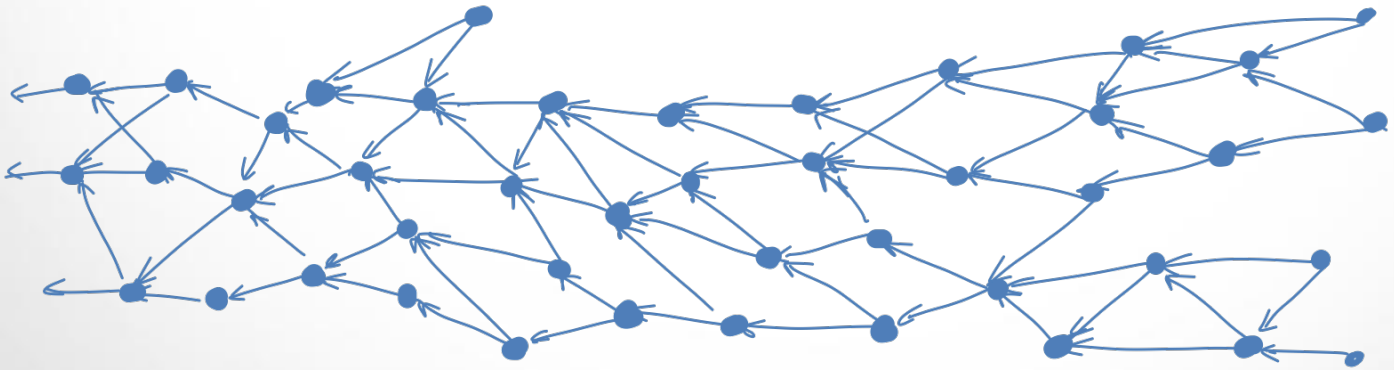
LMCMC

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

Number of tips

How many tips are left behind ?

How many tips over the time ?



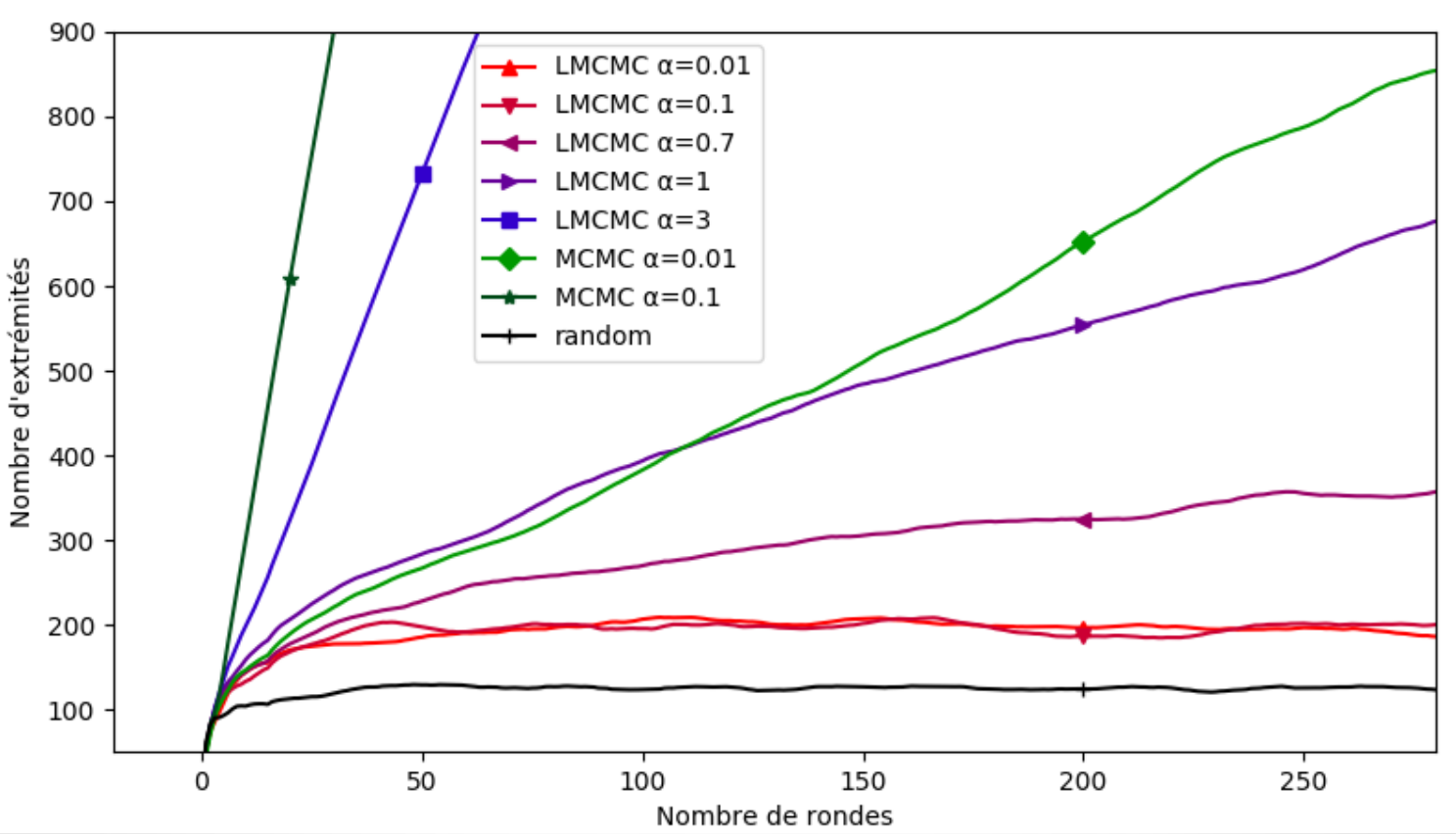
Number of tips

How many tips are left behind ?

How many tips over the time ?

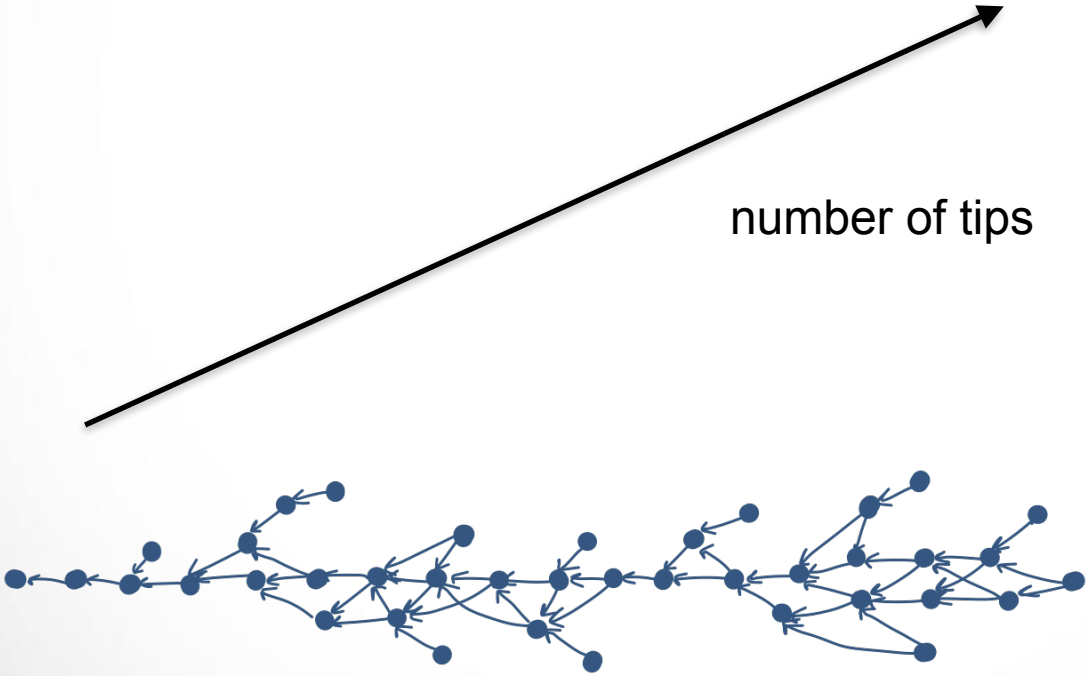
Number of tips

By simulation (discrete time)



Number of tips

What the tangle looks like for high alpha



Double Spending Attack

Double Spending Attack

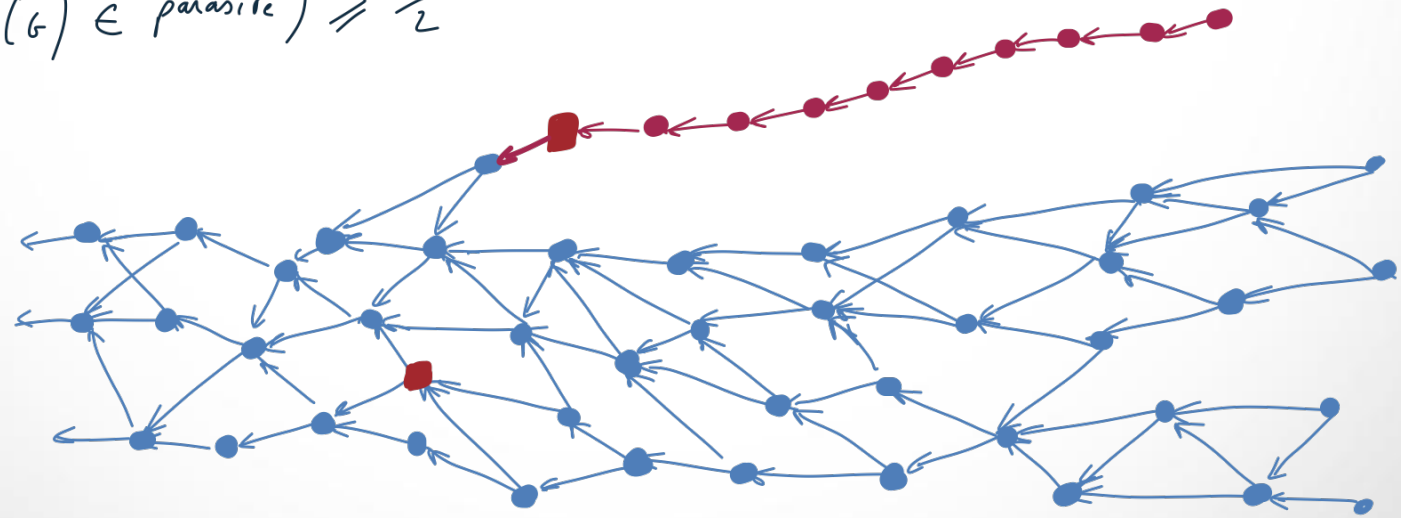
- Alice sends 10 IOTA to Bob for a sandwich
- Bob waits to see the transaction in the Tangle
- Bob gives Alice the sandwich
- Alice generates a lots of transactions so that her first transaction is discarded
- Alice eats the sandwich

Double Spending Attack

The parasite chain attack

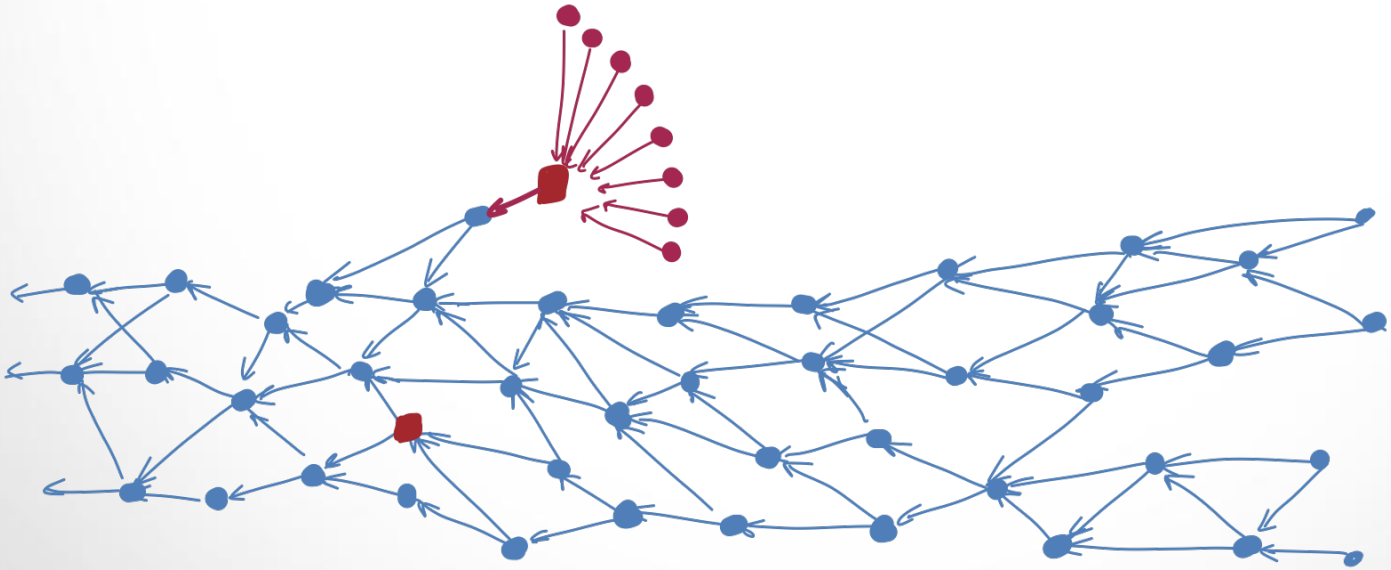
How many red site so that:

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



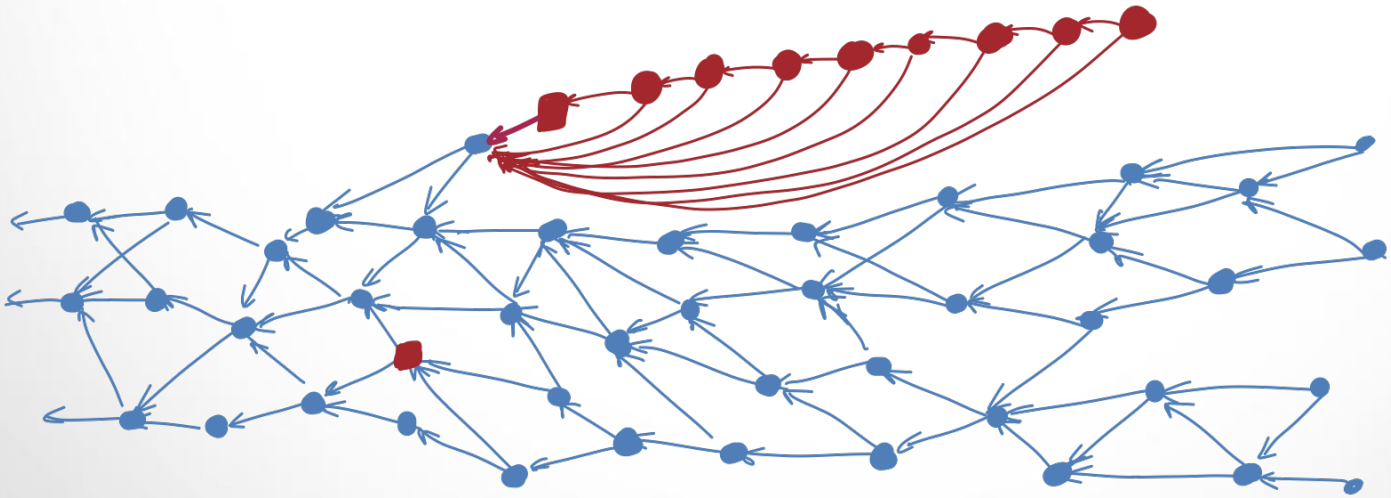
Parasite Chain Attack

The parasite chain attack



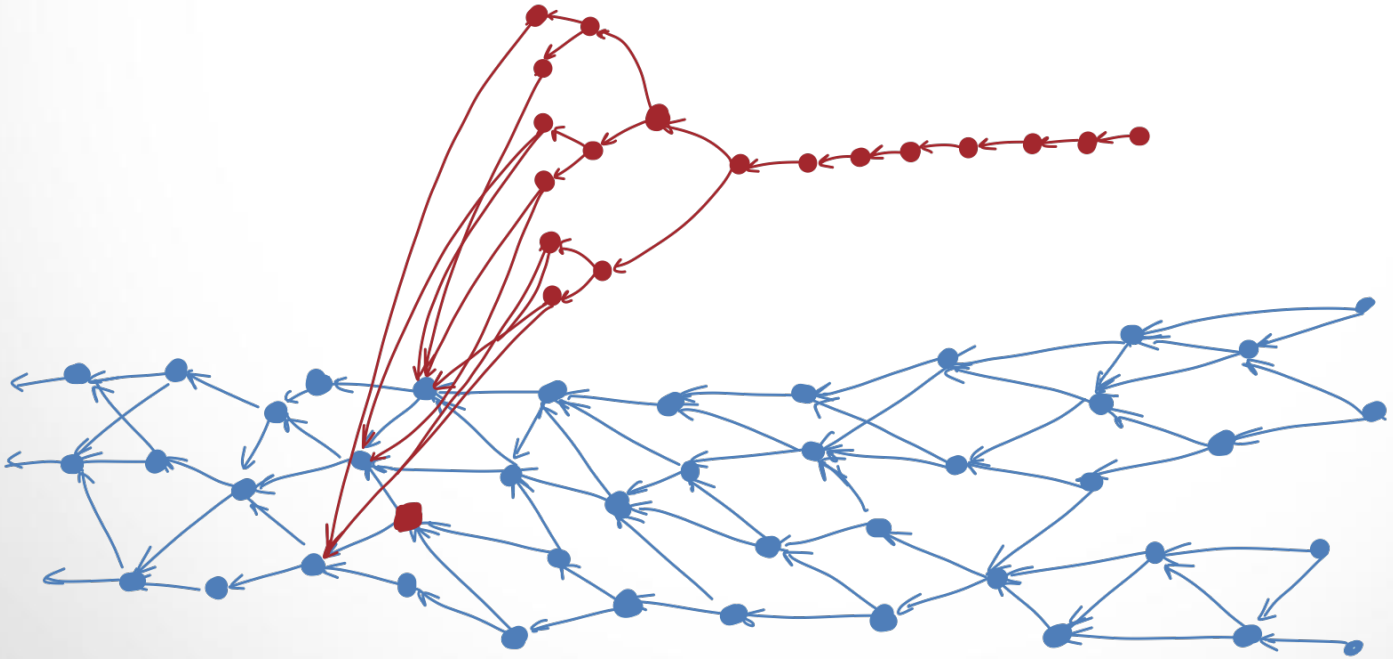
Parasite Chain Attack

The parasite chain attack



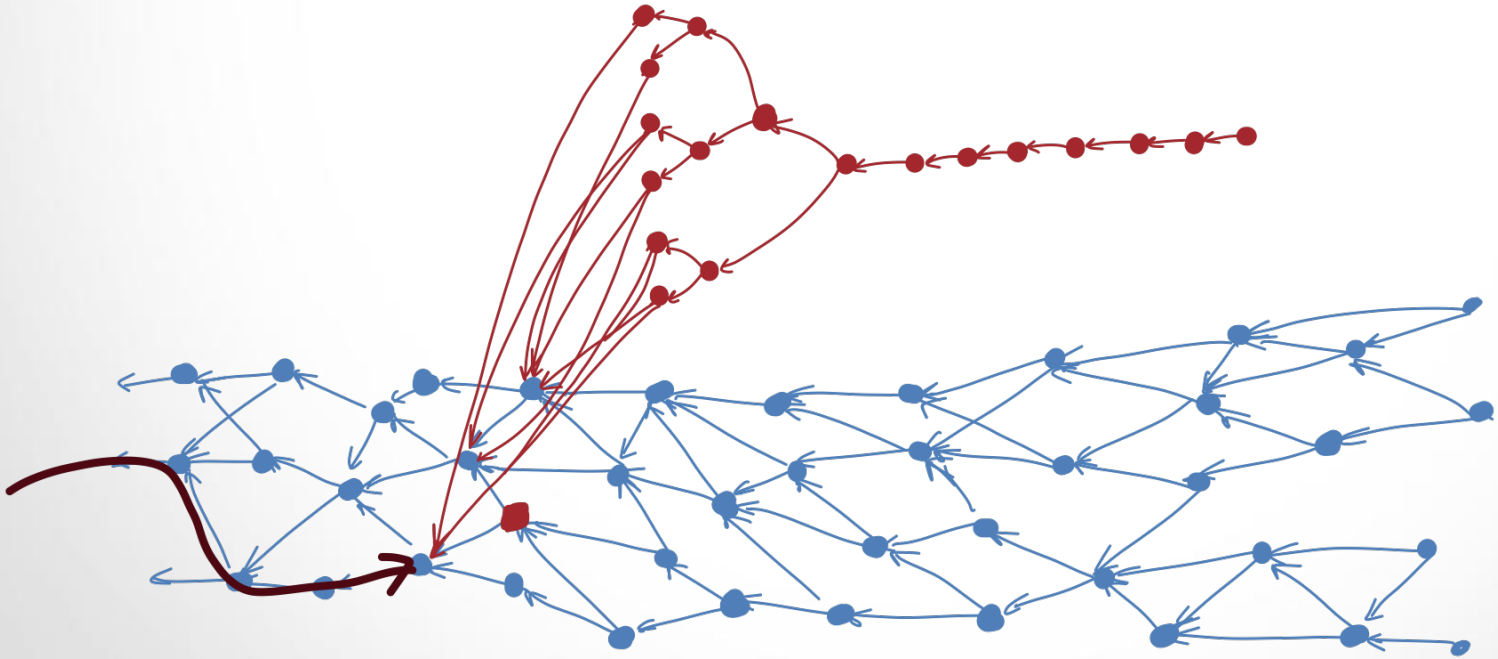
Double Spending Attack

Against MCMC



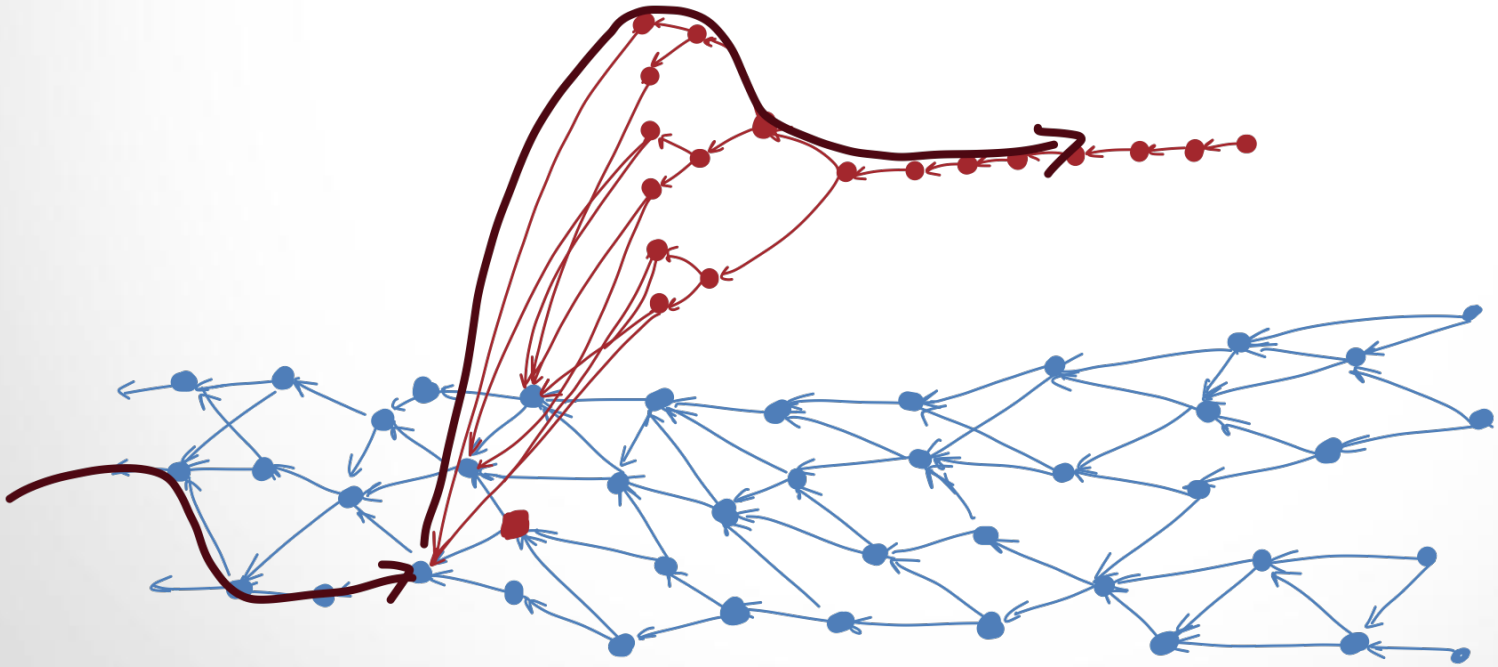
Double Spending Attack

Against MCMC



Double Spending Attack

Against MCMC



MCMC algorithm

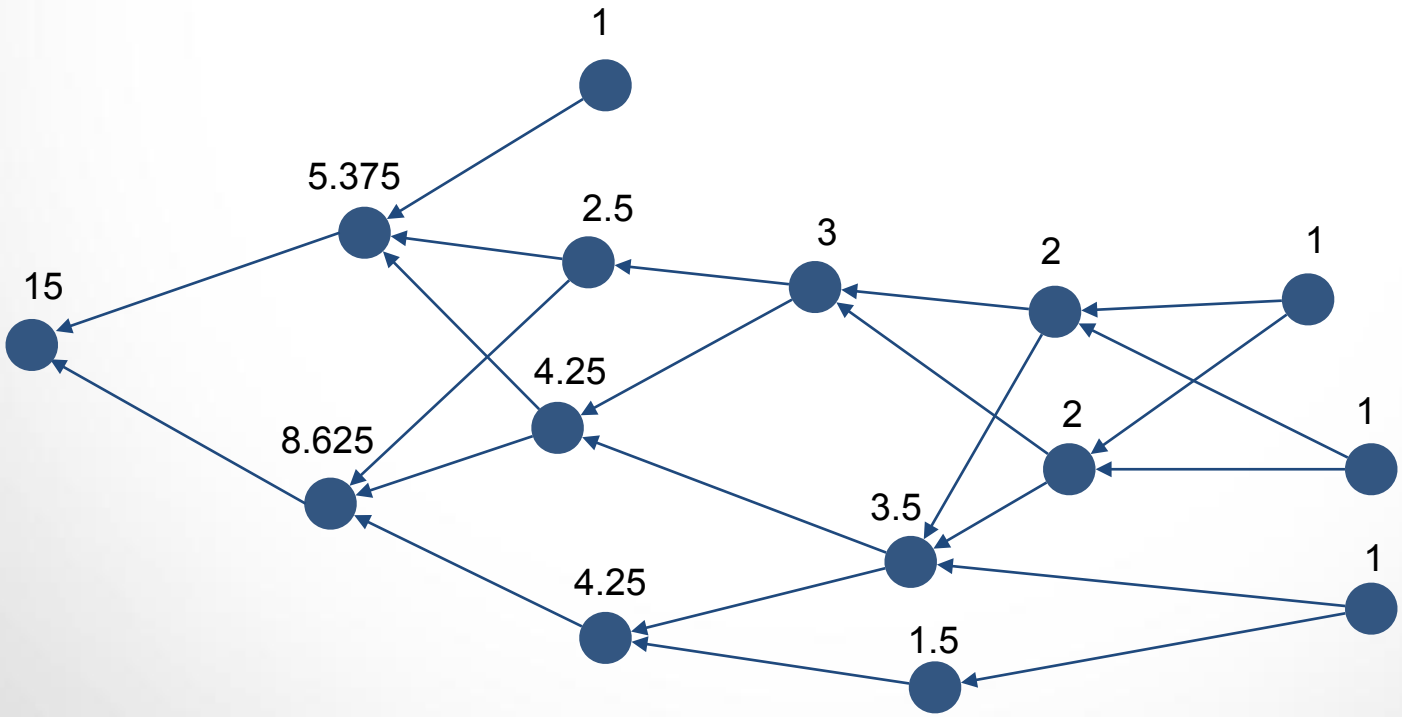
Limitation of the MCMC algorithm

Complexity: $O(n^2)$ to append a new site
Security ratio: tends very slowly towards 1 when alpha is small
Unconfirmed tips: alpha should be small to have a constant number of tips

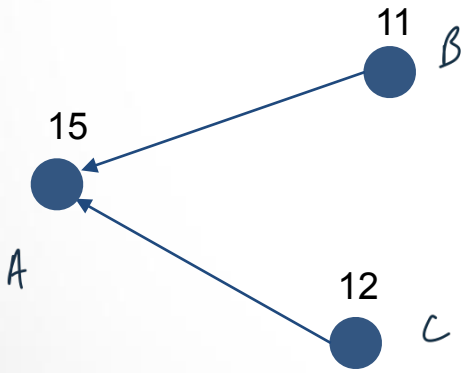
Real cumulative weight

Real cumulative weight

$$w(u) = 1 + \sum_{c \in \text{children}} w(c)/2$$



Random Walk

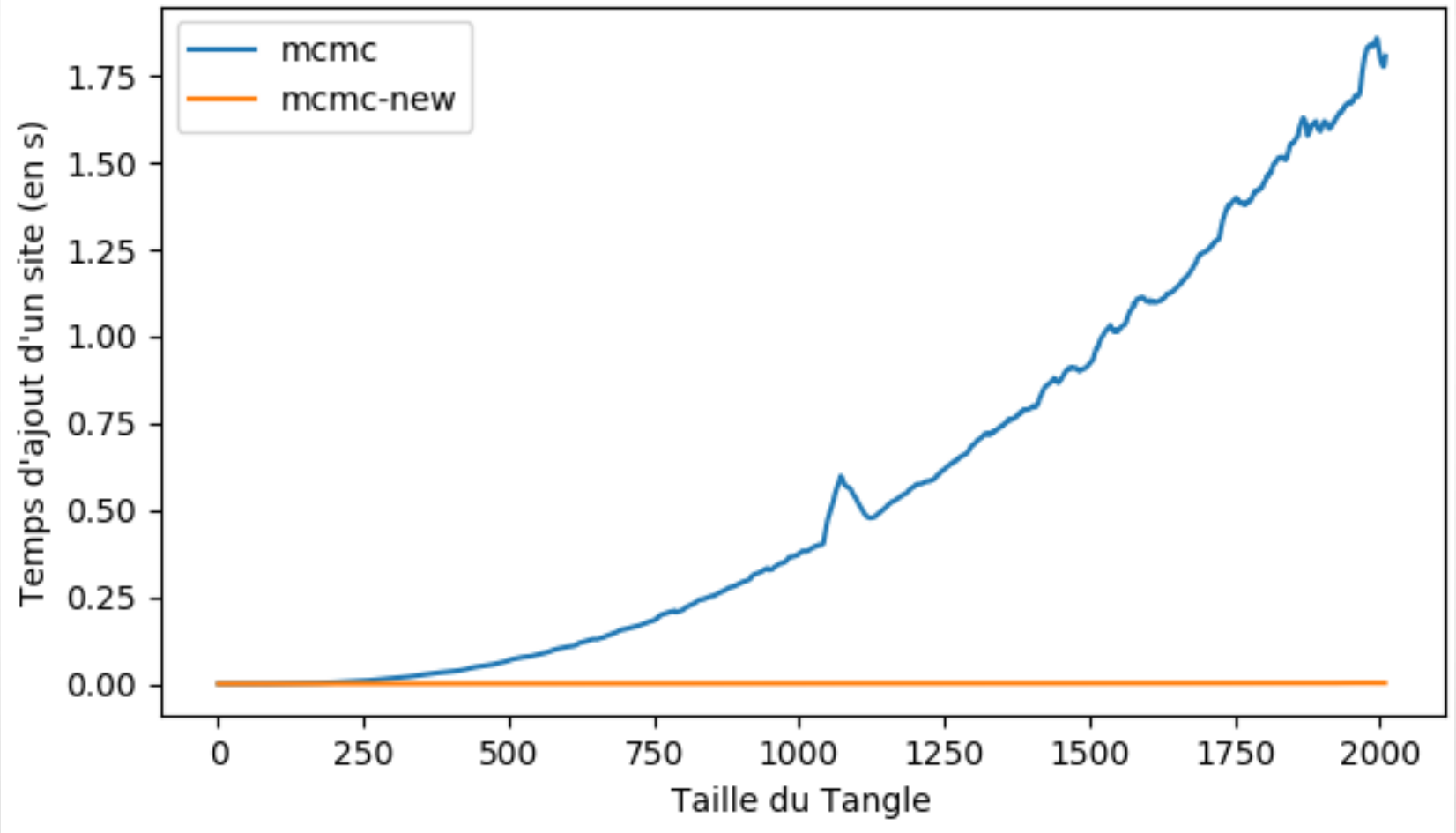


Transition function:

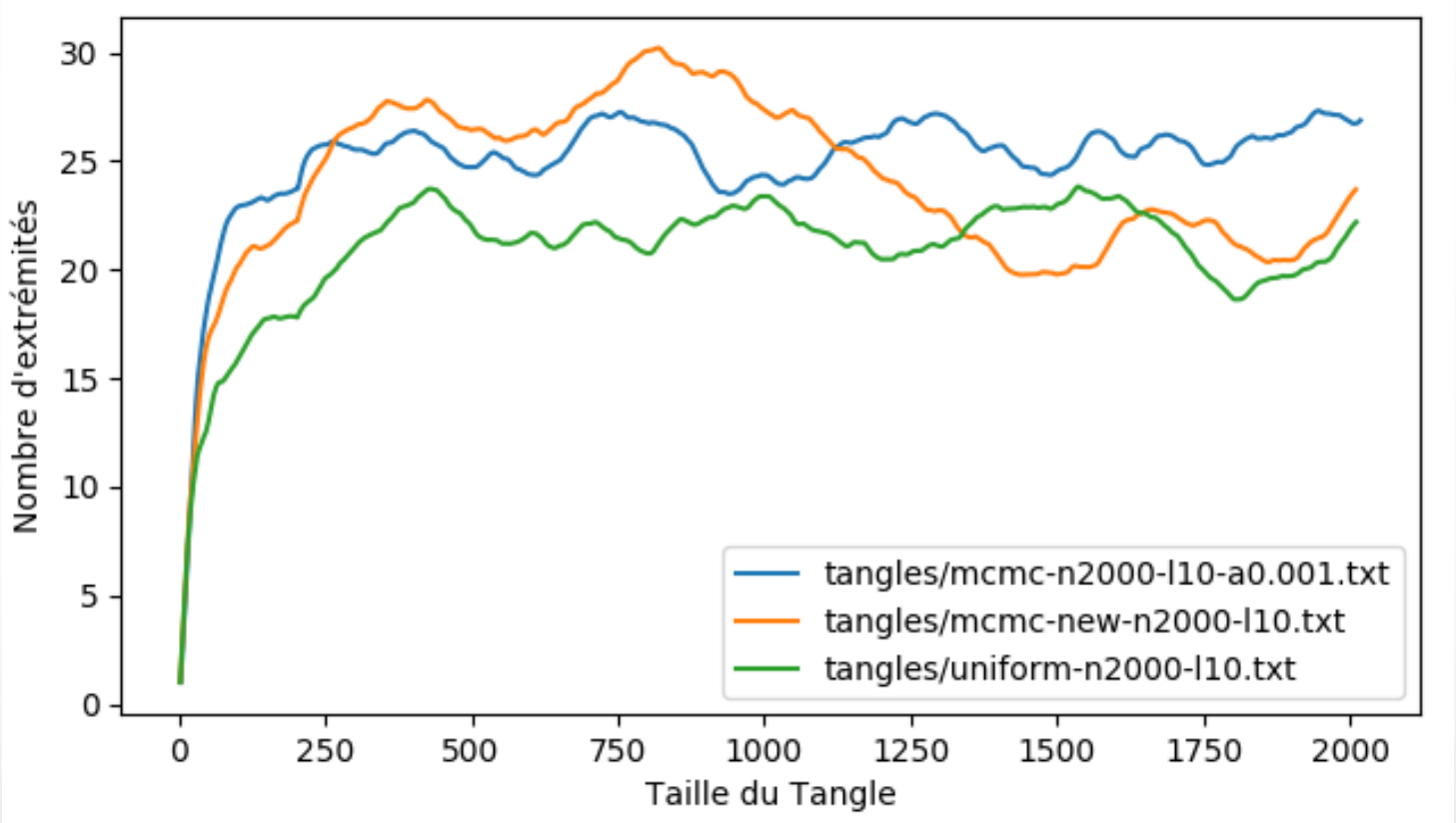
$$P_{A \to B} = \frac{11}{11+12}$$

Comparison

Complexity

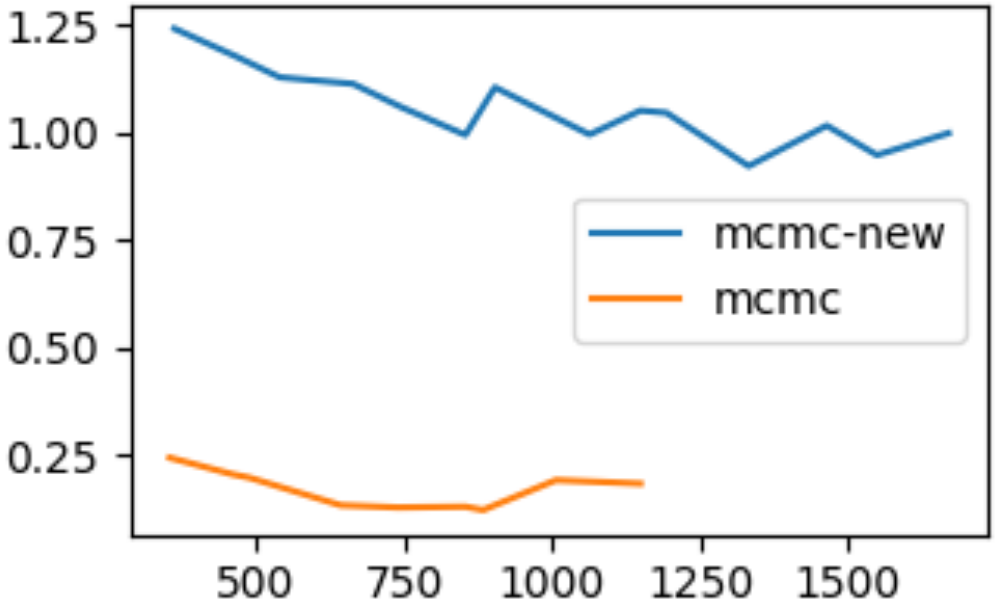

mcmc
mcmc-new
Temps d'ajout d'un site (en s)
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
0
250
500
750
1000
1250
1500
1750
2000
Taille du Tangle

Tips over time



Resistance to parasite chain

Security factor



Future of IOTA

Remove the coordinator

Conflict resolution based on a Fast Probabilistic Consensus (also using Proof of Stake)

Simpler PoW for trusted nodes

Simpler Tip Selection Algorithm

Nothing planed related to smart-contract

Thank you for your attention!