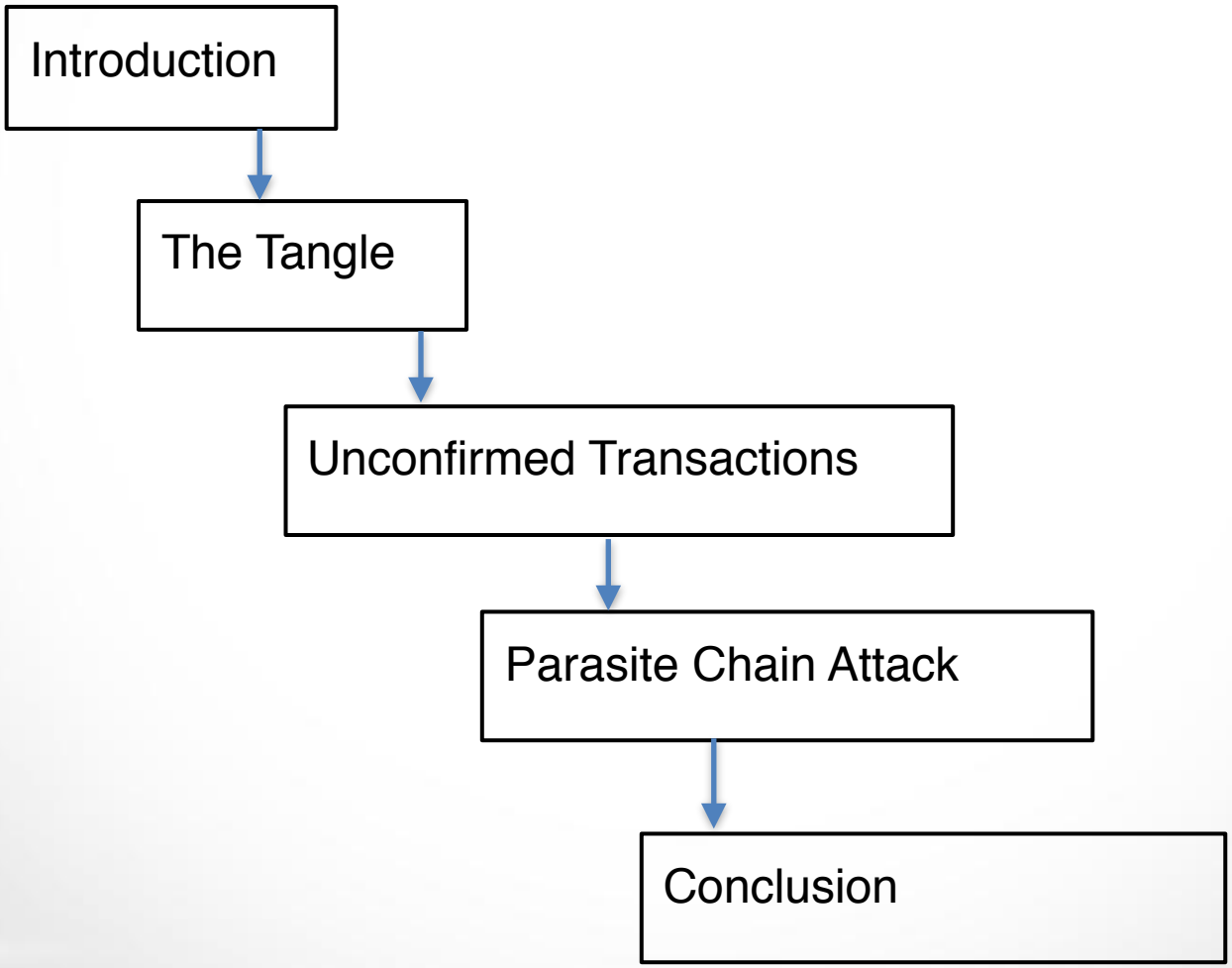
The graph of transactions in the IOTA cryptocurrency

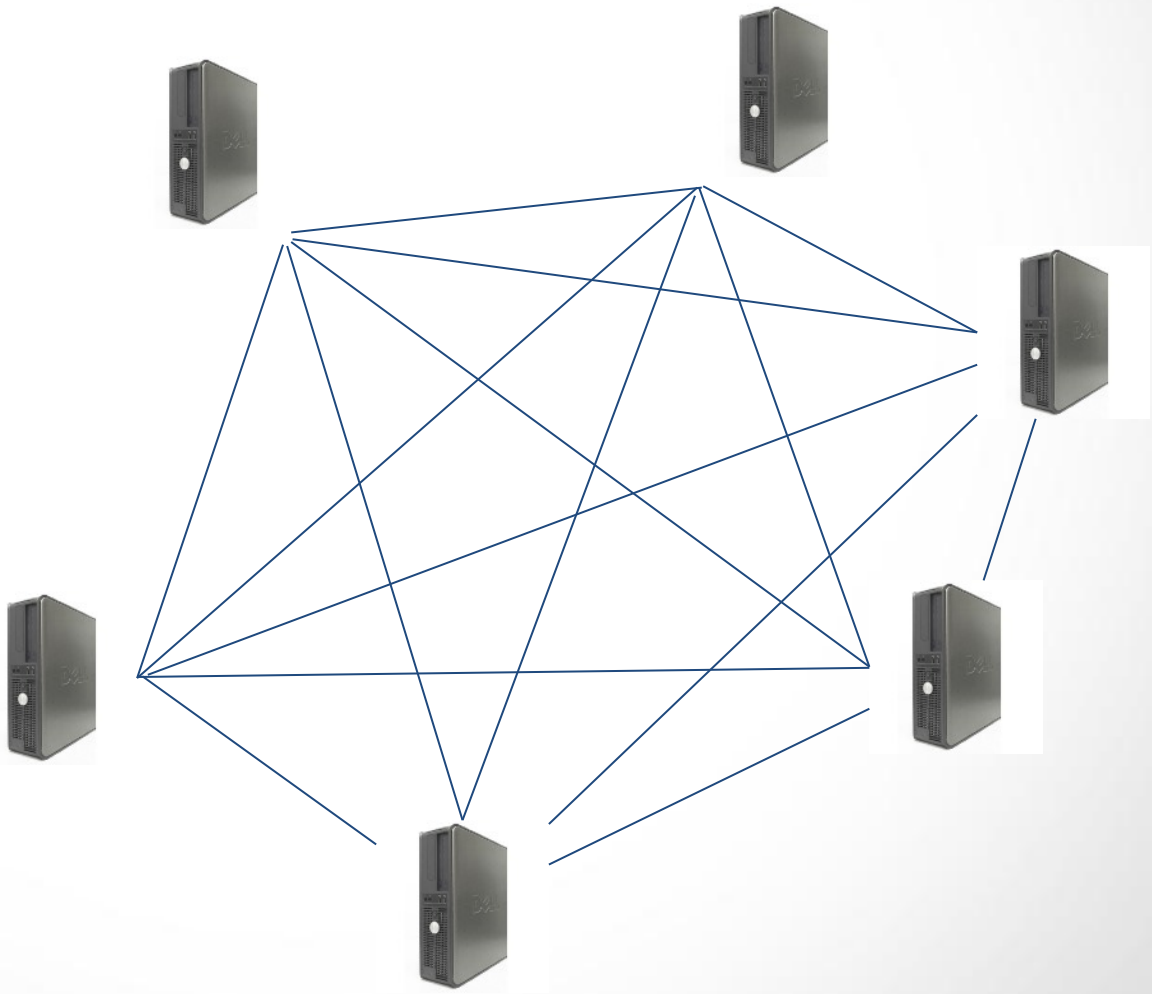
Quentin Bramas bramas@unistra.fr

Jun, 20th, 2018, Clermont-Ferrand

Talk Chain

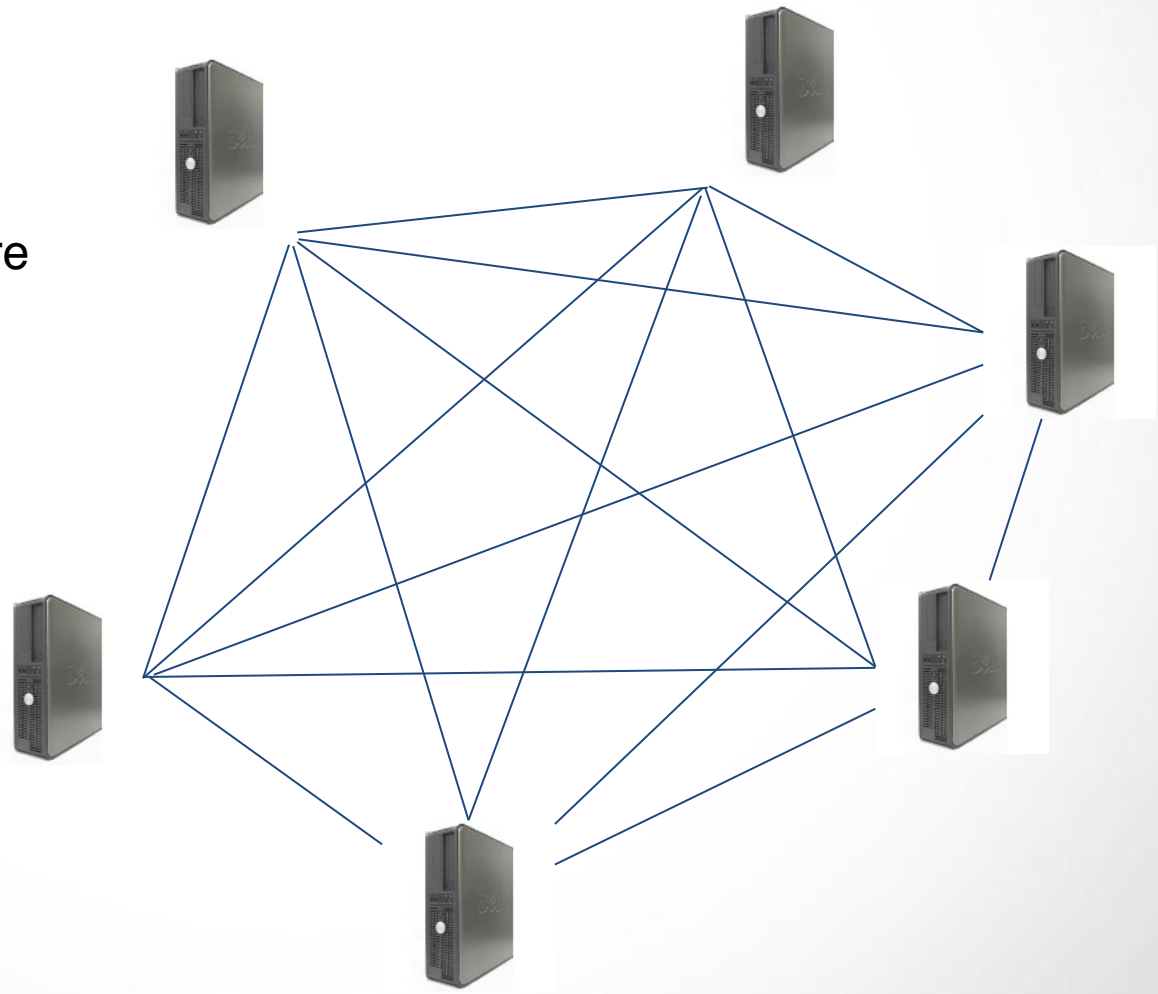

Introduction
The Tangle
Unconfirmed Transactions
Parasite Chain Attack
Conclusion

Data is distributed :



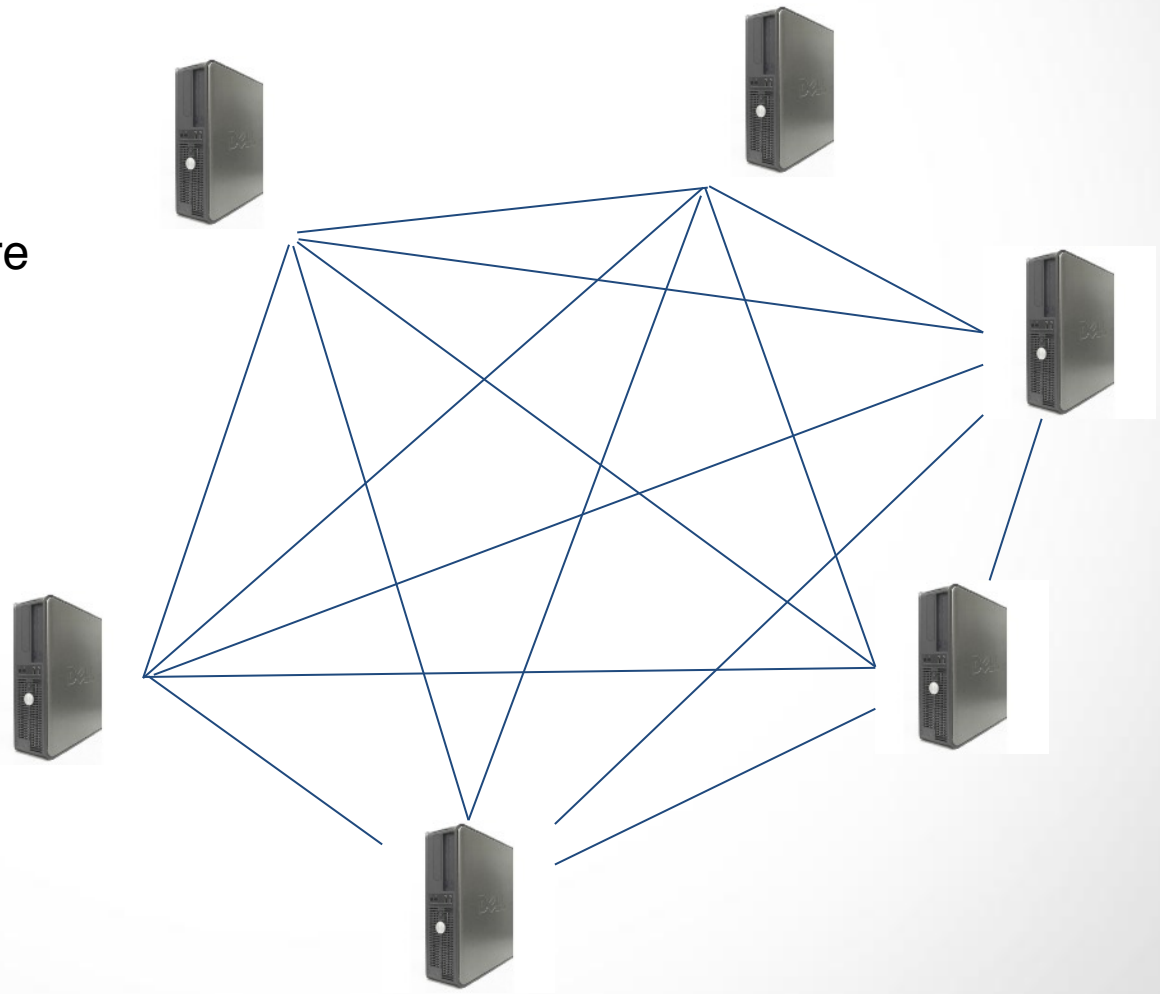
Data is distributed :

- no single point of failure



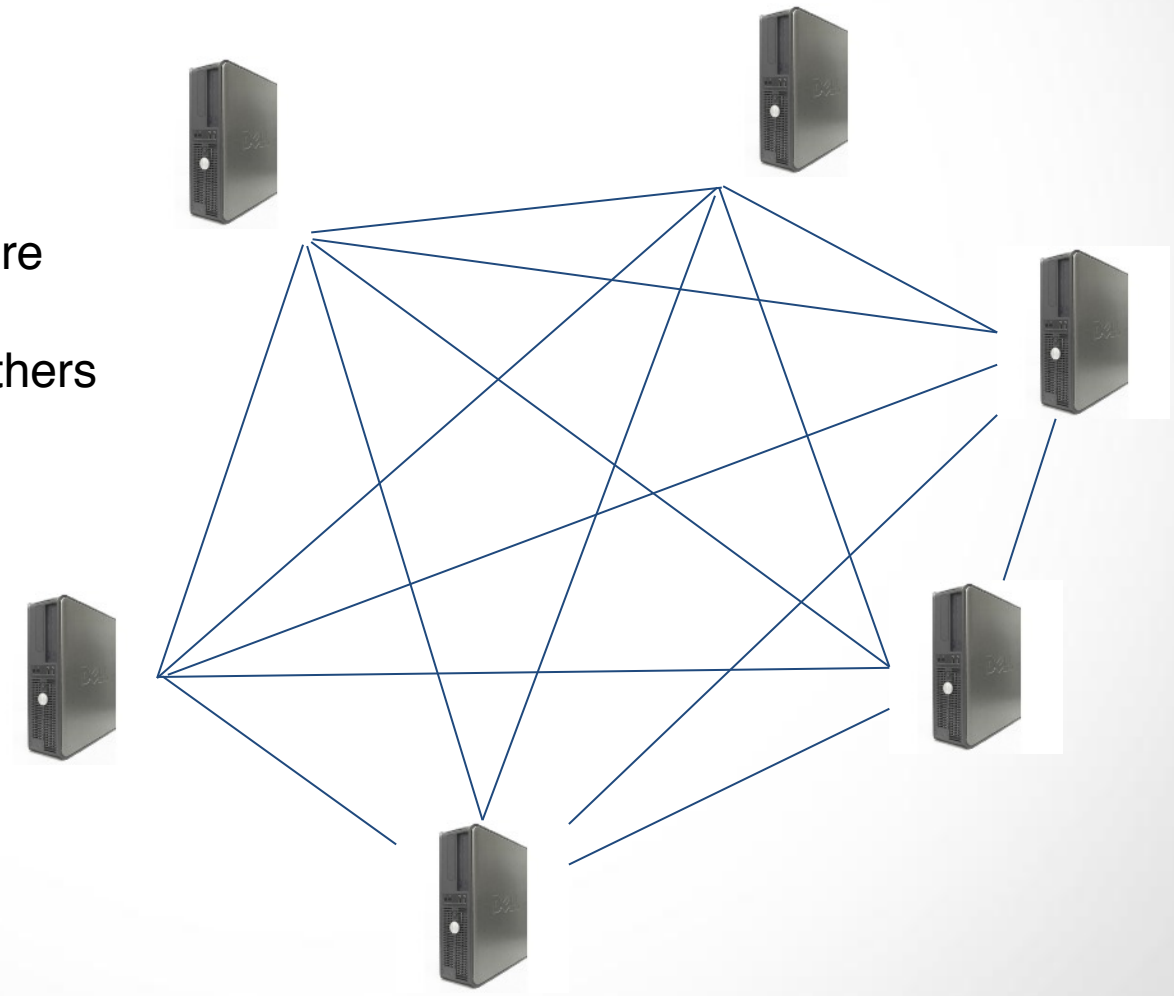
Data is distributed :

- no single point of failure
- no central Authority



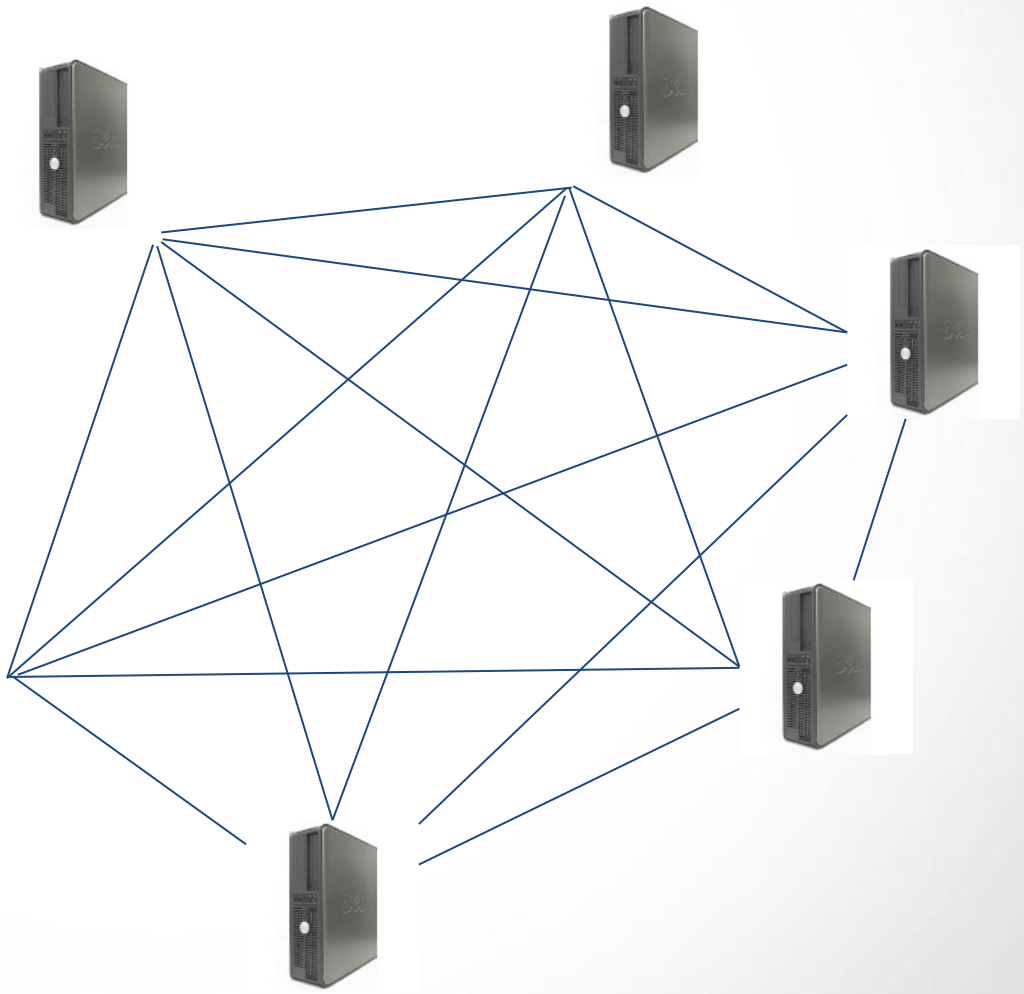
Data is distributed :

- no single point of failure
- no central Authority
- no need to trust the others

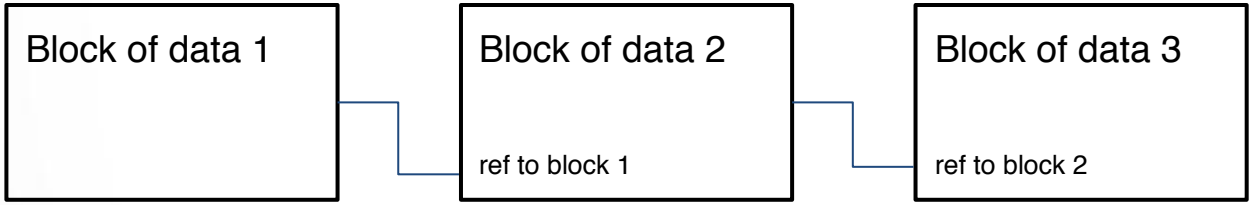


Data is distributed :

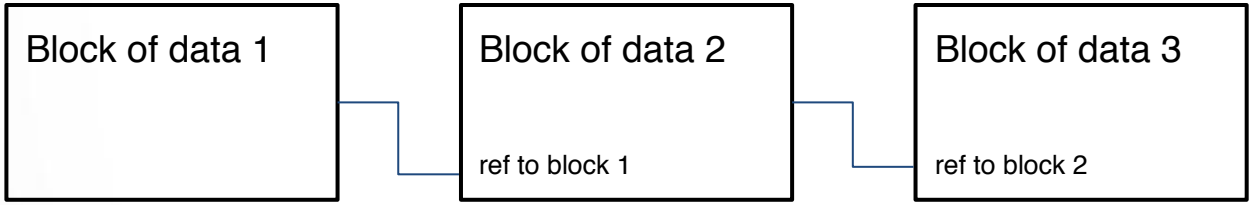
- no single point of failure
- no central Authority
- no need to trust the others



Blockchain:

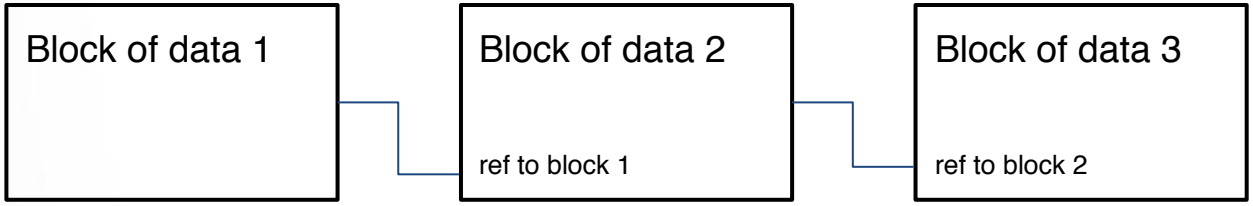

Block of data 1
Block of data 2
ref to block 1
Block of data 3
ref to block 2

Blockchain:



Basic principle of the Bitcoin Protocol :

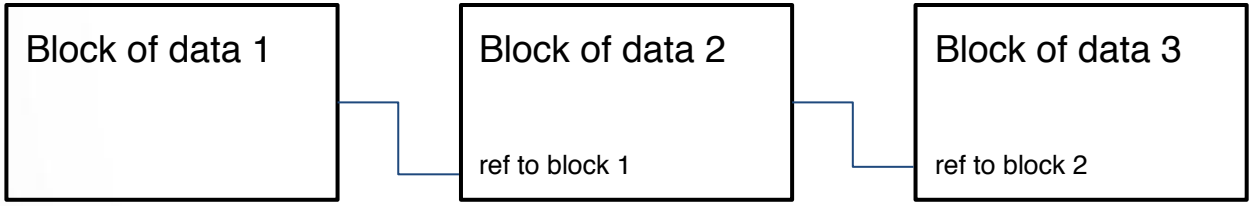
Blockchain:



Basic principle of the Bitcoin Protocol :

- Choose randomly one node

Blockchain:

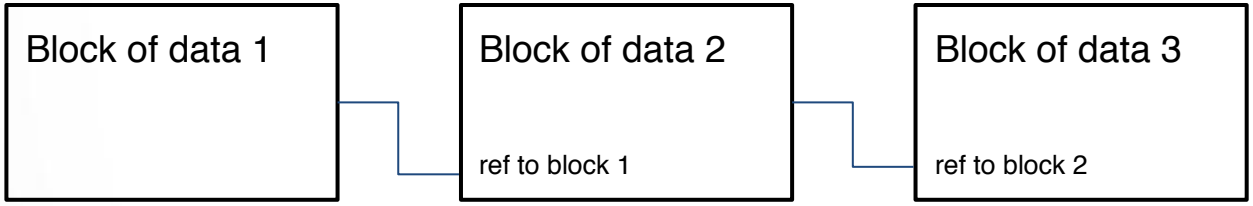


Basic principle of the Bitcoin Protocol :

- Choose randomly one node

The more computing power, the more chance you have to be selected

Blockchain:



Basic principle of the Bitcoin Protocol :

The more computing power, the more chance you have to be selected

- Choose randomly one node
- This node decides what to write in the Blockchain

Problem

It does not scale

Problem

It does not scale

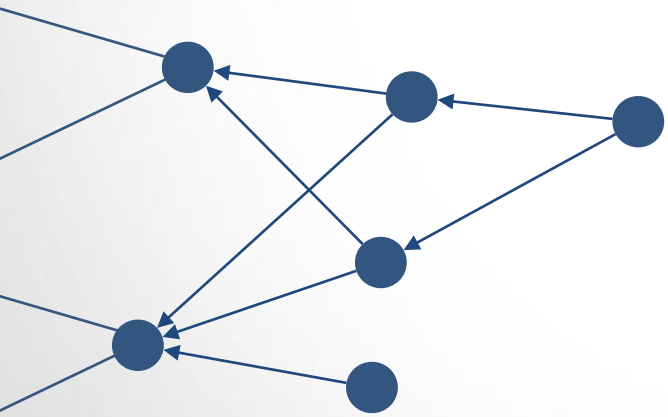
The Tangle (IOTA)

The Tangle (IOTA)

Each transaction is a small block that reference two previous ones

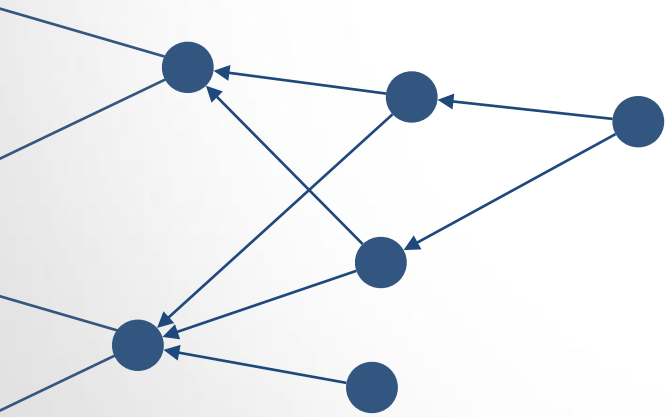
The Tangle (IOTA)

Each transaction is a small block that reference two previous ones



The Tangle (IOTA)

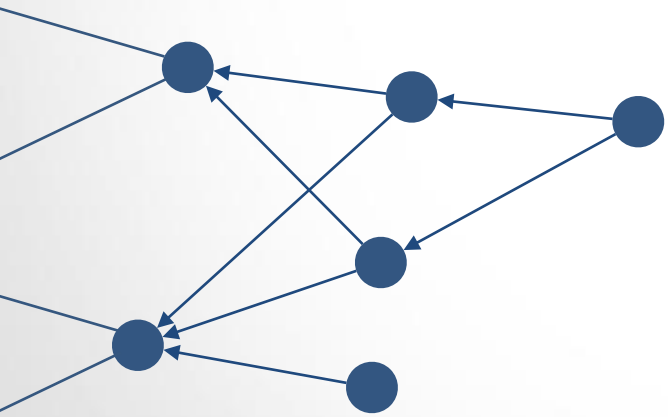
Each transaction is a small block that reference two previous ones



You come up with a DAG
(Directed Acyclic Graph)

The Tangle (IOTA)

Each transaction is a small block that reference two previous ones

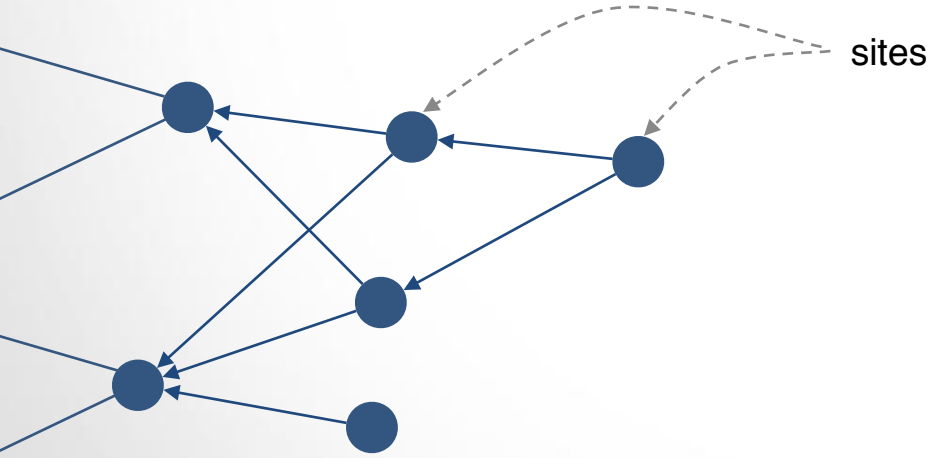


You come up with a DAG
(Directed Acyclic Graph)

You're only limited by bandwidth and storage

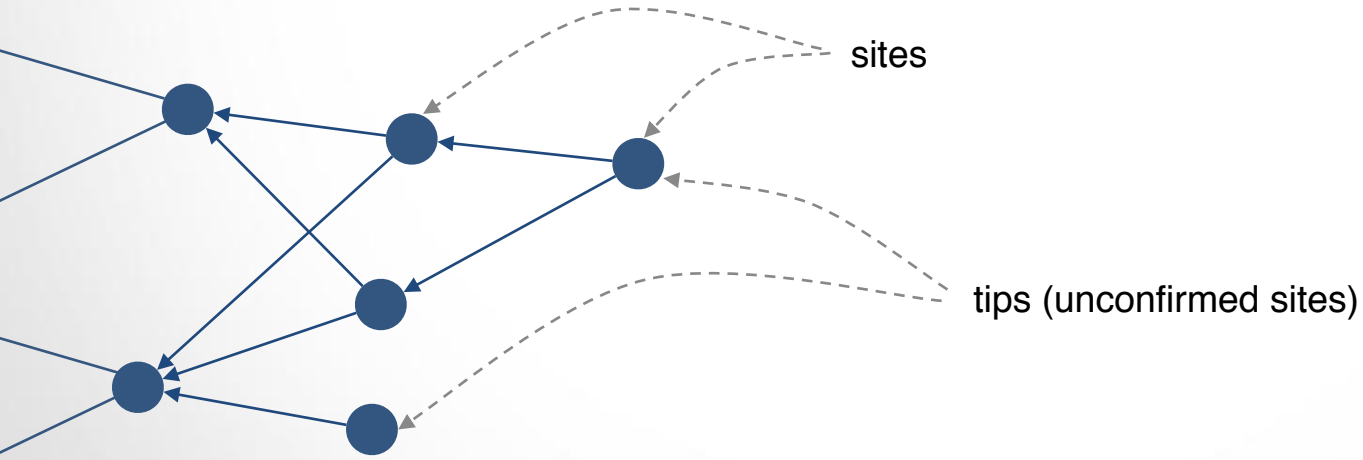
The Tangle (IOTA)

Each transaction is a small block that reference two previous ones



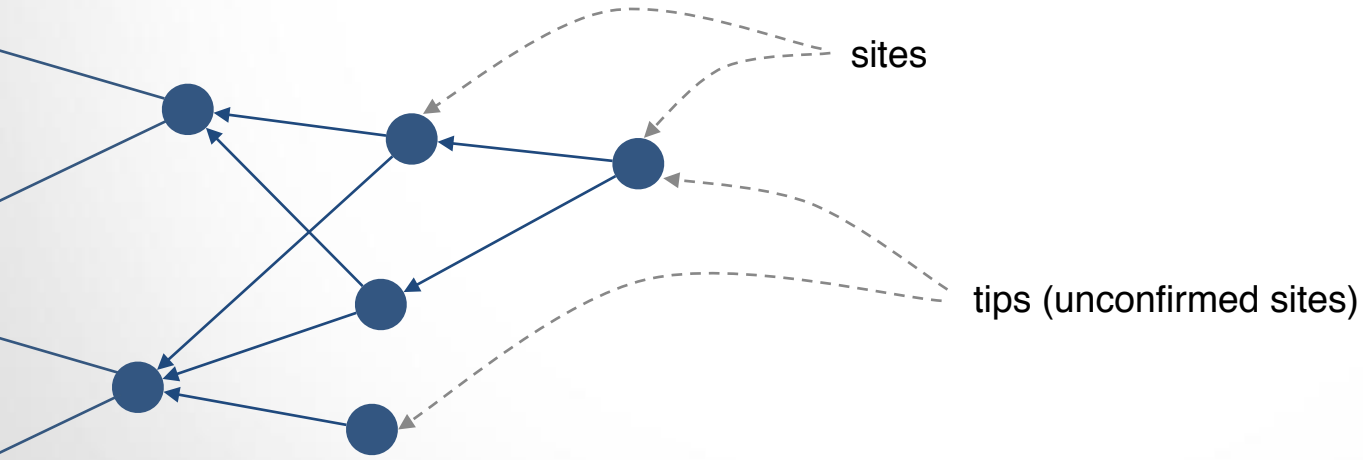
The Tangle (IOTA)

Each transaction is a small block that reference two previous ones



The Tangle (IOTA)

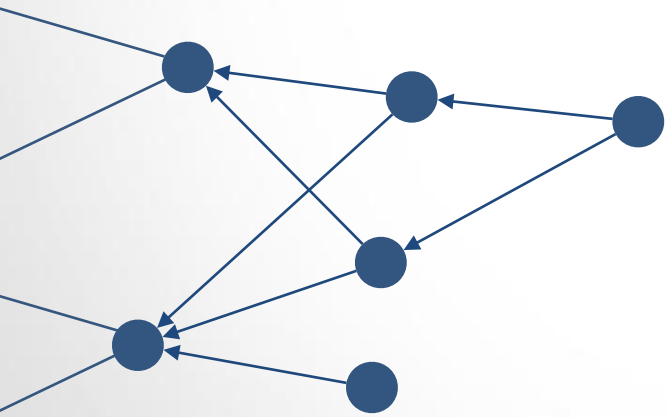
Each transaction is a small block that reference two previous ones



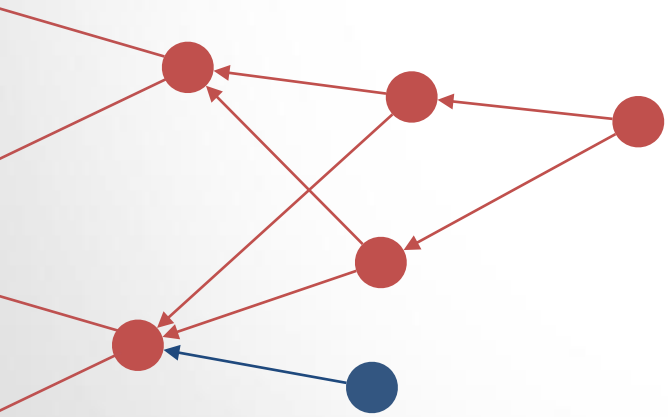
A new site and its parents should not create conflicts.

The Tangle (IOTA)

How to read a value?



The Tangle (IOTA)



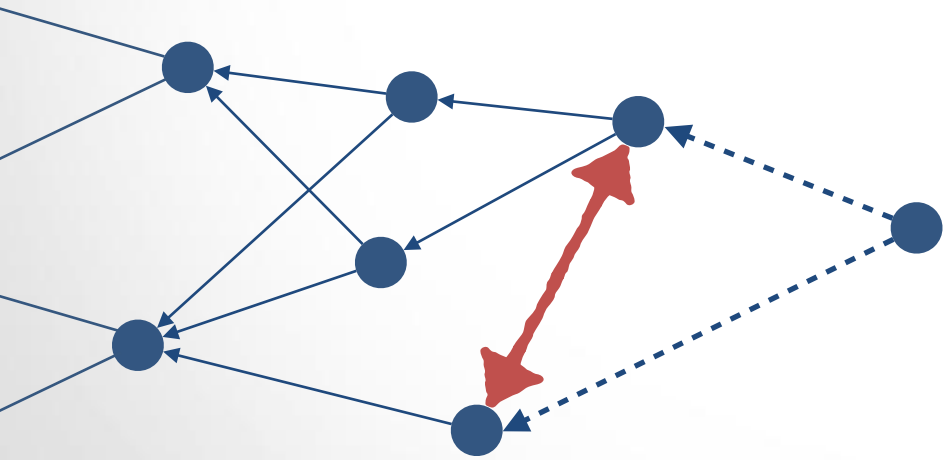
How to read a value?

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

The Tangle (IOTA)

How to read a value?

What if tips are conflicting?

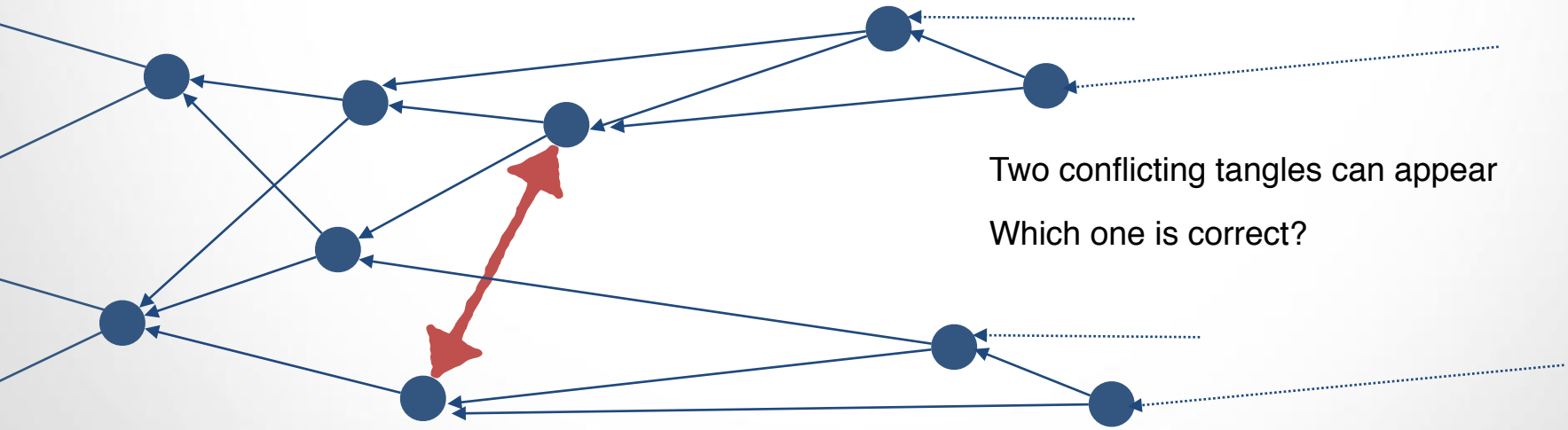


A new site cannot confirm conflicting sites

The Tangle (IOTA)

How to read a value?

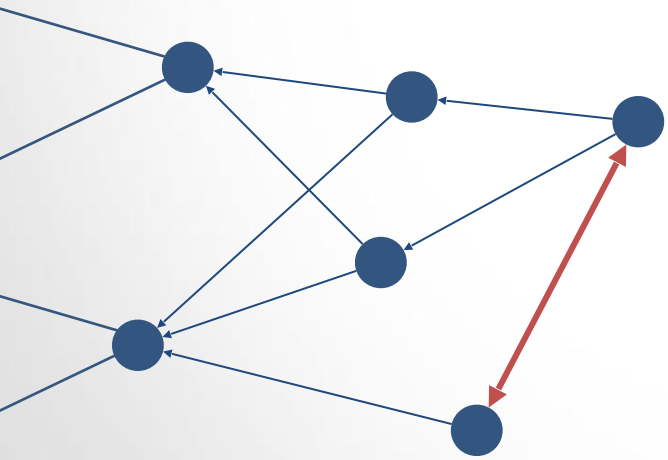
What if tips are conflicting?



Two conflicting tangles can appear

Which one is correct?

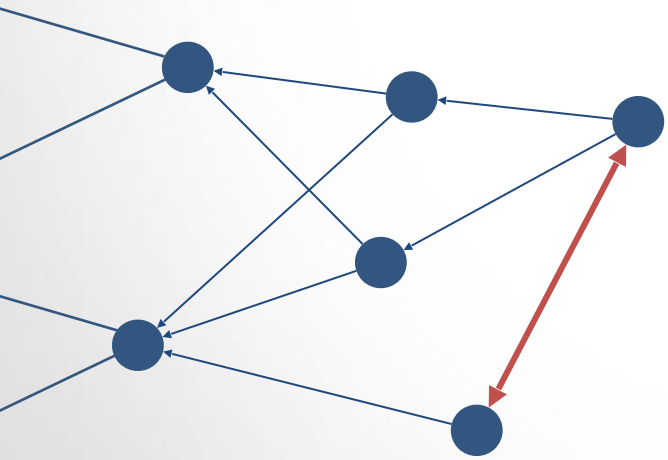
The Tangle (IOTA)



Tip Selection Algorithm (TSA):

- so we know how to read values
- so we know where to extend 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 (IOTA)

In the Tangle, forks are ok if not conflicting

The Tangle (IOTA)

In the Tangle, forks are ok if not conflicting

But conflicting forks are worst in this case

The Tangle (IOTA)

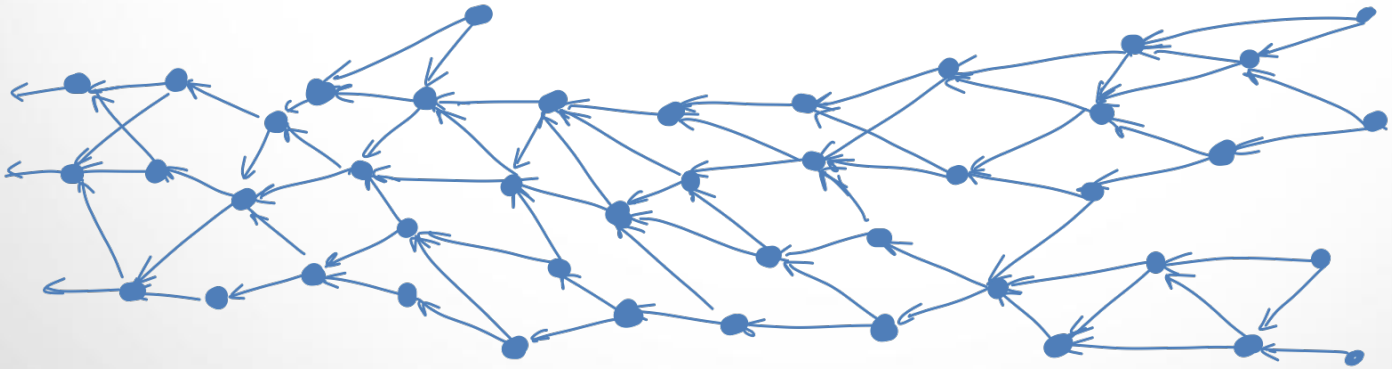
In the Tangle, forks are ok if not conflicting

But conflicting forks are worst in this case

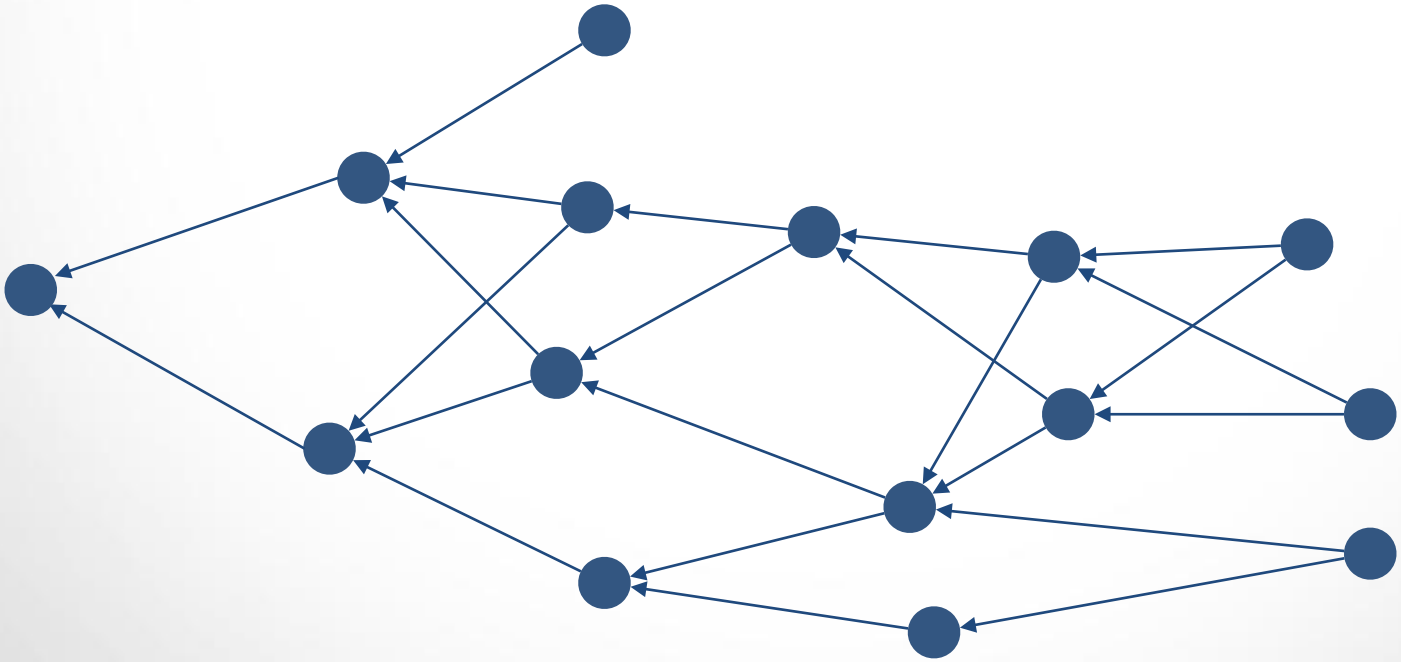
The Tangle (IOTA)

In the Tangle, forks are ok if not conflicting

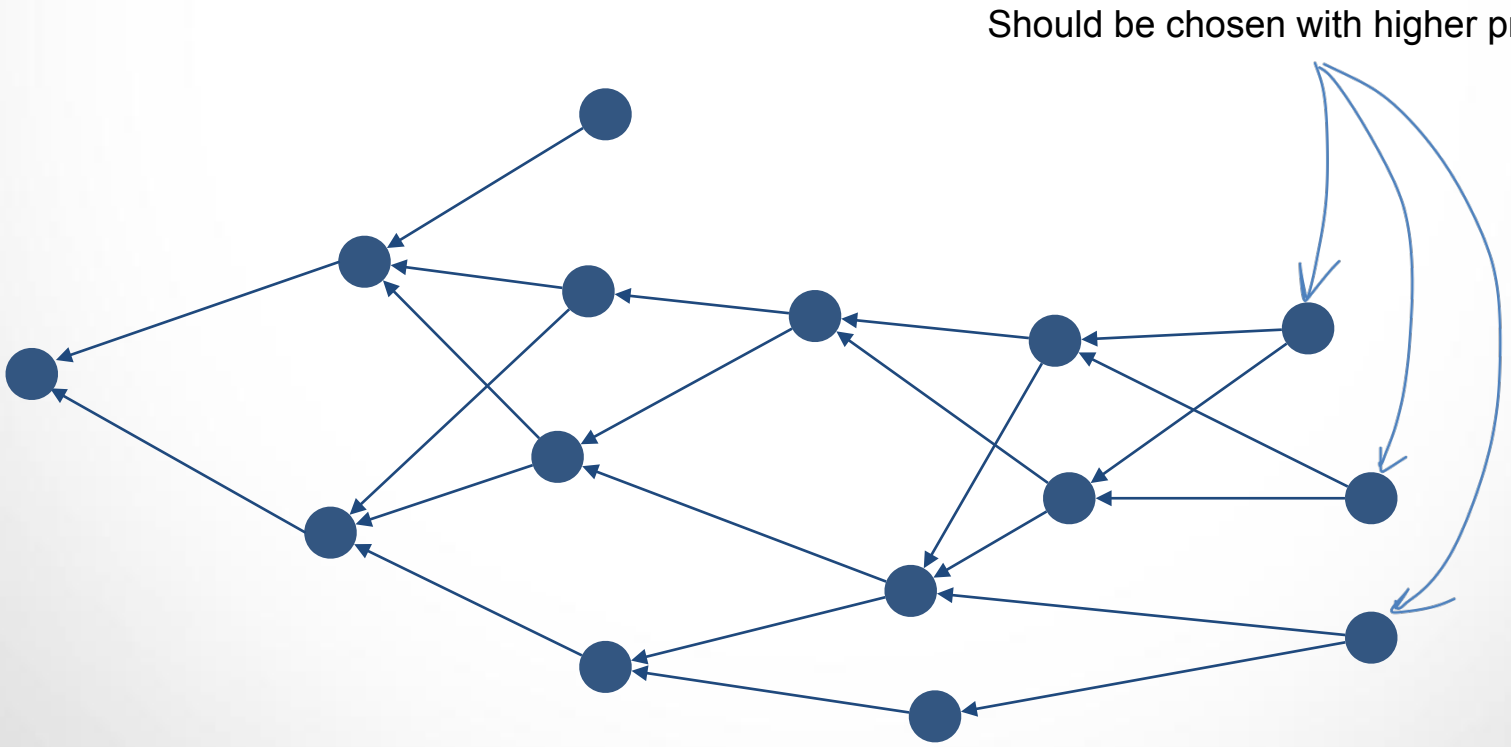
So its better to have something like this



The Tangle (IOTA)

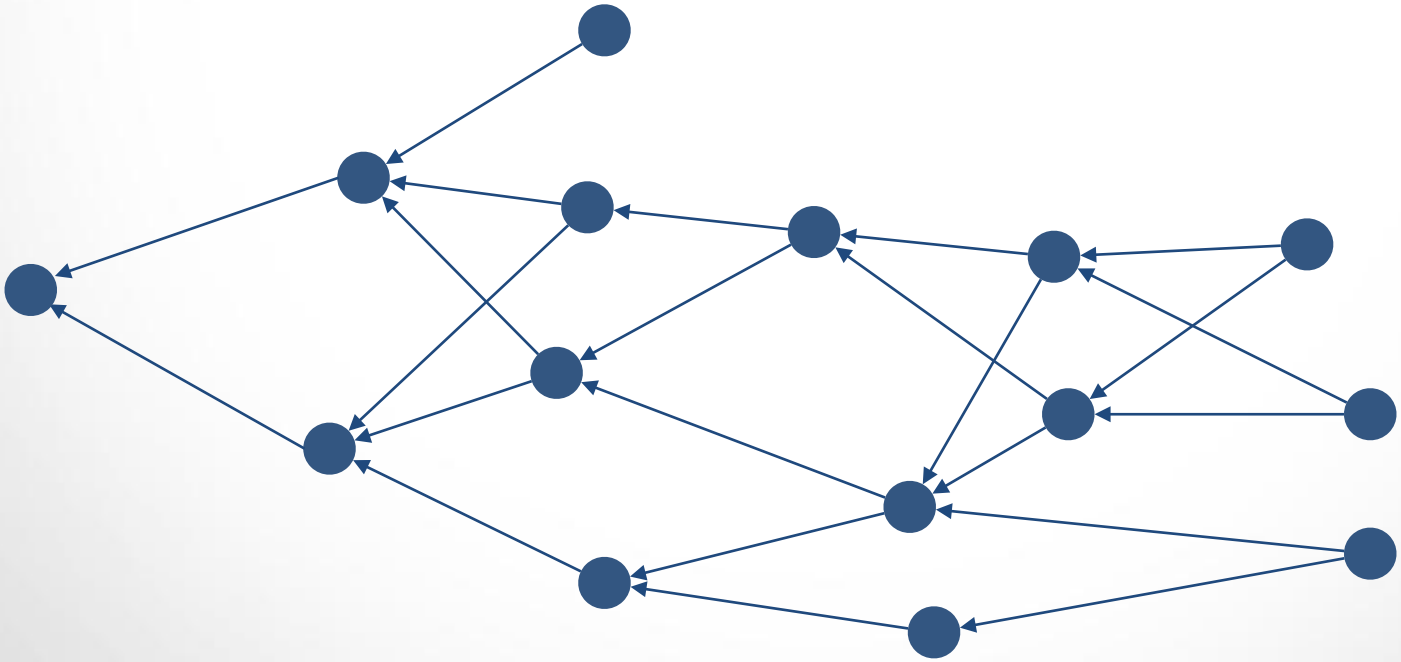


The Tangle (IOTA)



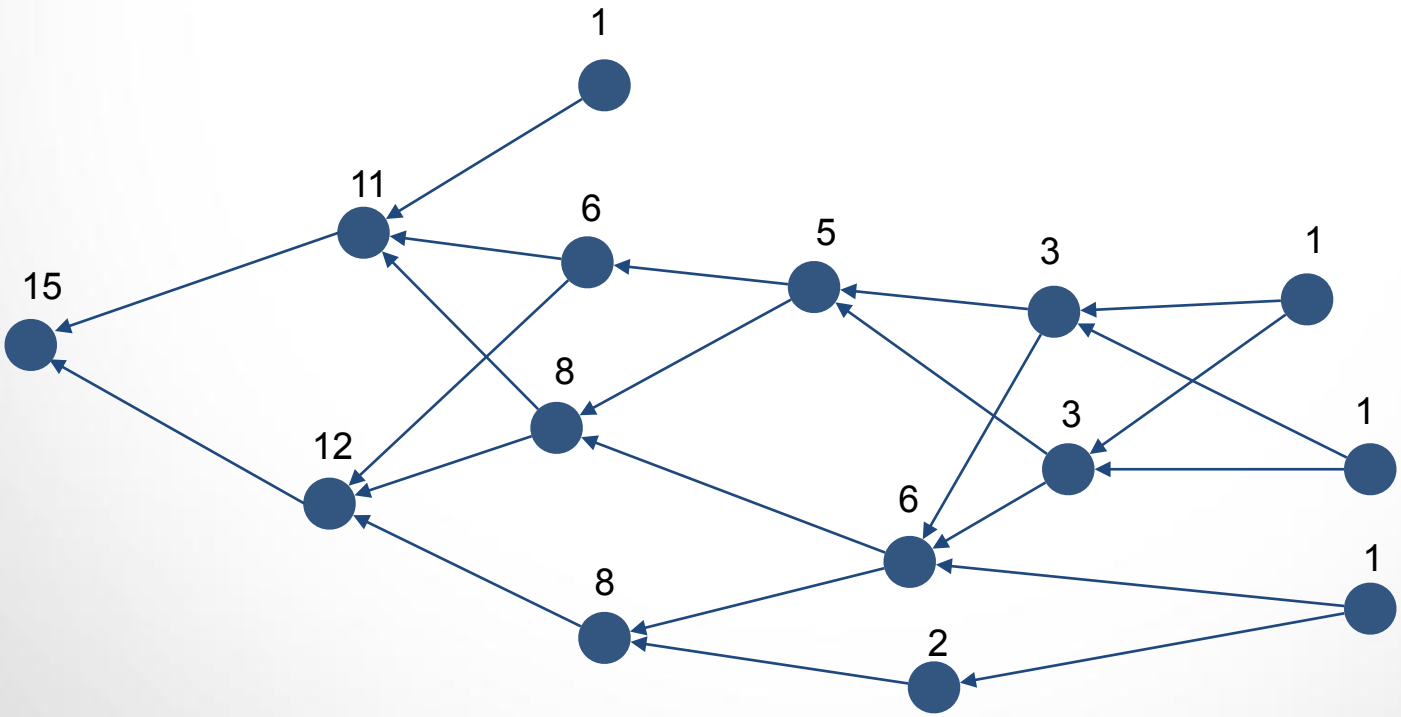
The Tangle (IOTA)

Compute cumulative weight to each site



The Tangle (IOTA)

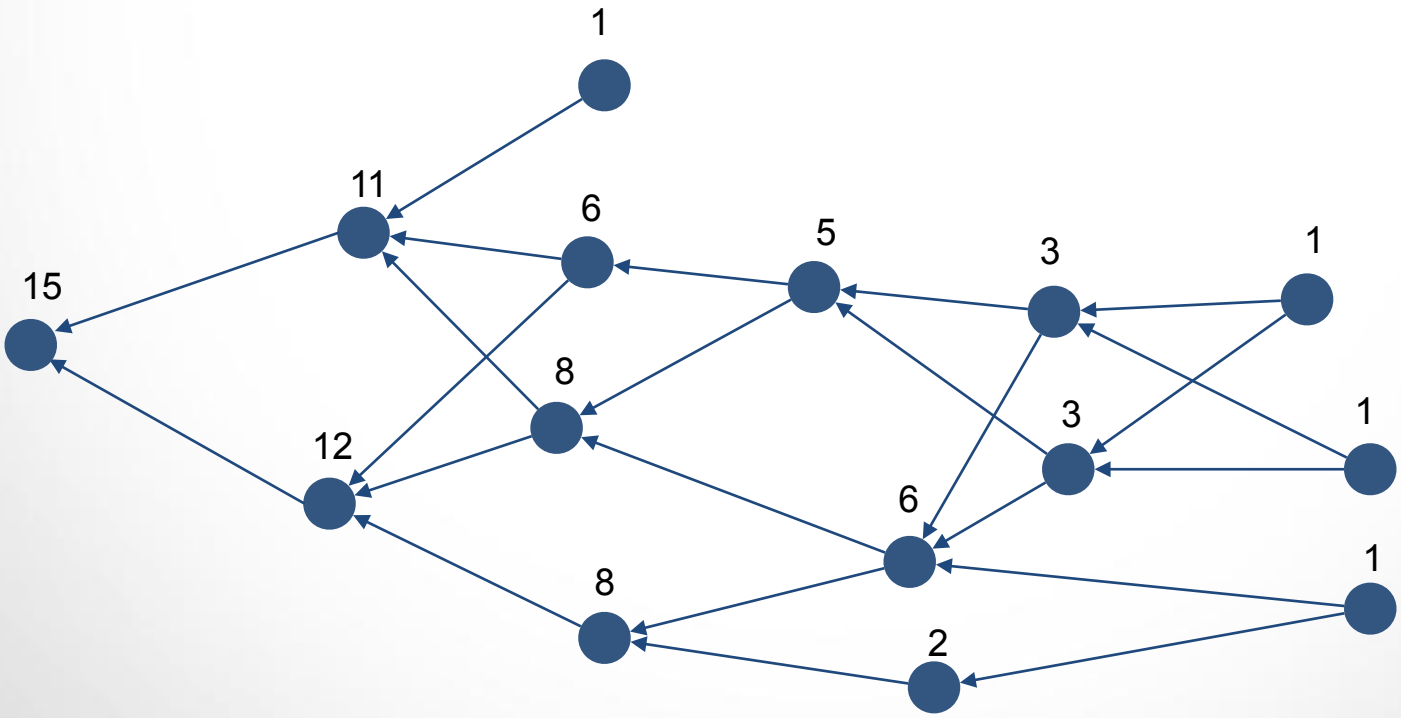
Compute cumulative weight to each site



The Tangle (IOTA)

Compute cumulative weight to each site

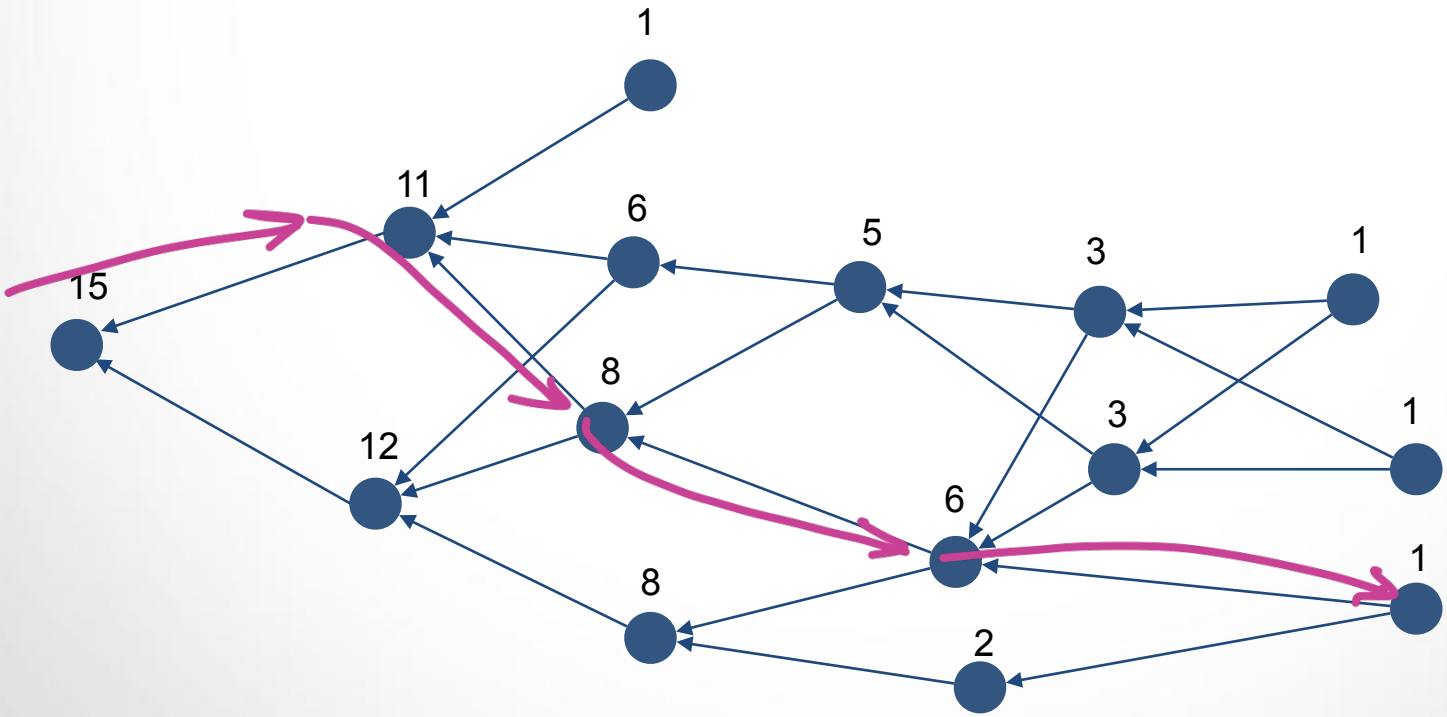
Perform a random walk



The Tangle (IOTA)

Compute cumulative weight to each site

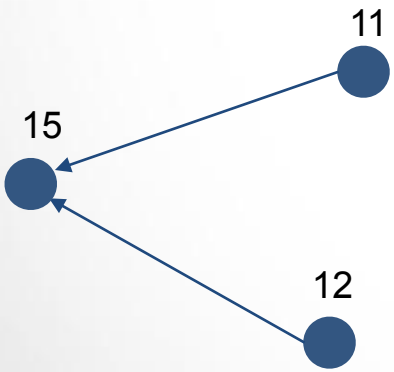
Perform a random walk



The Tangle (IOTA)

Compute cumulative weight to each site

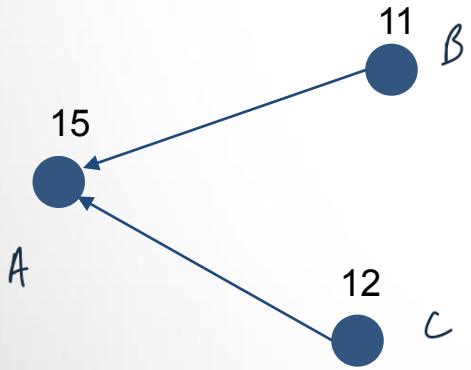
Perform a random walk



The Tangle (IOTA)

Compute cumulative weight to each site

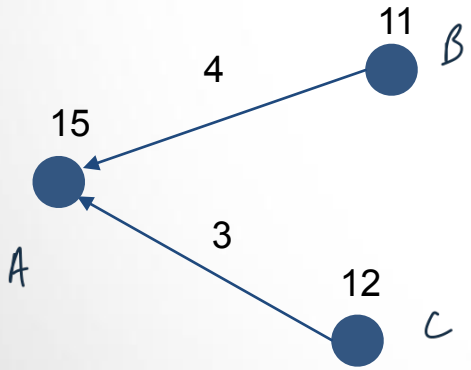
Perform a random walk



The Tangle (IOTA)

Compute cumulative weight to each site

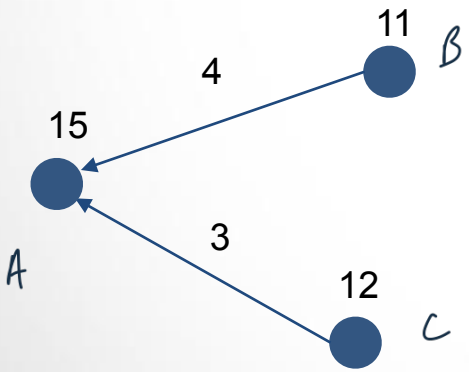
Perform a random walk



The Tangle (IOTA)

Compute cumulative weight to each site

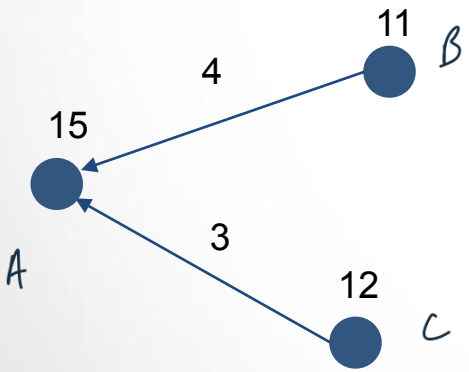
Perform a random walk



Transition function:

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

The Tangle (IOTA)



Compute cumulative weight to each site

Perform a random walk

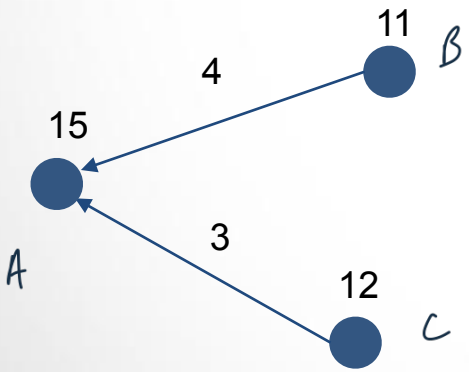
Transition function:

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

MCMC

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

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

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

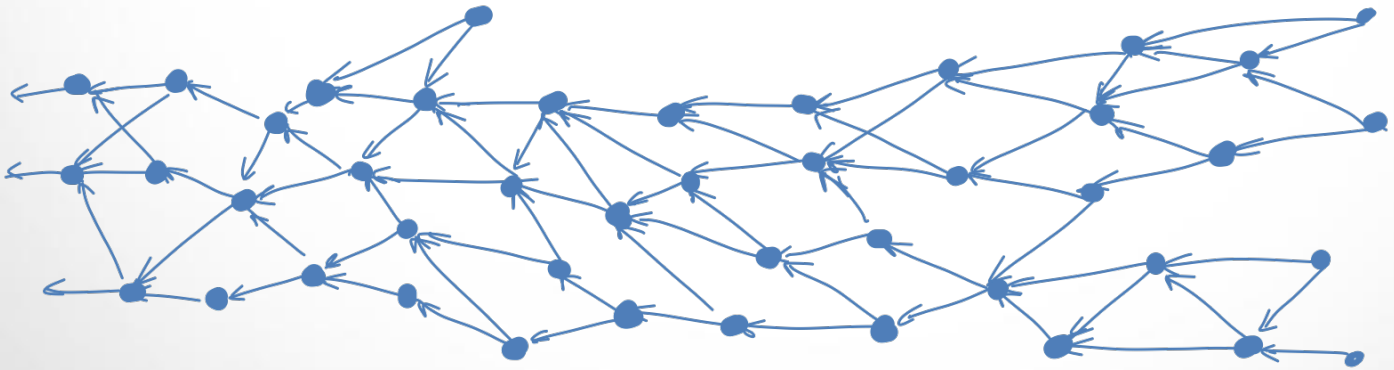
How many tips are left behind ?

How many tips are left behind ?

How many tips over the time ?

How many tips are left behind ?

How many tips over the time ?

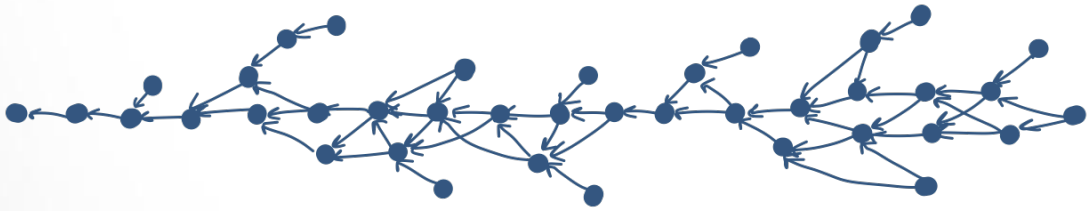


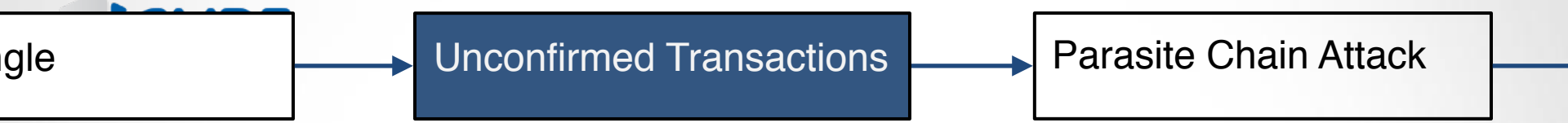
How many tips are left behind ?

How many tips over the time ?

How many tips are left behind ?

How many tips over the time ?




gle
Unconfirmed Transactions
Parasite Chain Attack

How many tips are left behind ?

How many tips are left behind ?

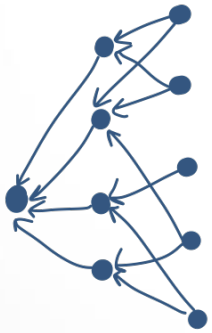
- theoretical analysis, assuming random tip selection

How many tips are left behind ?

- theoretical analysis, assuming random tip selection
- by simulation, for other tip selection

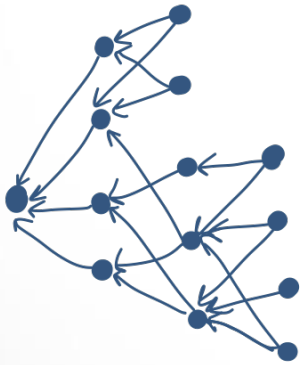
Theoretical analysis, assuming random tip selection

Discrete time model. At each round: Poisson(λ) new sites



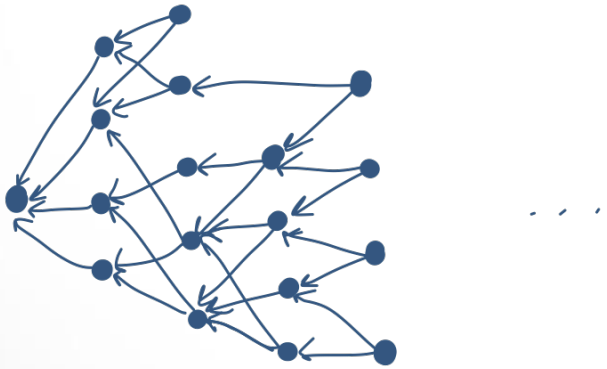
Theoretical analysis, assuming random tip selection

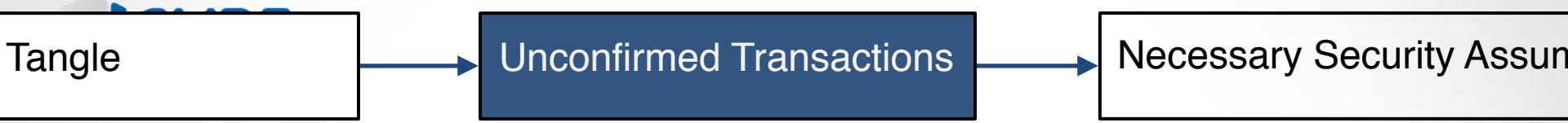
Discrete time model. At each round: Poisson(λ) new sites



Theoretical analysis, assuming random tip selection

Discrete time model. At each round: Poisson(λ) new sites

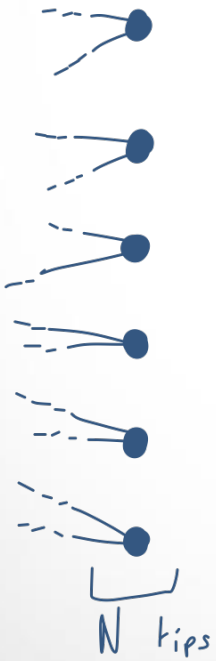




Theoretical analysis, assuming random tip selection

Tangle → Unconfirmed Transactions → Necessary Security Assum

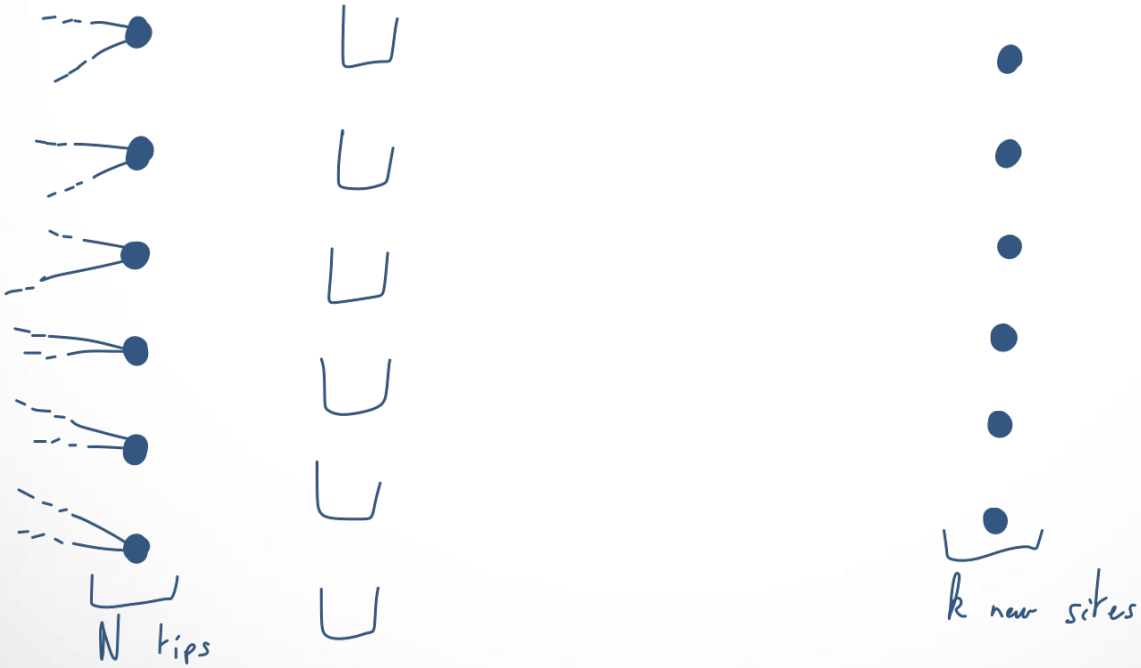
Theoretical analysis, assuming random tip selection



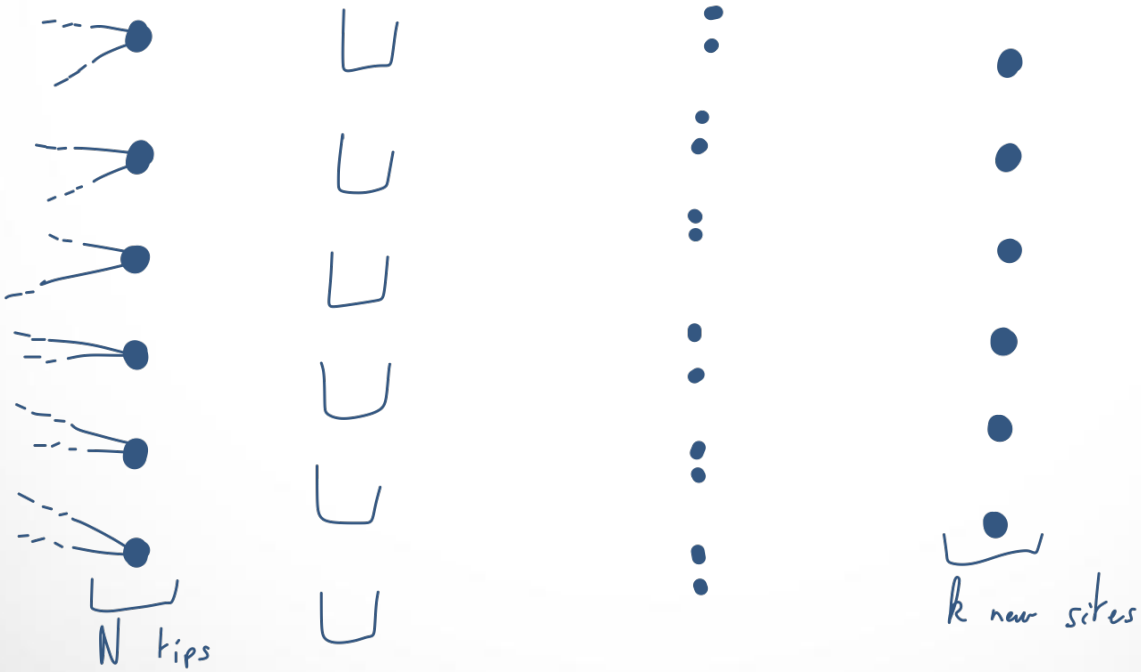
Theoretical analysis, assuming random tip selection

Tangle → Unconfirmed Transactions → Necessary Security Assum

Theoretical analysis, assuming random tip selection

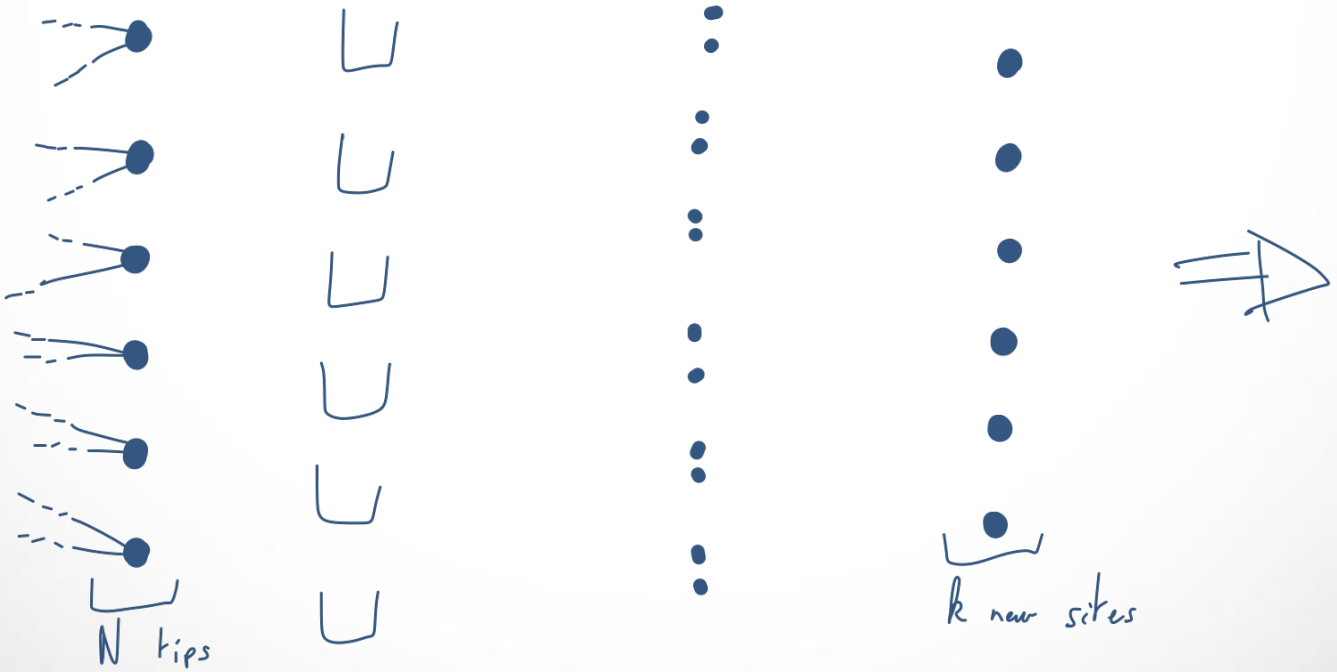


Theoretical analysis, assuming random tip selection

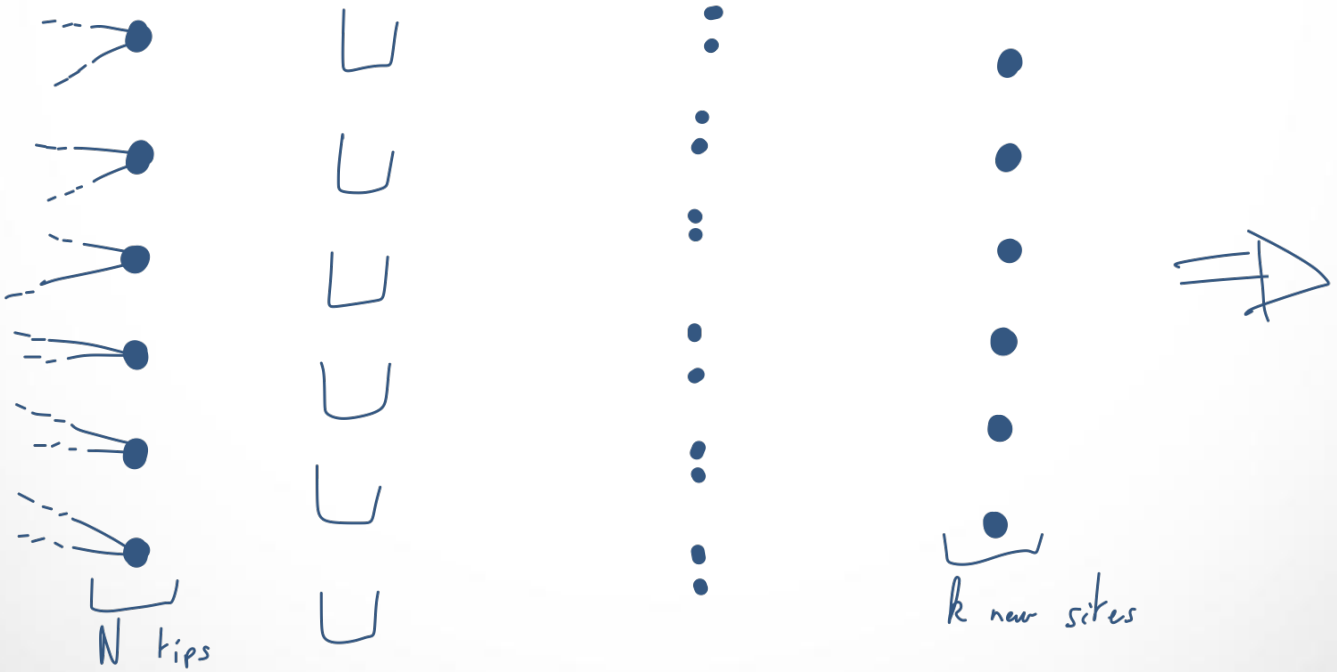


Tangle → Unconfirmed Transactions → Necessary Security Assum

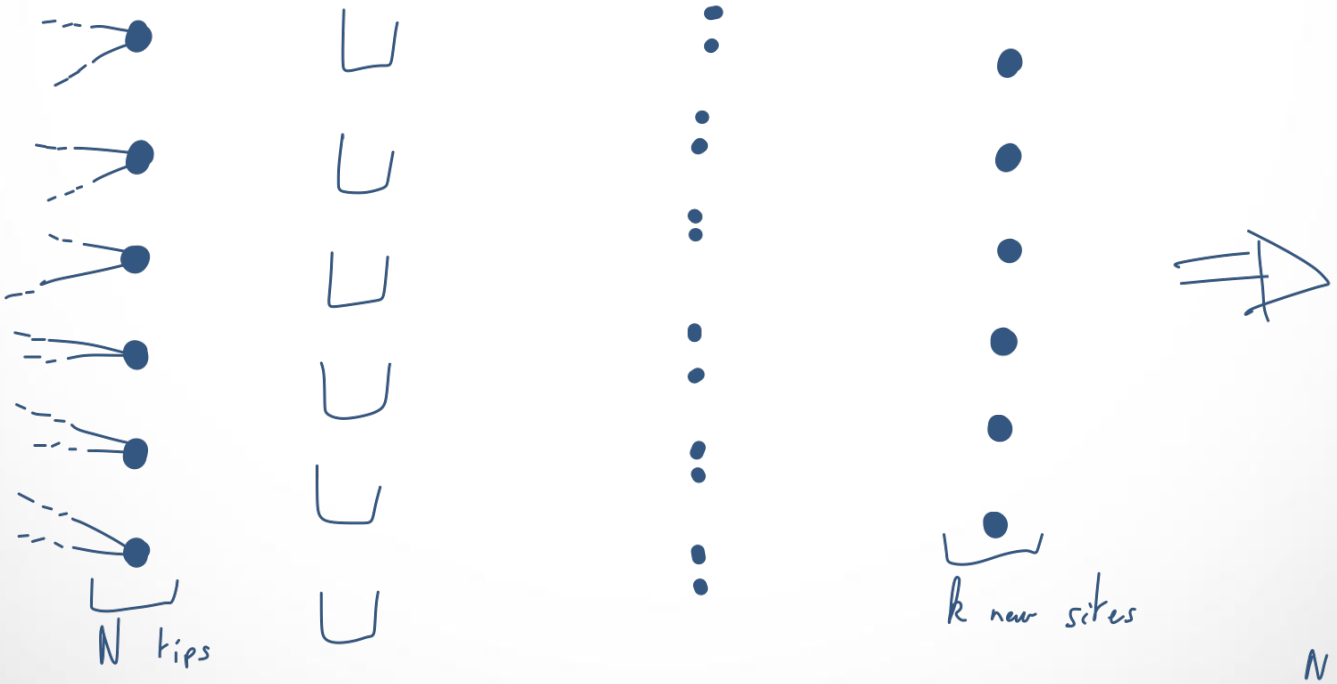
Theoretical analysis, assuming random tip selection

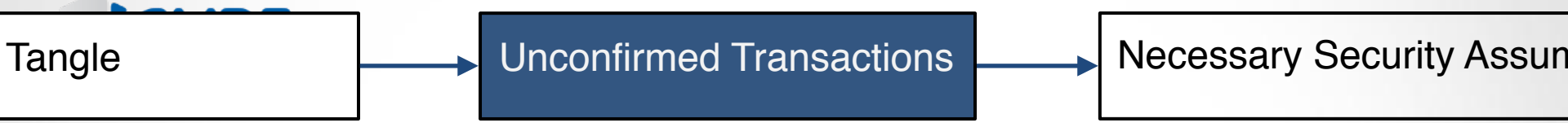


Theoretical analysis, assuming random tip selection



Theoretical analysis, assuming random tip selection




Tangle
Unconfirmed Transactions
Necessary Security Assum

$P_N \xrightarrow{k} N' =$

outcomes

$P_N \xrightarrow{k} N' =$

Probability of 1 outcome × # outcomes

$P_{N \xrightarrow{k} N'} =$

Probability of 1 outcome × # outcomes

$$P_{N \xrightarrow{k} N'} = \left\{ \begin{matrix} 2k \\ N - N' - k \end{matrix} \right\}$$

Probability of 1 outcome × # outcomes

$$P_{N \xrightarrow{k} N'} = \left\{ \begin{matrix} 2k \\ N - N' - k \end{matrix} \right\}$$

partition $2k$ in $N - N' - k$ subsets.

Probability of 1 outcome

outcomes

$$P_{N \xrightarrow{k} N'} = \frac{N!}{(N'-k)!} \left\{ {2k \atop N-N'-k} \right\}$$

partition $2k$ in $N-N'-k$ subsets.

Probability of 1 outcome × # outcomes

$$P_{N \xrightarrow{k} N'} = \frac{N!}{(N'-k)!} \left\{ {2k \atop N-N'-k} \right\}$$

distribute those subsets in the N tips

partition 2k in N-N'-k subsets.

Probability of 1 outcome

outcomes

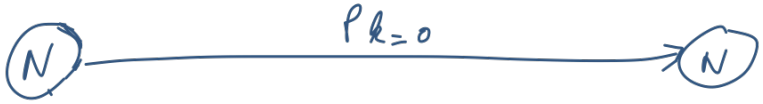
$$P_{N \xrightarrow{k} N'} = \frac{1}{N^{2k}} \frac{N!}{(N'-k)!} \left\{ {2k \atop N-N'-k} \right\}$$

distribute those subsets in the N tips

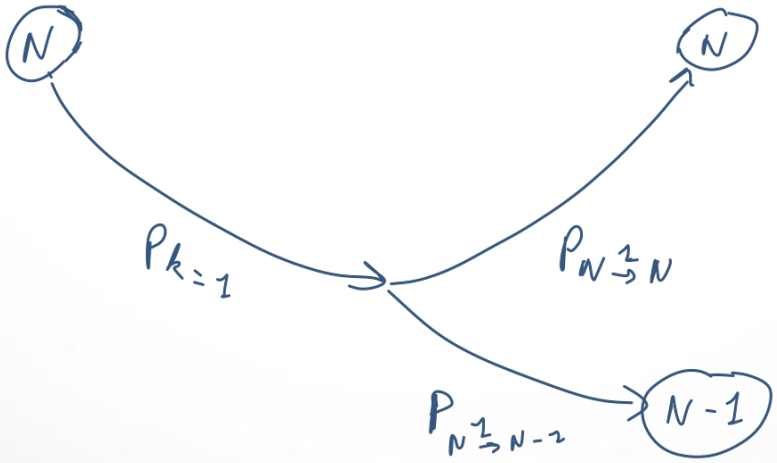
partition 2k in N-N'-k subsets.

Tangle → **Unconfirmed Transactions** → Necessary Security Assum

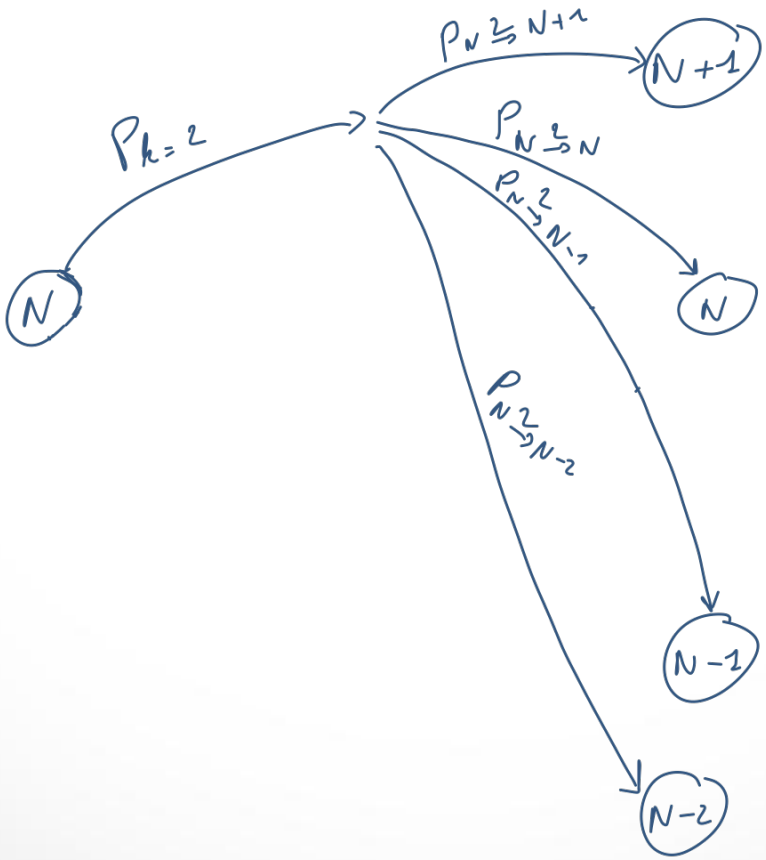
$$k \sim Pois(\lambda)$$



$$k \sim Pois(\lambda)$$

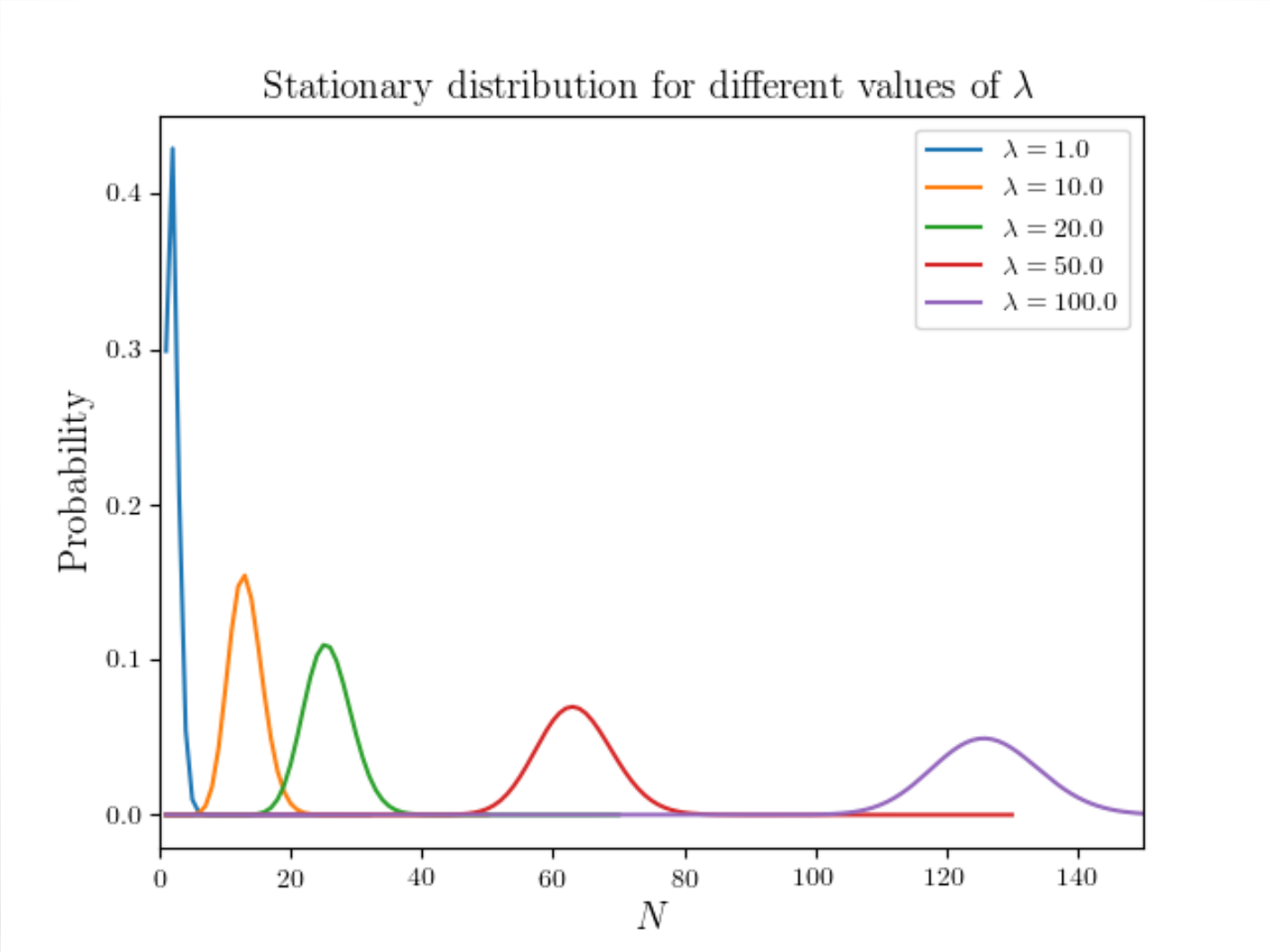


$k \sim Pois(\lambda)$

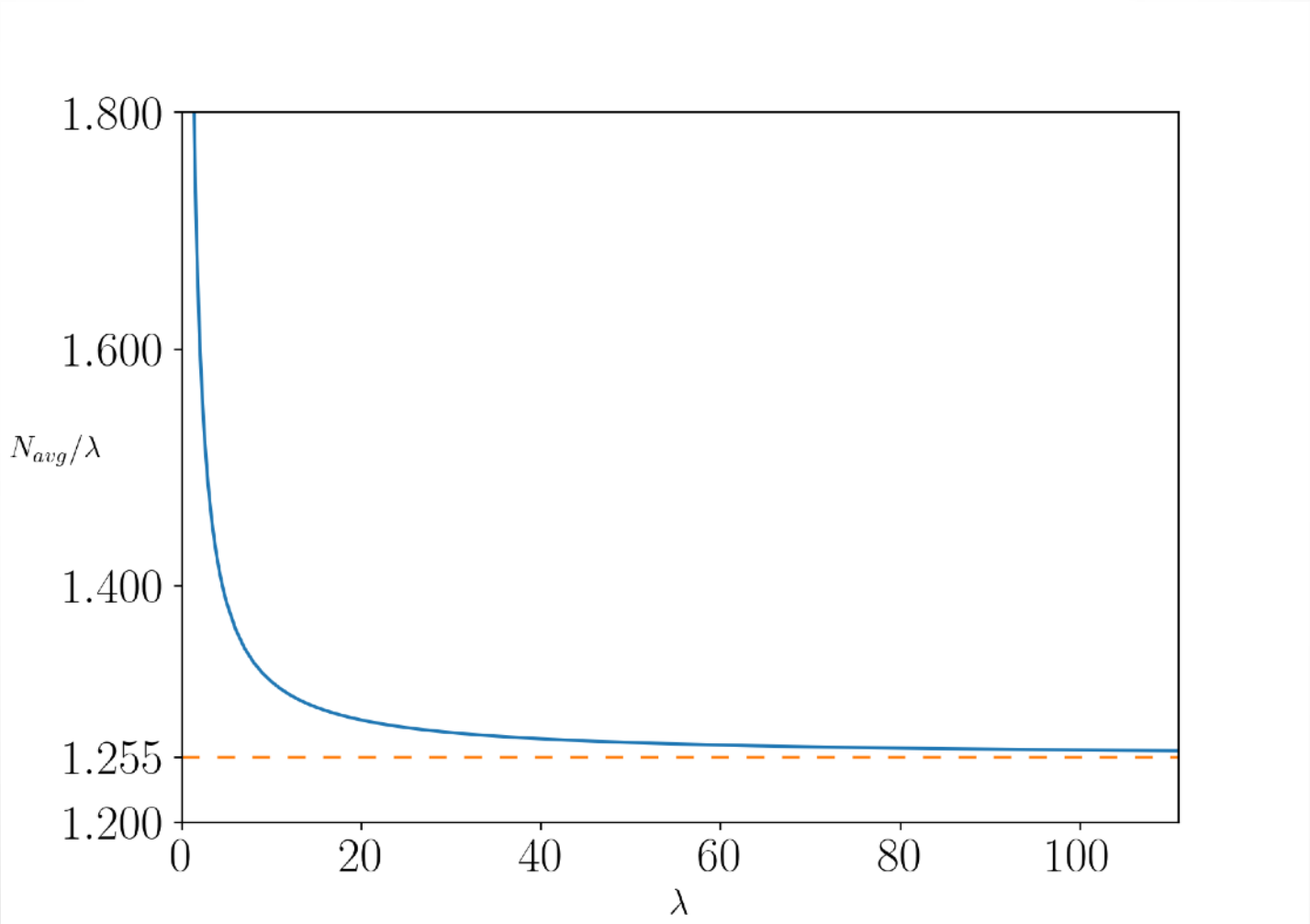


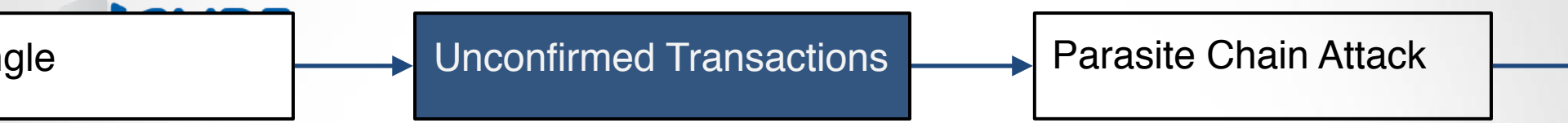
$$\sum_k \mathbb{P}\left(Pois(\lambda)=k\right) P_N^{\,k} \to N'$$

Tangle → Unconfirmed Transactions → Necessary Security Assum



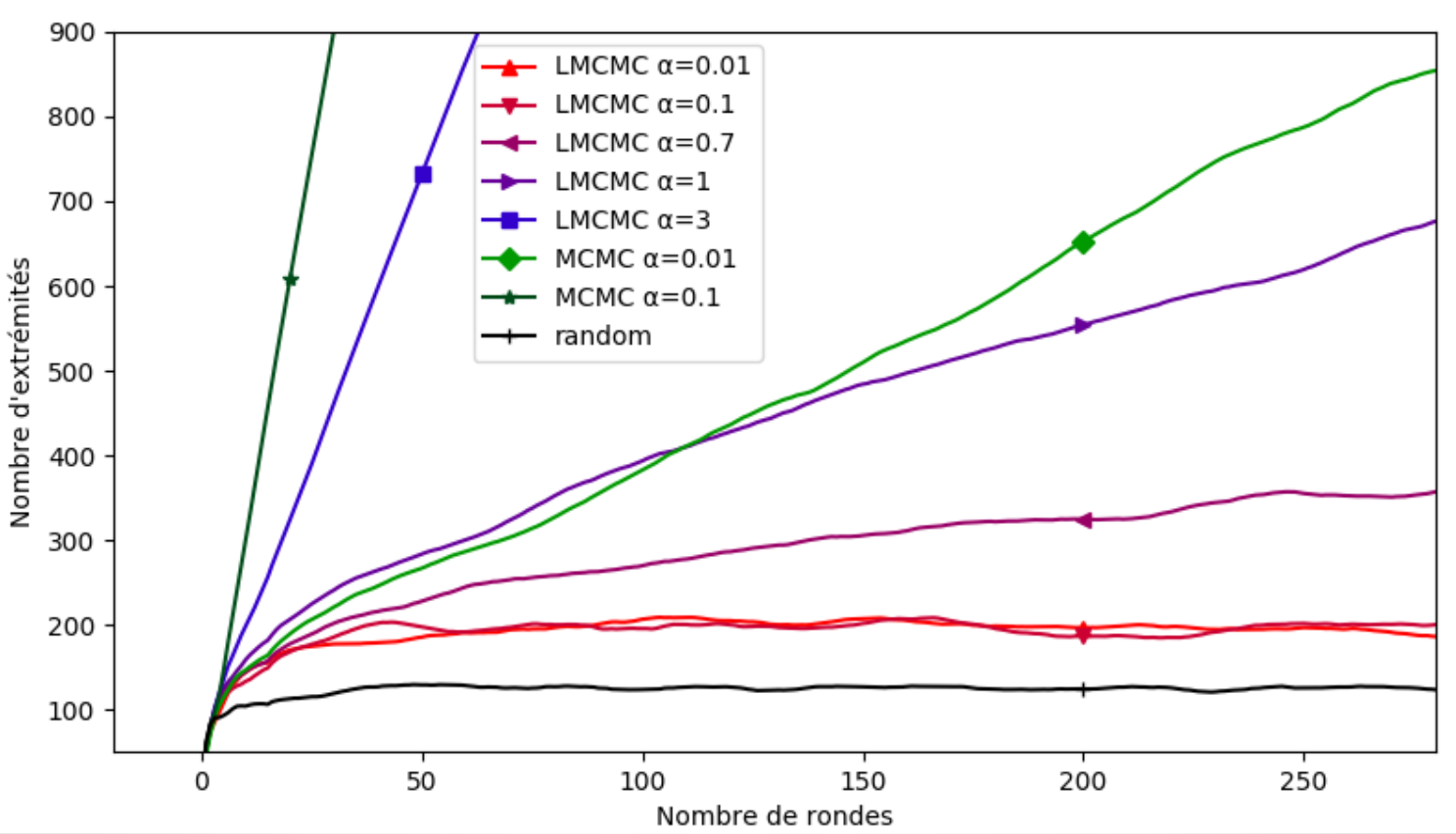
Tangle → Unconfirmed Transactions → Necessary Security Assum



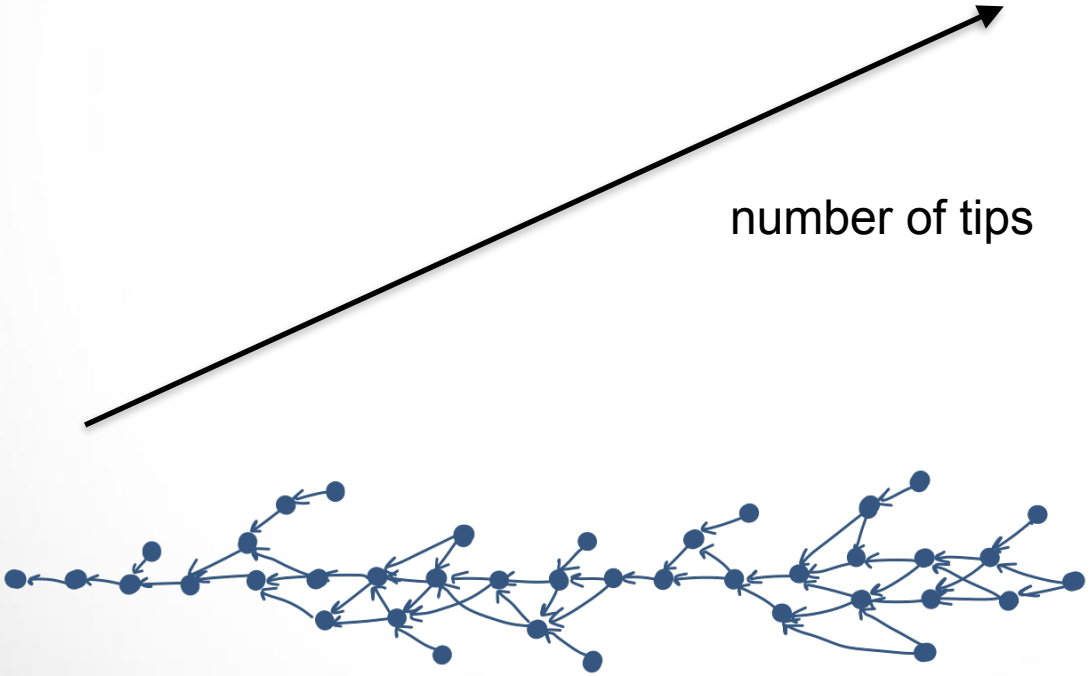


By simulation, for other tip selection

By simulation, for other tip selection



By simulation, for other tip selection



med Transactions → Parasite Chain Attack → Conclusion

Double Spending Attack

Double Spending Attack

- Alice send 10 IOTA to Bob for a sandwich

Double Spending Attack

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

Double Spending Attack

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

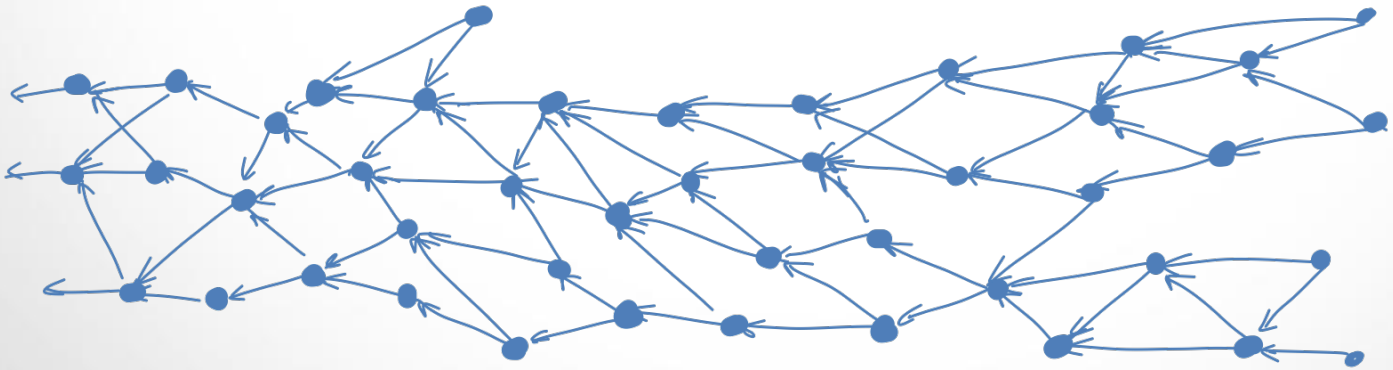
Double Spending Attack

- Alice send 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

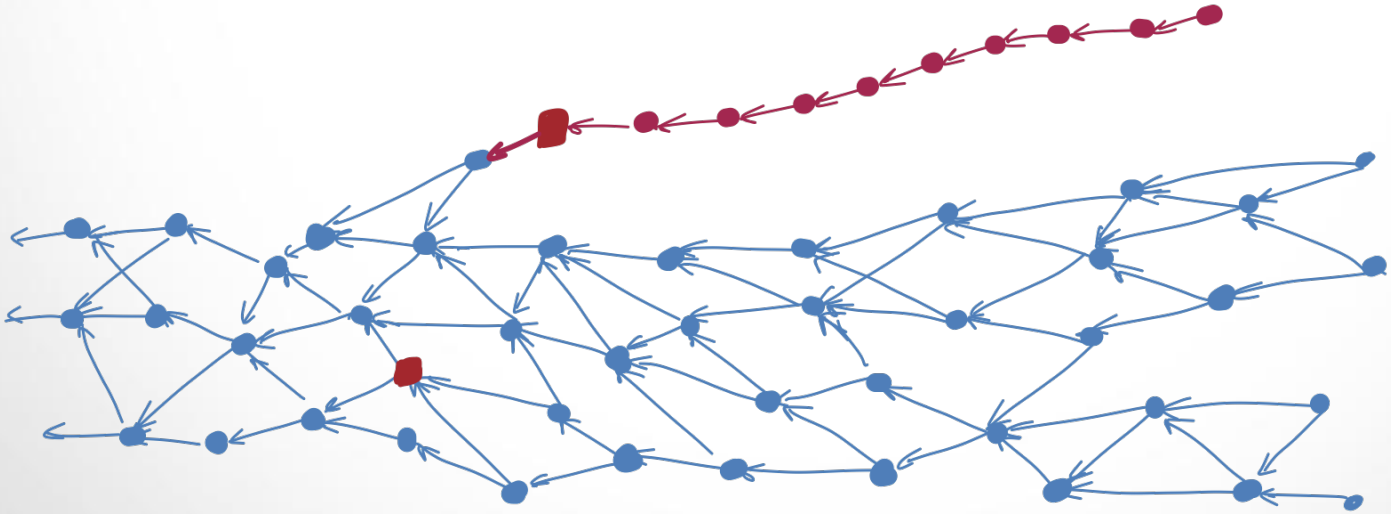
Double Spending Attack

- Alice send 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

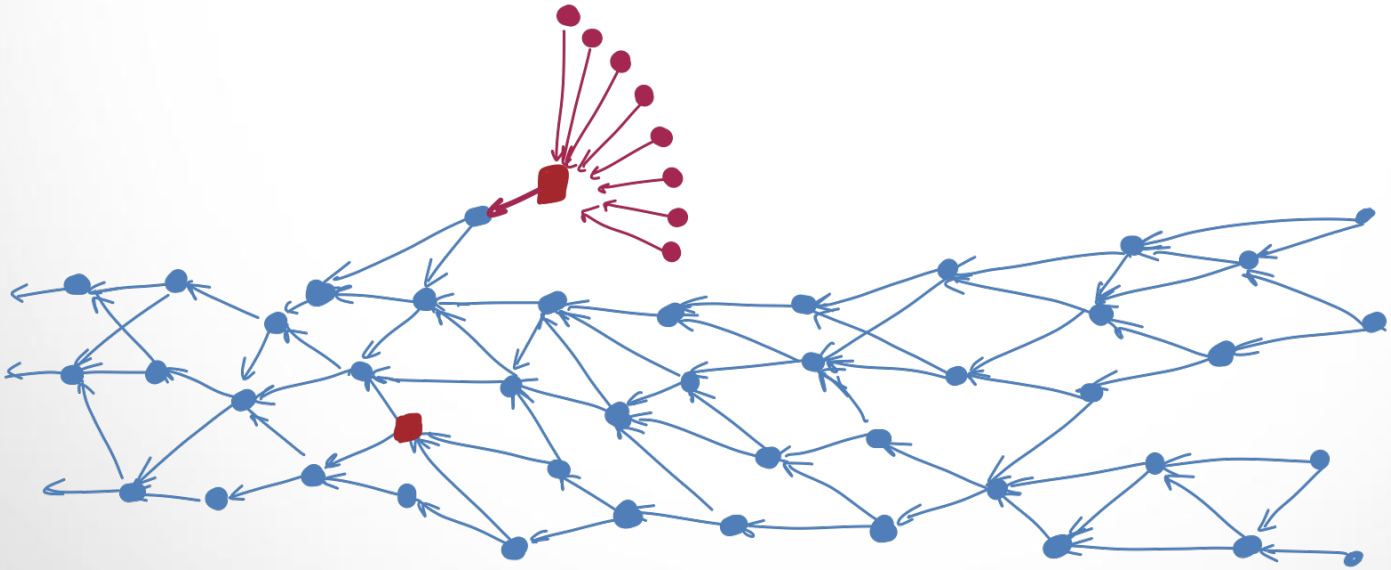
The parasite chain attack



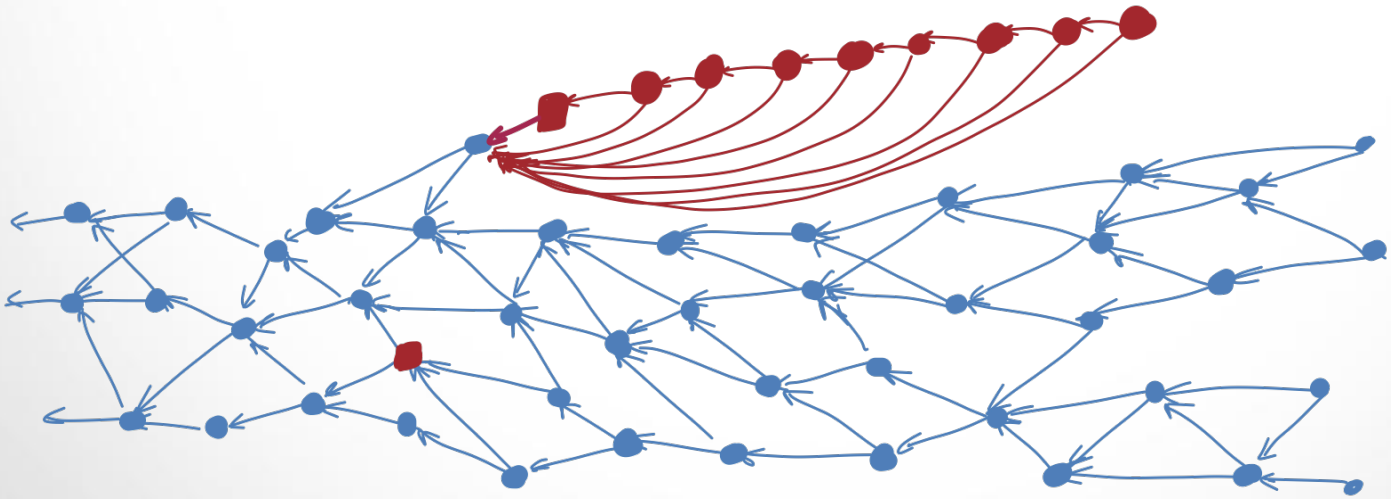
The parasite chain attack



The parasite chain attack



The parasite chain attack



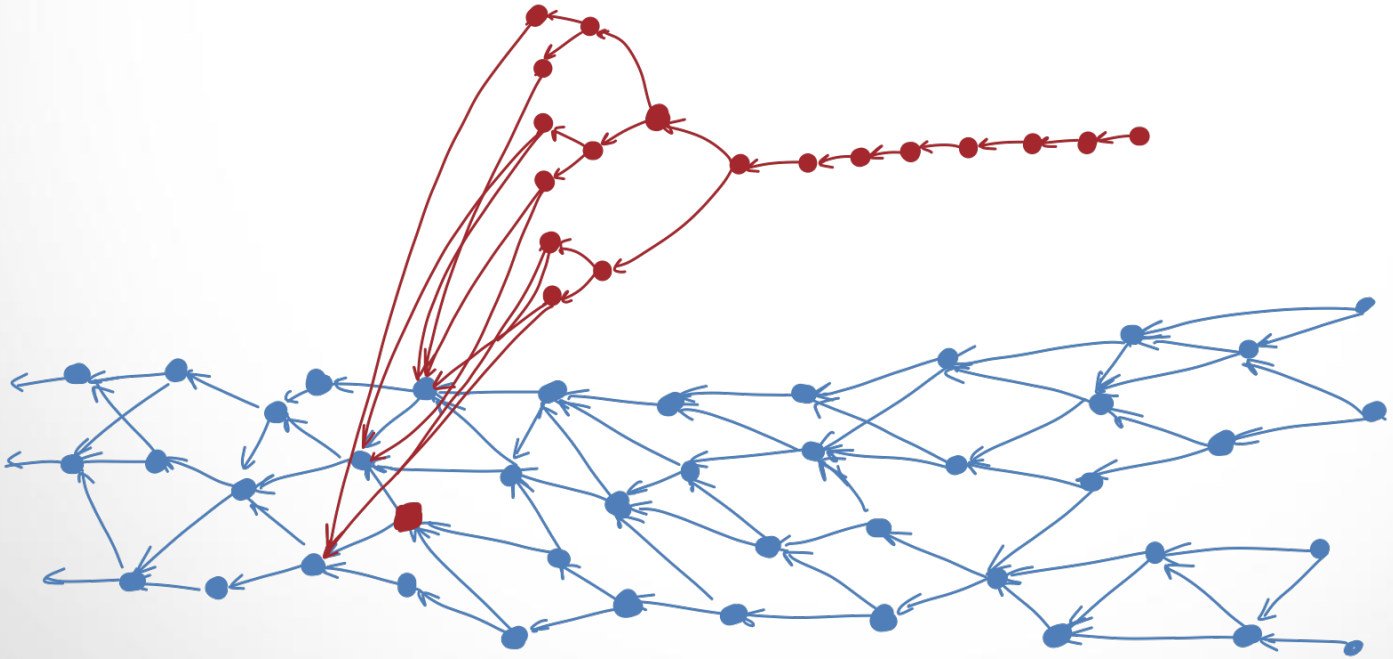
med Transactions → Parasite Chain Attack → Conclusion

Theoretical analysis

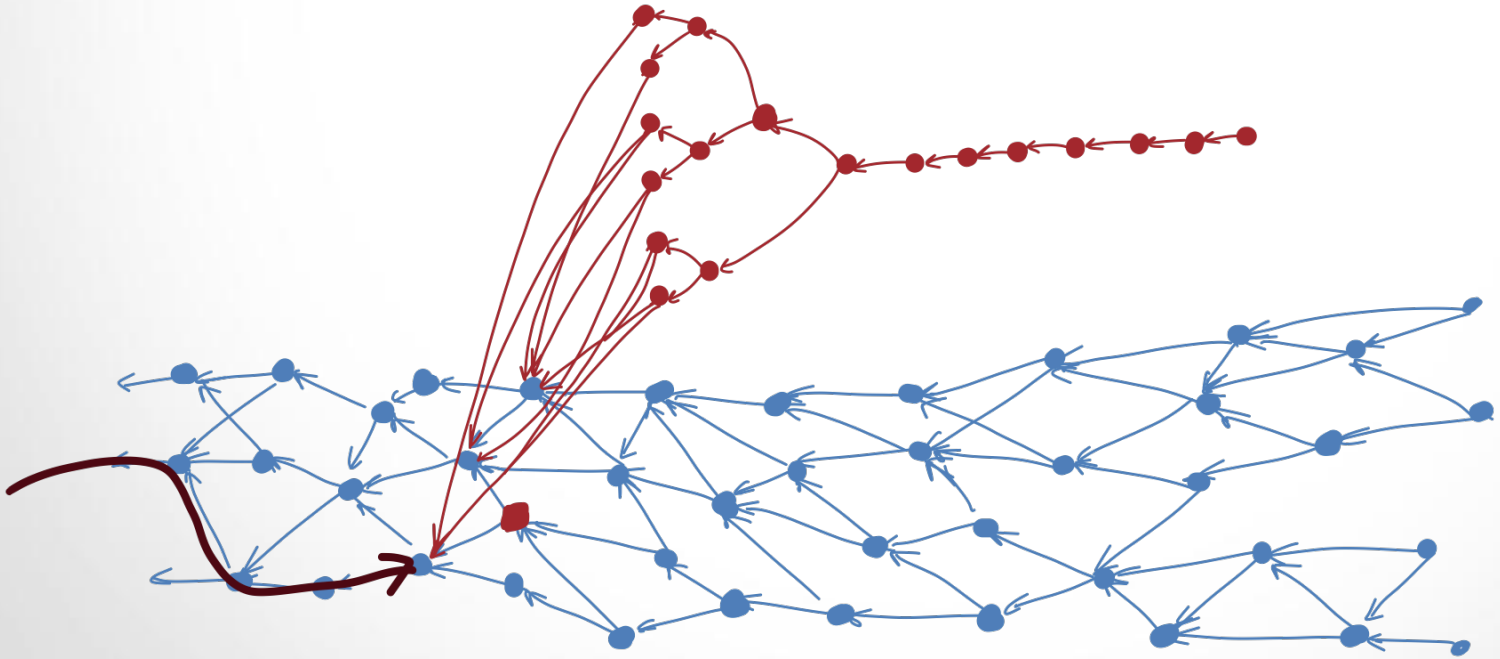
Theoretical analysis

Simulations

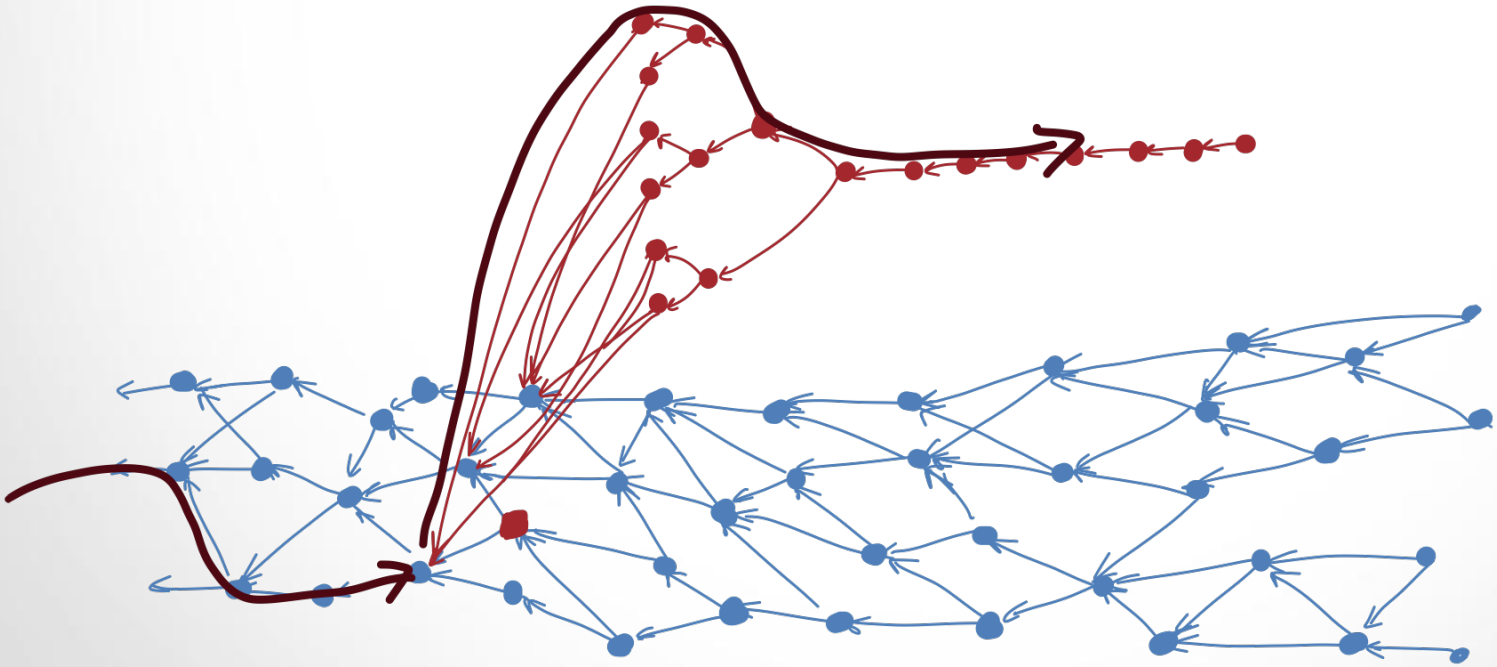
Theoretical analysis



Theoretical analysis



Theoretical analysis



Theoretical analysis

Theorem

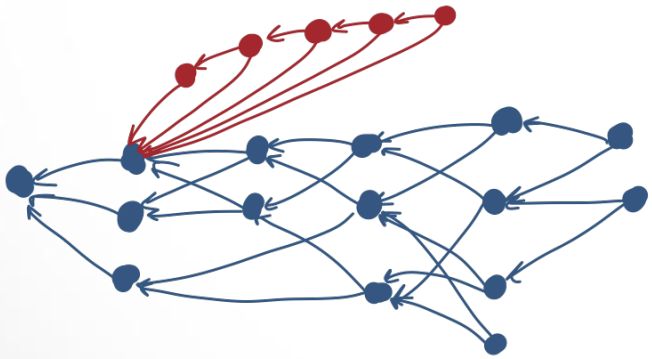
An attack is possible if hashing power of the adversary > hashing power used by the all nodes.

Corollary

An attack is possible if hashing power of the adversary > hashing power of the all nodes

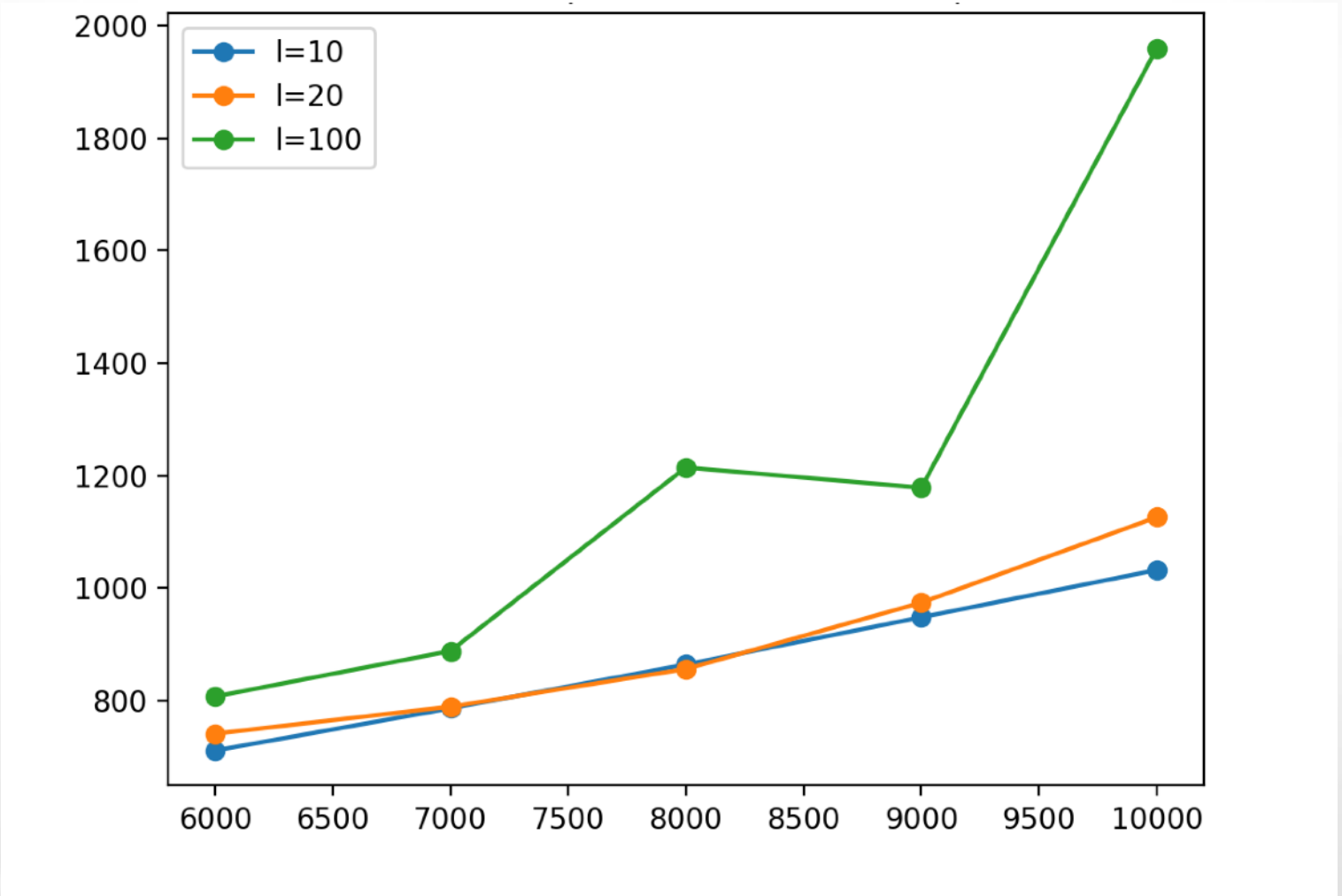
if all the honest nodes constantly generates new sites

By simulation



How many red site so that:

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


2000
1800
1600
1400
1200
1000
800
6000
6500
7000
7500
8000
8500
9000
9500
10000
l=10
l=20
l=100

Conclusion

Conclusion

The Tangle *(Theoretical Protocol)* : Security based on PoW
IOTA *(Current Implementation)* : Central coordinator

Conclusion

The Tangle *(Theoretical Protocol)* : Security based on PoW
IOTA *(Current Implementation)* : Central coordinator

How to attach the parasite chain?

Conclusion

The Tangle *(Theoretical Protocol)* : Security based on PoW
IOTA *(Current Implementation)* : Central coordinator

How to attach the parasite chain?

Number of tips  Resistance to parasite chain attack