How To Select its Parents in the Tangle

Vidal Attias, Quentin Bramas

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 (IOTA)
The Tangle (IOTA)

Each transaction is a small block that references two previous ones.
The Tangle (IOTA)

Each transaction is a small block that references two previous ones.
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 (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 (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)
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

11
15
12
The Tangle (IOTA)

MCMC Tip selection algorithm

- Compute cumulative weight to each site
- Perform a random walk
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:

\[
P(A \rightarrow B) = \frac{f(\Delta_{A1B})}{f(\Delta_{A1C}) + f(\Delta_{A1B})}
\]
The Tangle (IOTA)

Compute cumulative weight to each site
Perform a random walk

Transition function:

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

MCMC

$$f(\Delta) = e^{-\Delta}$$
The Tangle (IOTA)

MCMC Tip selection algorithm

Compute cumulative weight to each site
Perform a random walk

Transition function:

\[
\mathbb{P}(A \rightarrow B) = \frac{\Pi(\Delta_{A \rightarrow B})}{\Pi(\Delta_{A \rightarrow c}) + \Pi(\Delta_{A \rightarrow b})}
\]

MCMC

\[
\Pi(\Delta) = e^{-\lambda \Delta}
\]

LMCMC

\[
\Pi(\Delta) = \Delta^{-\lambda}
\]
Real cumulative weight

\[ w(n) = 1 + \sum_{c \in \text{children}} w(c)/2 \]
Real cumulative weight

\[ w(u) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Real cumulative weight

\[ w(m) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Real cumulative weight

\[ w(u) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Real cumulative weight

\[ w(u) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Real cumulative weight

\[ \omega(w) = 1 + \sum_{c \in \text{children}} \omega(c)/2 \]
Real cumulative weight

\[ w(u) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Real cumulative weight

\[ w(m) = 1 + \sum_{c \in \text{children}} \frac{w(c)}{2} \]
Random Walk

Transition function:
Random Walk

Transition function:

\[ P_{A \to B} = \frac{11}{11 + 12} \]
Comparison
Number of tips

How many tips are left behind?
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?
Tips over time
Tips over time
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 lot 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
The parasite chain attack
Parasite Chain Attack

The parasite chain attack

How many red site so that:

\[ P(TSA(6) \in \text{parasite}) \geq \frac{\epsilon}{2} \]
Parasite Chain Attack

Against MCMC
Parasite Chain Attack

Against MCMC
Parasite Chain Attack

Against MCMC
Resistance to parasite chain

![Graph showing the relationship between Security factor and Size of the Tangle.

Security factor vs. Size of the Tangle

- mcmc-new
- mcmc

Graph shows trends in Security factor across different sizes of the Tangle.
Complexity
Conclusion

Future Work
Conclusion

We defined a good tip selection algorithm

Future Work
Conclusion

We defined a good tip selection algorithm

Future Work

Even better tip selection algorithms
Conclusion

We defined a good tip selection algorithm

Future Work

Even better tip selection algorithms

Thank you for your attention!