G-IOTA/E-IOTA
Fair and Efficient Aware Tangle

Gewu BU (Sorbonne Université)

Önder GURCAN (CEA LIST)

Wassim HANA (Sorbonne Université)

Maria POTOP-BUTUCARU (Sorbonne Université)

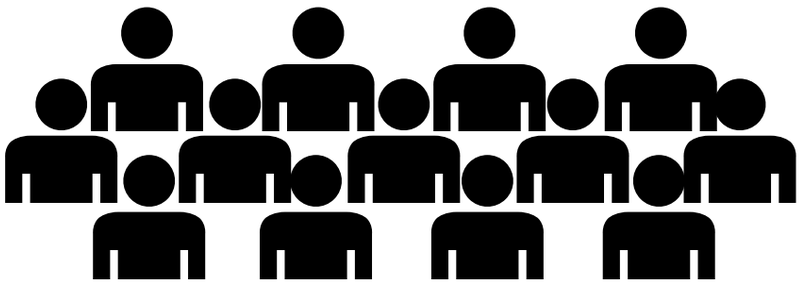
Fairness

?

IOTA

IOTA

Bitcoin

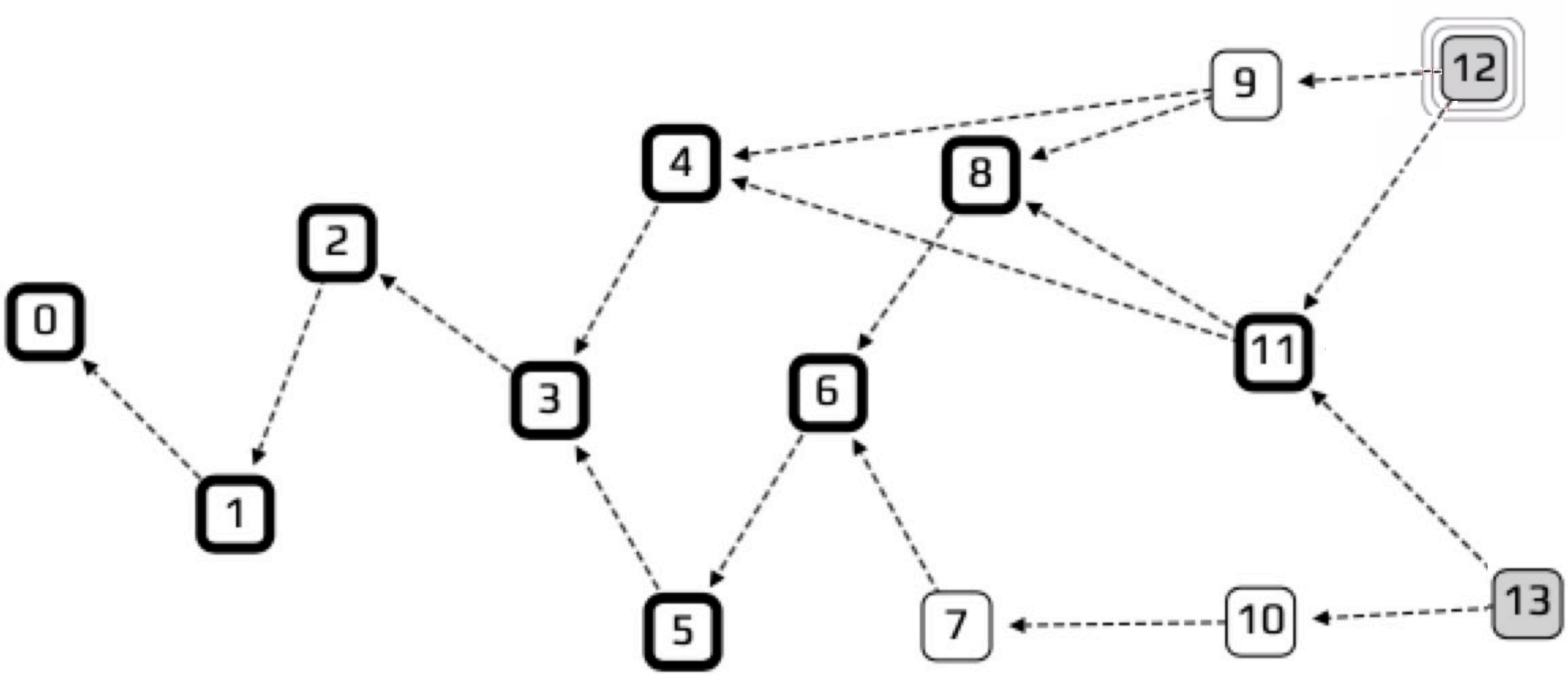


Users

Miners

IOTA-Tangle: a Transactions-DAG [1]

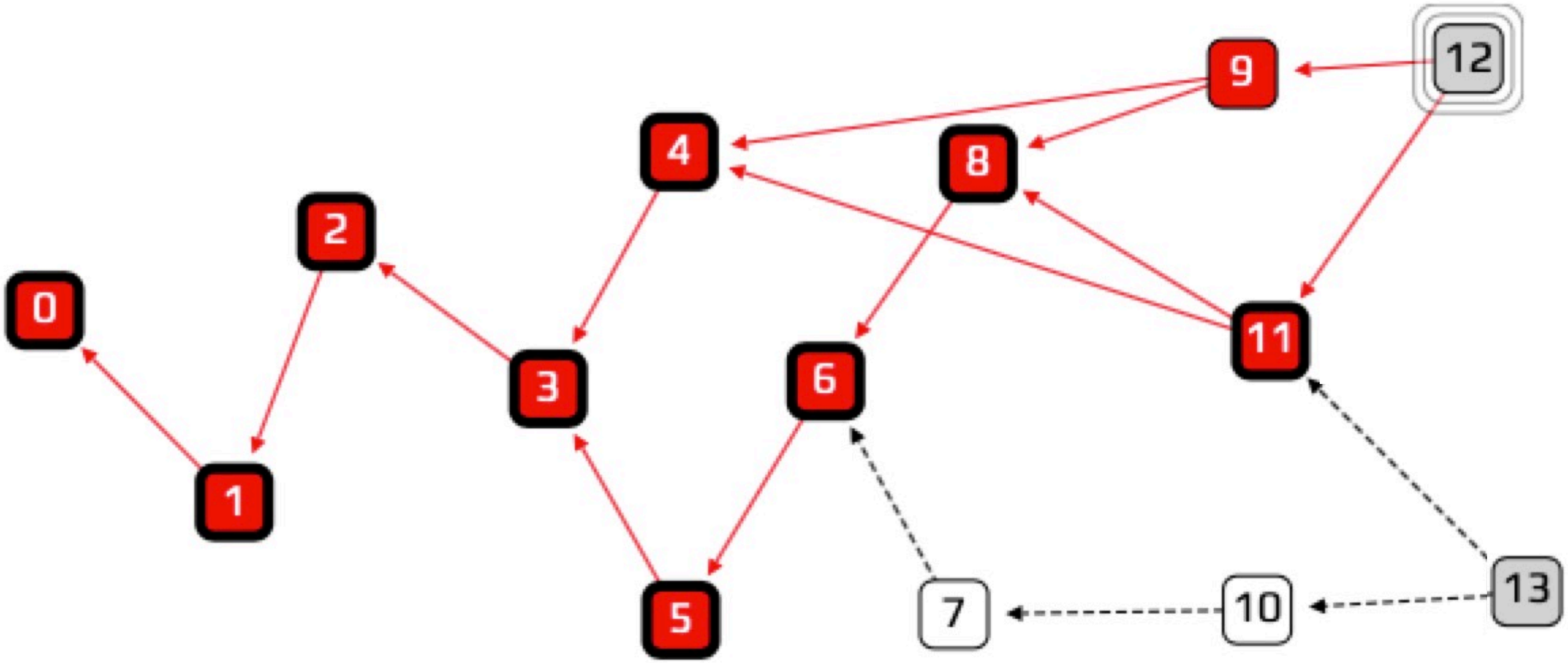
(DAG: Directed acyclic graph)



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

IOTA-Tangle: a Transactions-DAG [1]

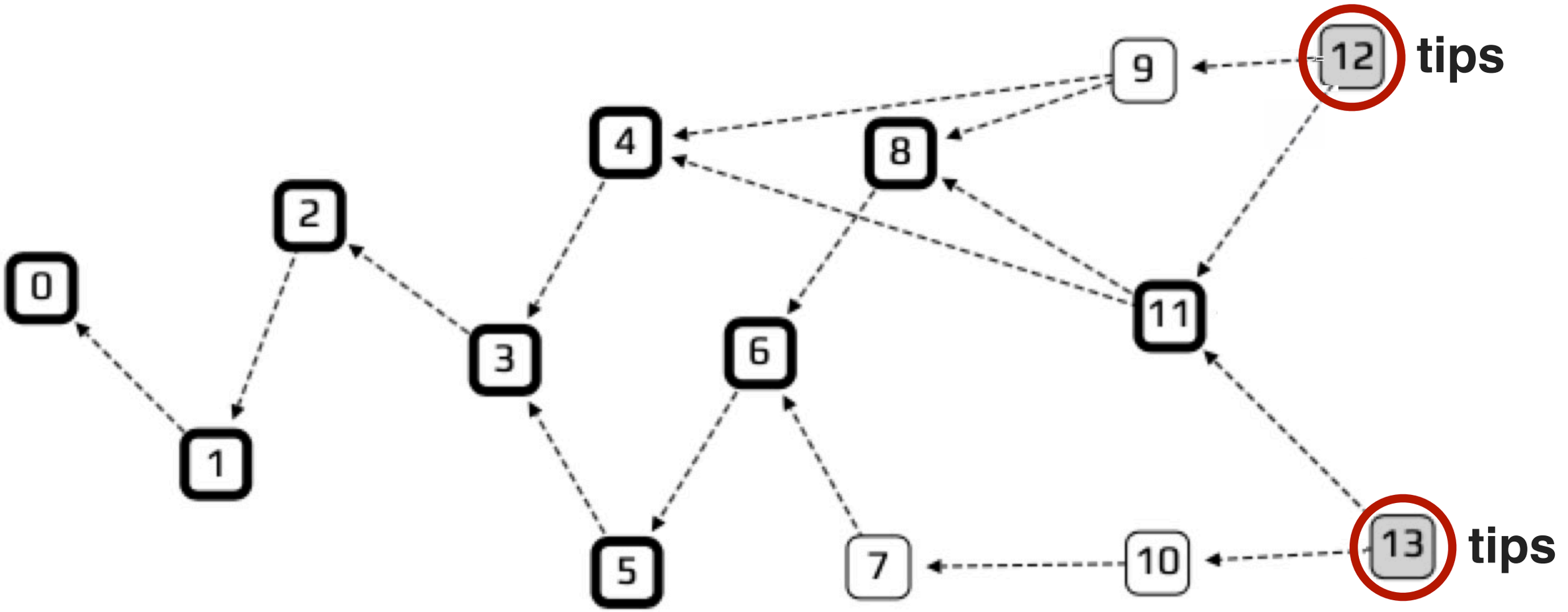
(DAG: Directed acyclic graph)



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

IOTA-Tangle: a Transactions-DAG [1]

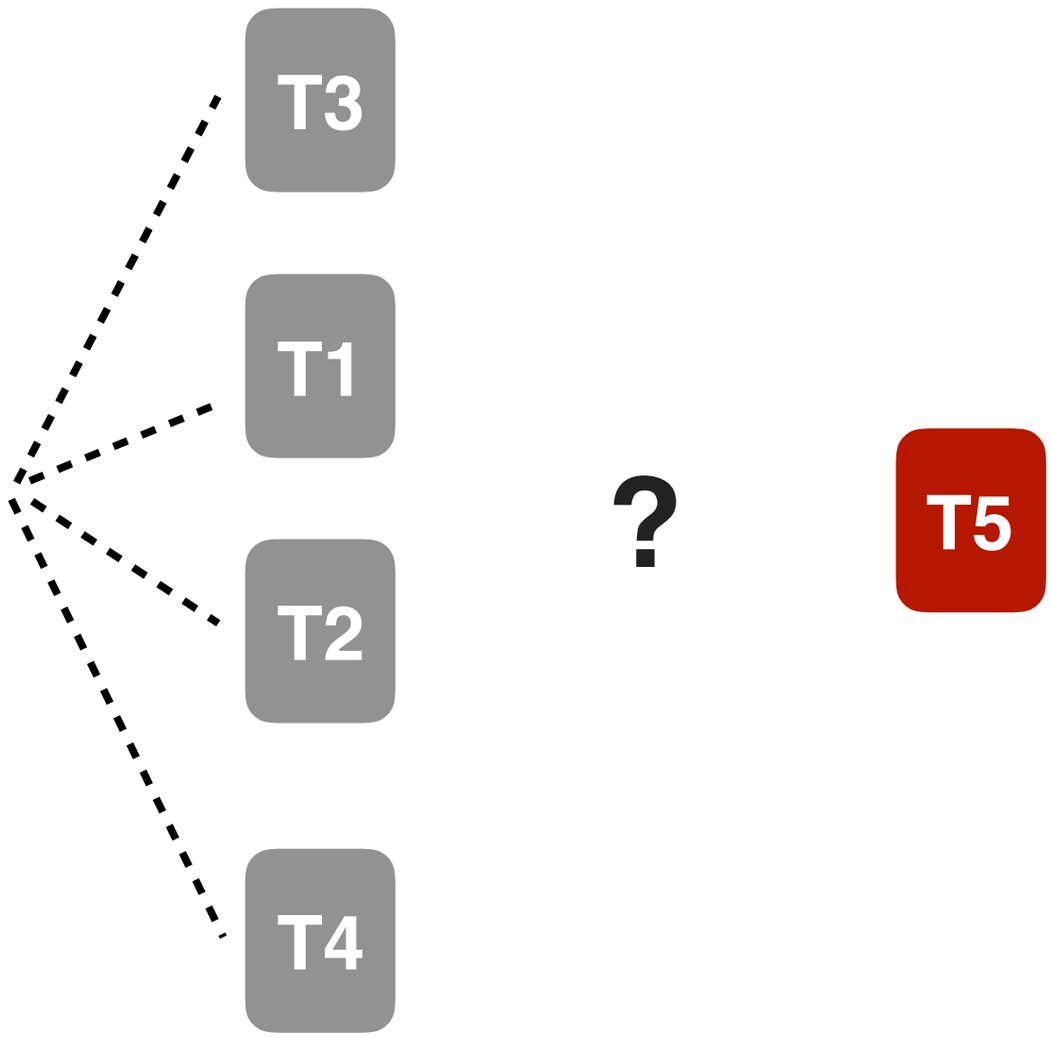
(DAG: Directed acyclic graph)



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

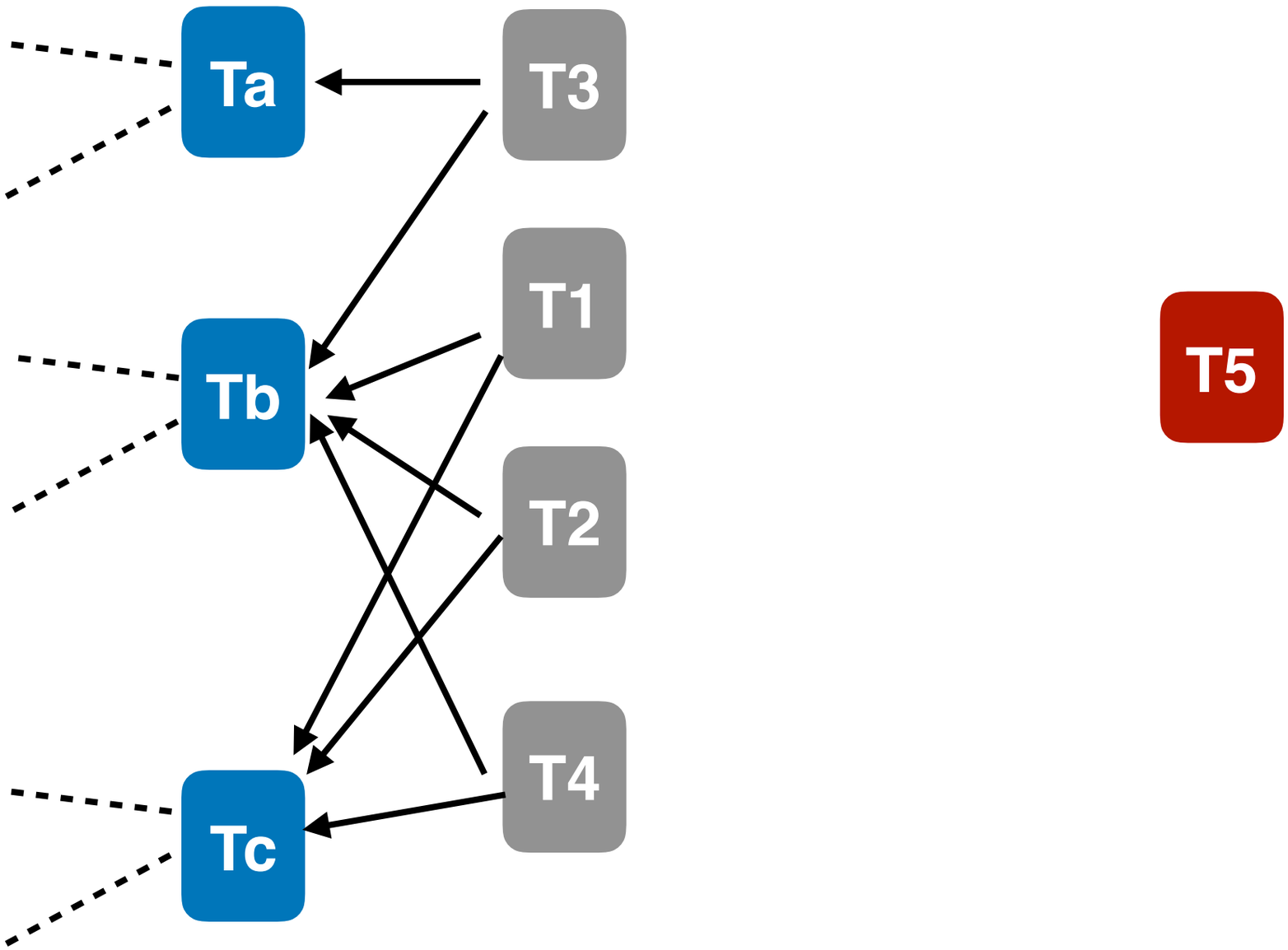
Tips selection Algorithm[1]

(TSA)



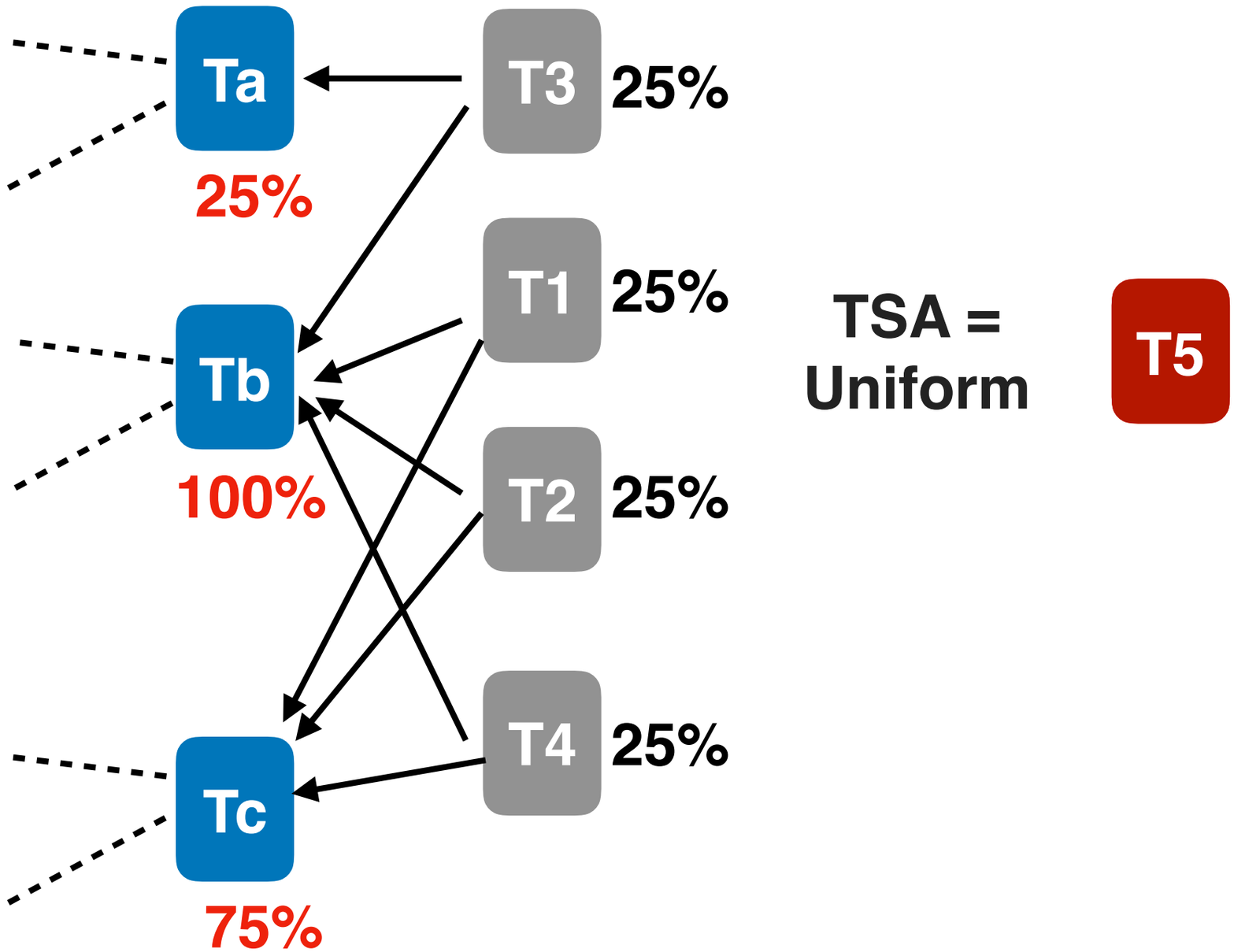
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Level of Confidence [1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Level of Confidence [1]



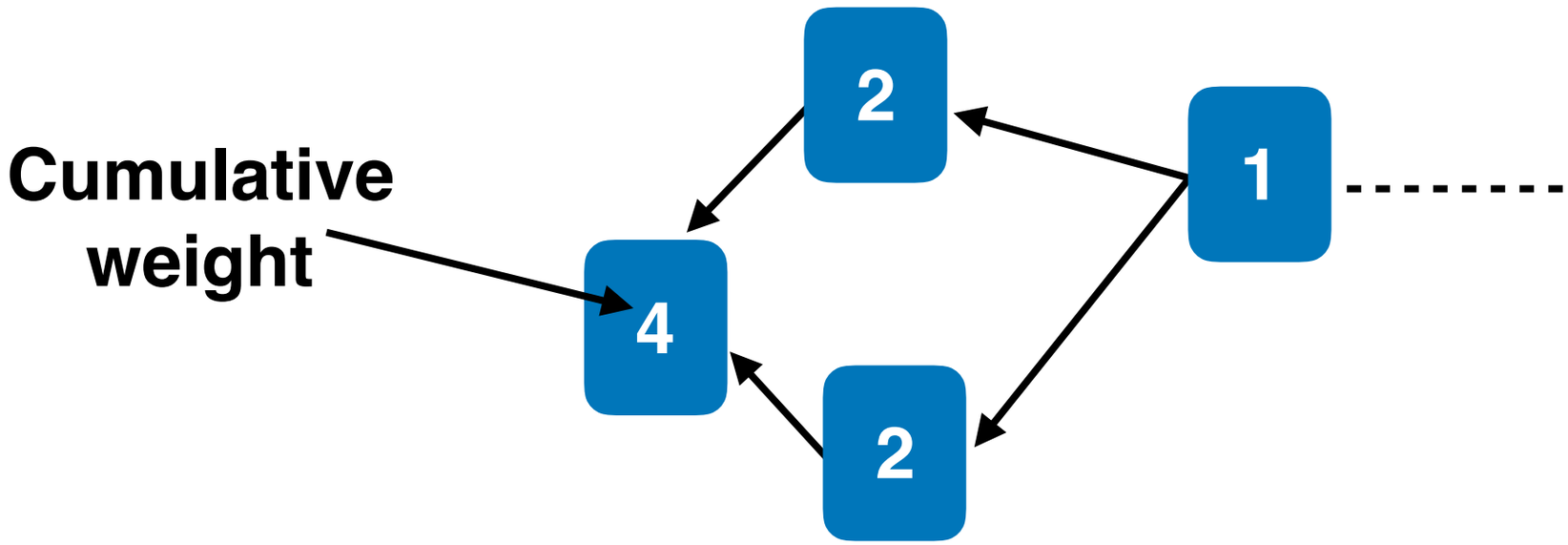
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]

Fairness

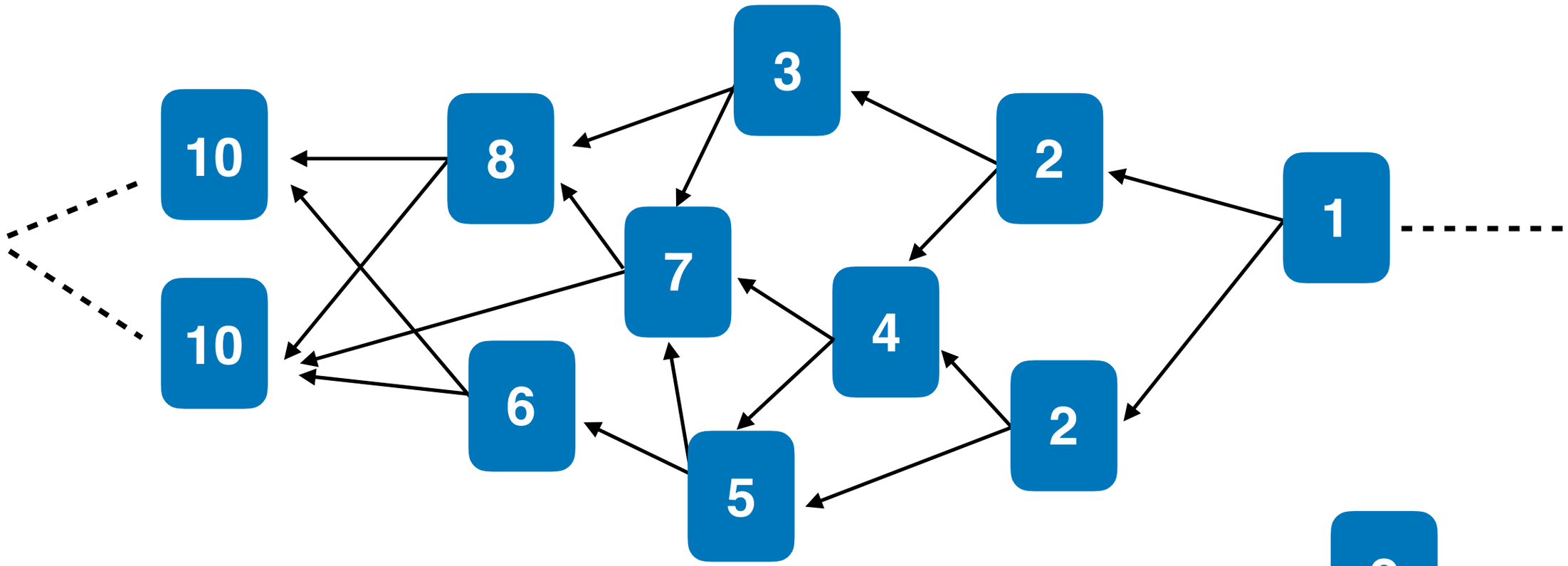
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

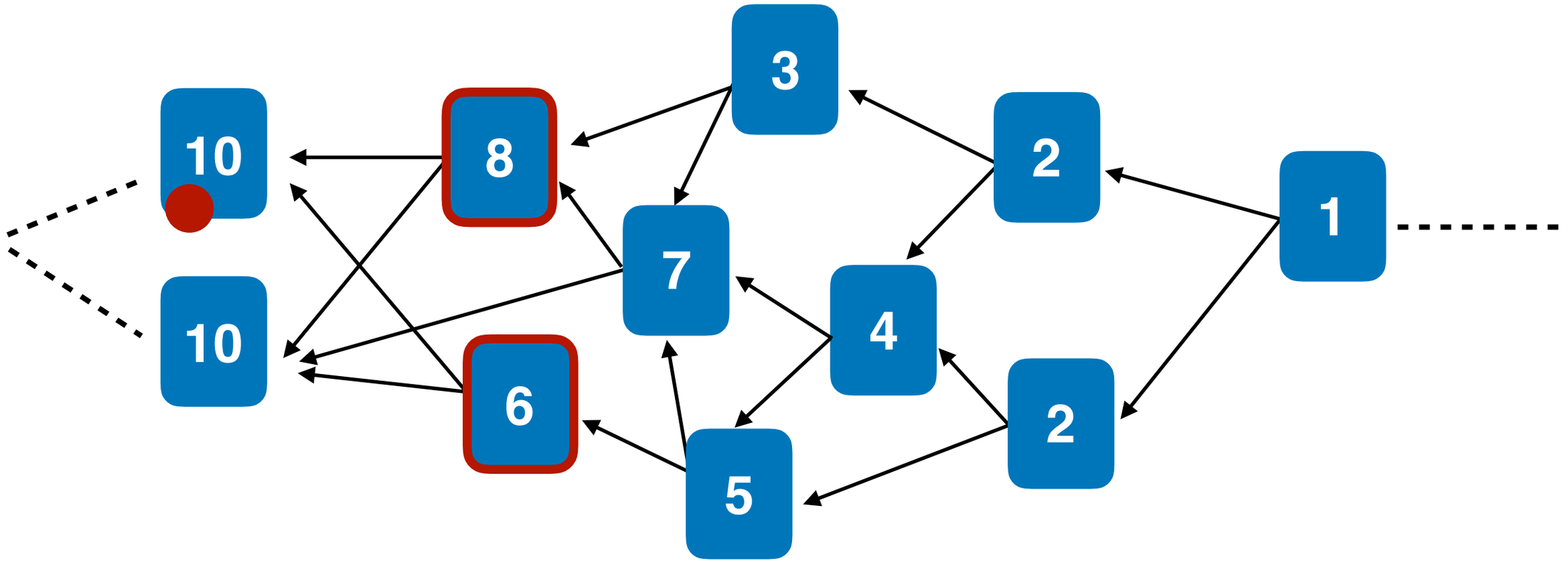
Weighted Random Walk TSA [1]



Cumulative weight

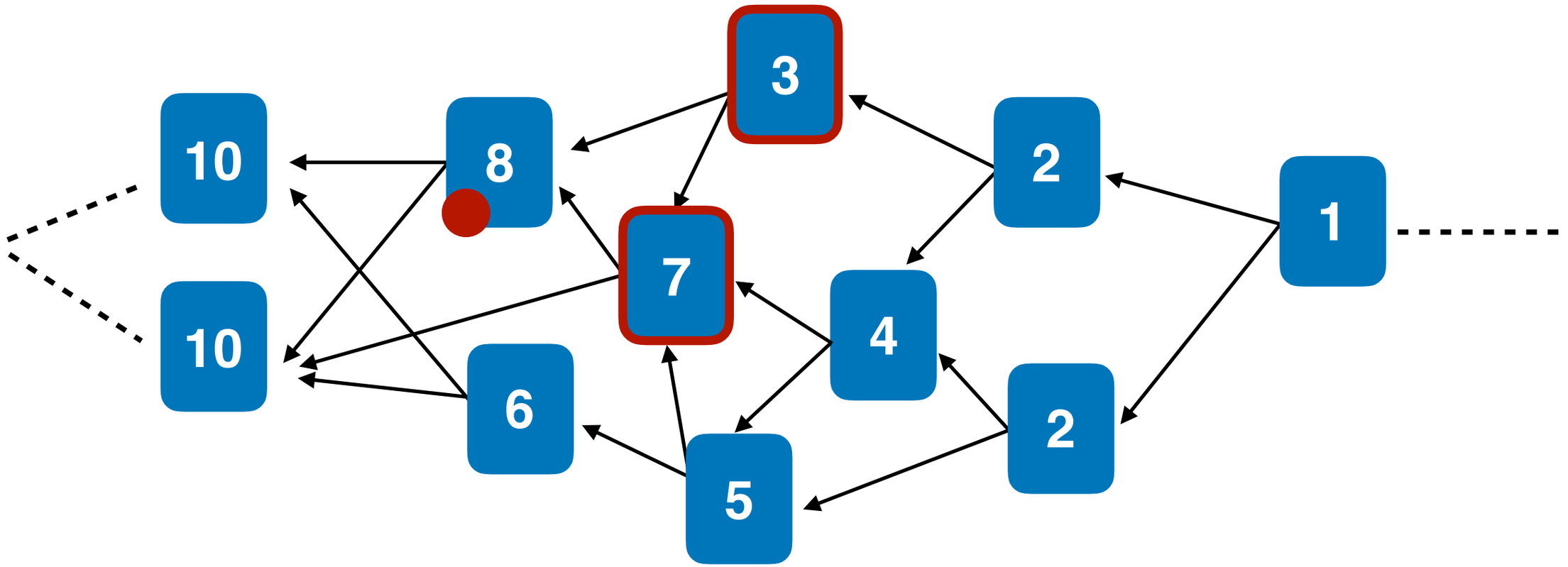
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



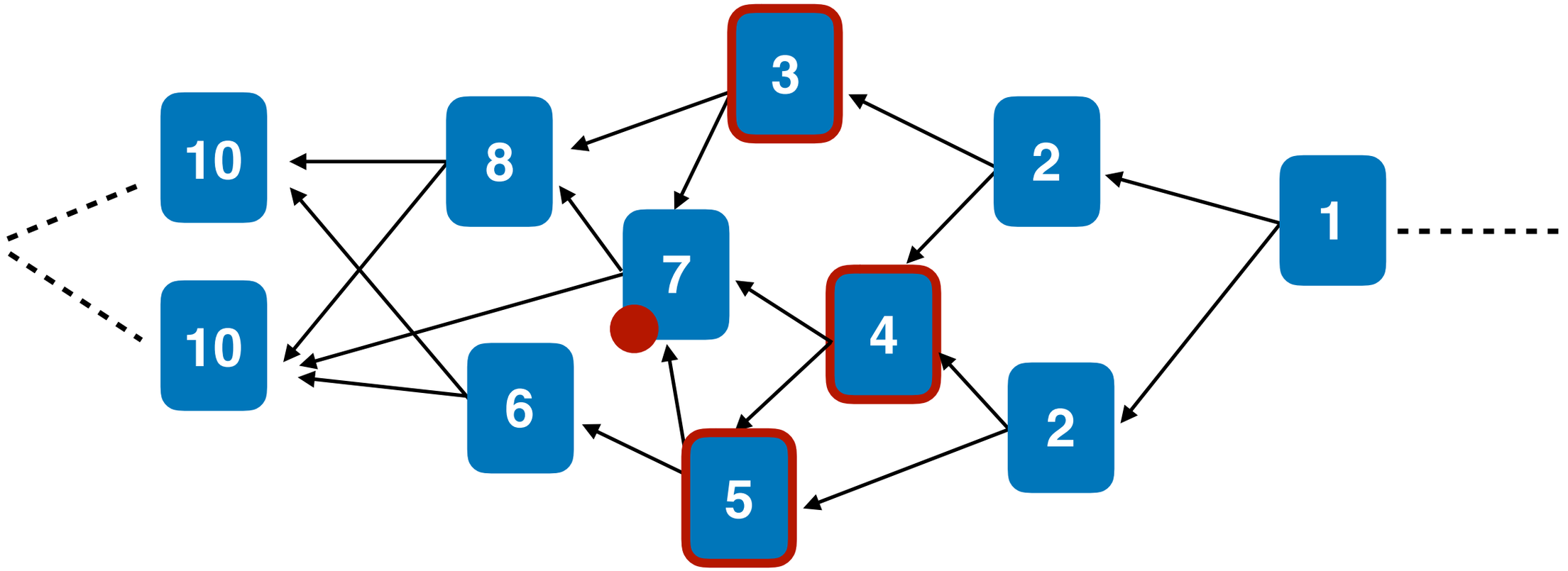
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



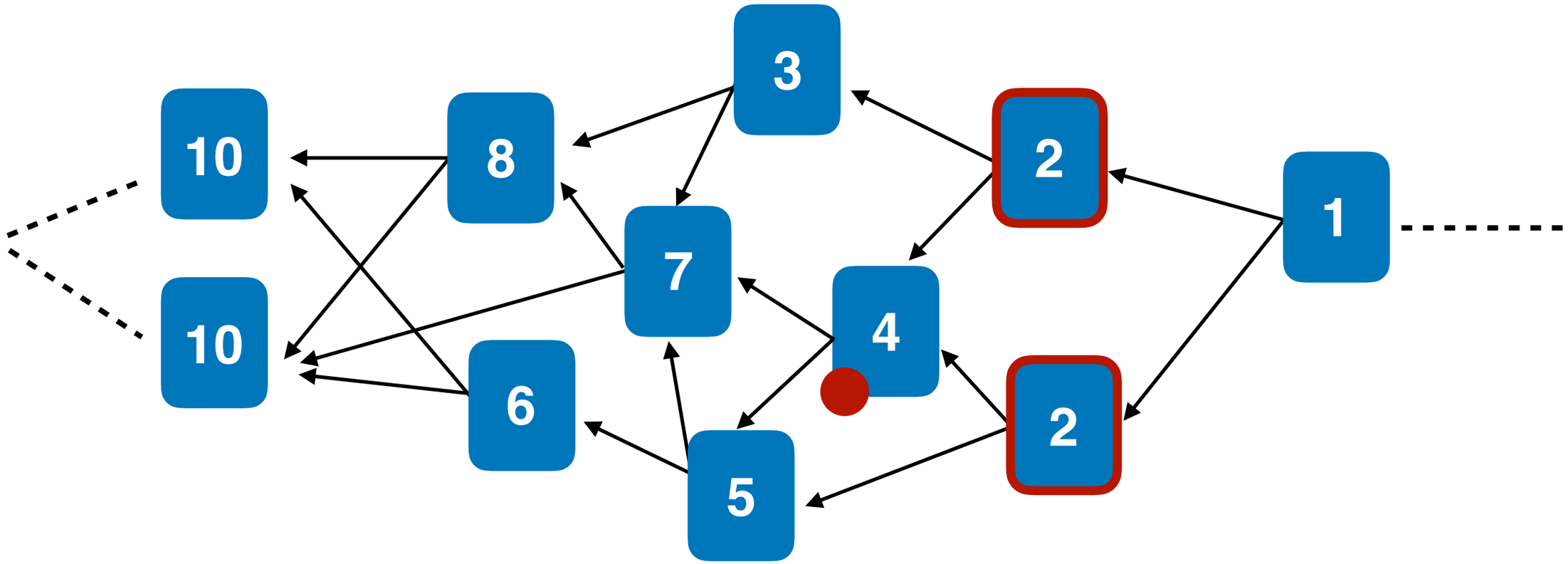
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



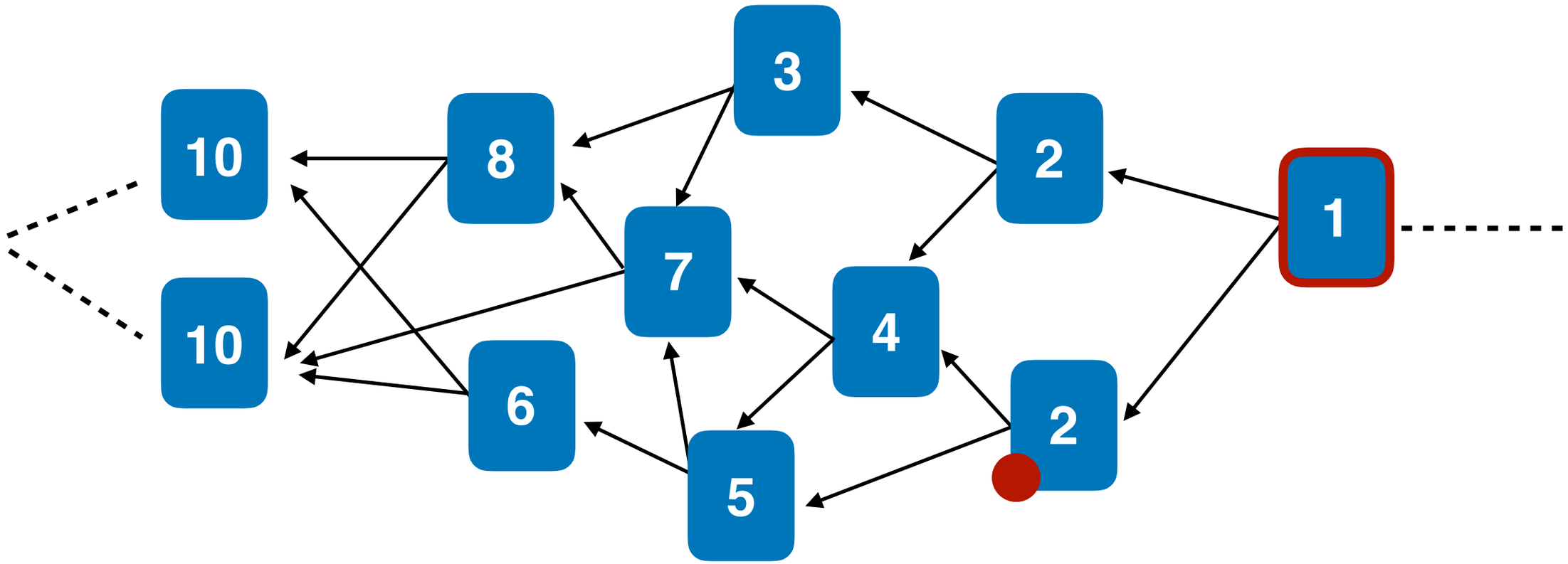
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



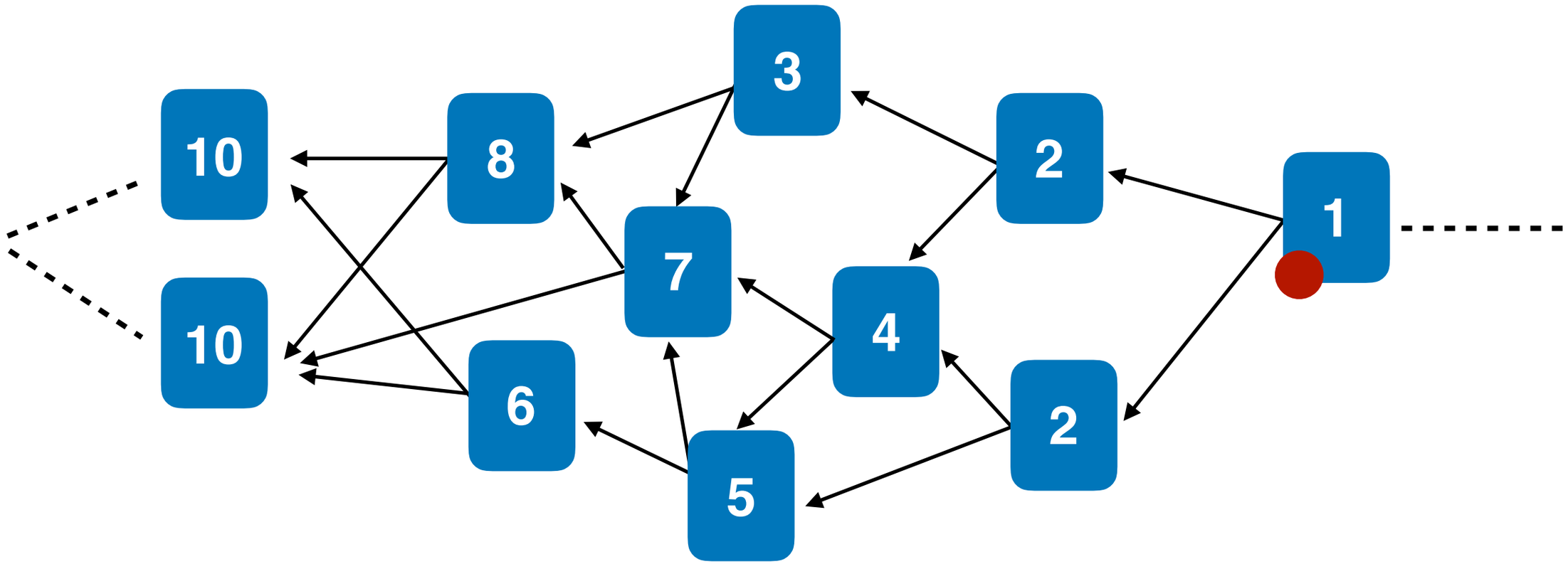
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Weighted Random Walk TSA [1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Rapidly Decaying parameter α [1]

α -> Infinity

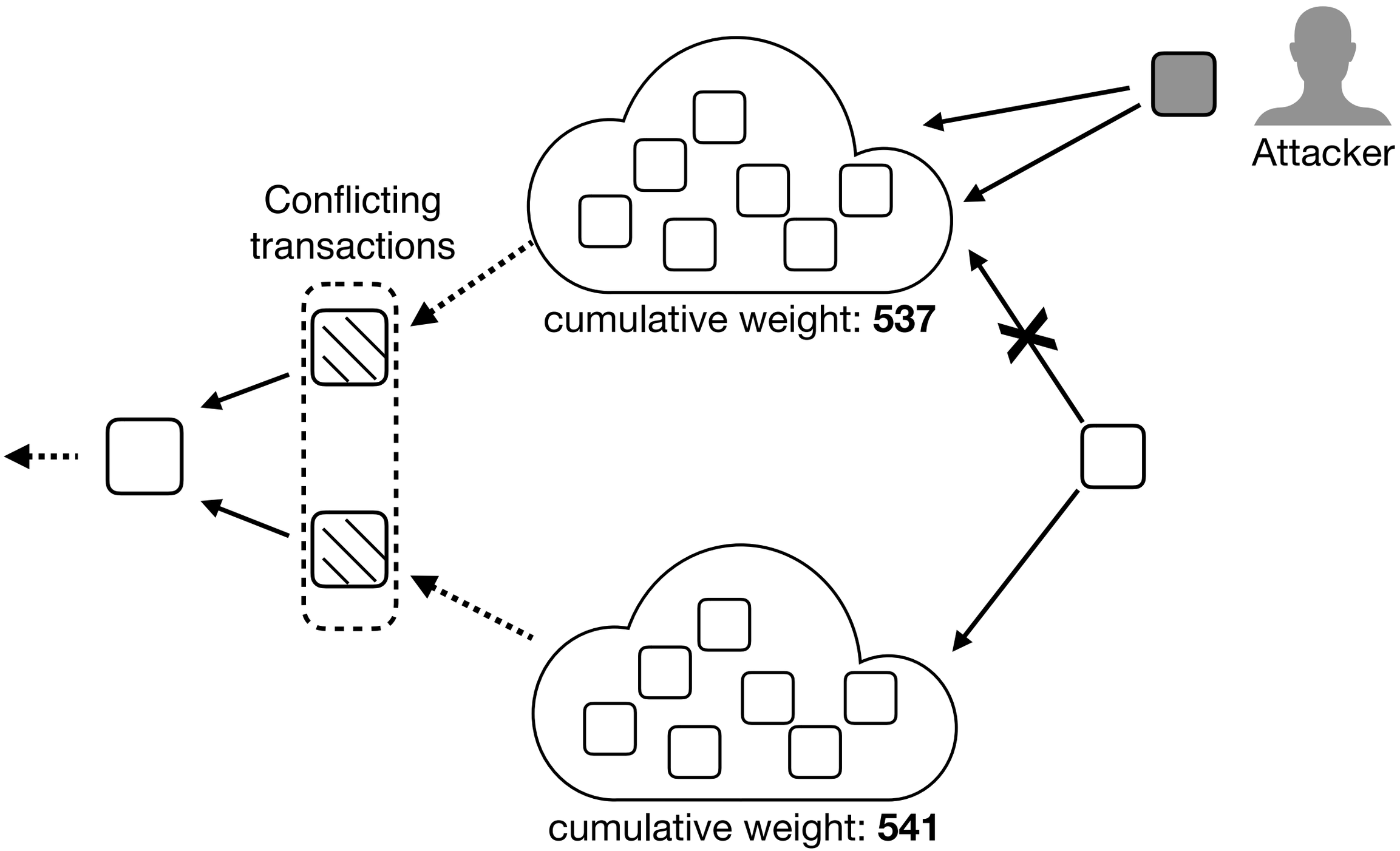
To the next hop having the maximal CW

α -> 0

Weighted Random Walk -> Unweighted Random Walk

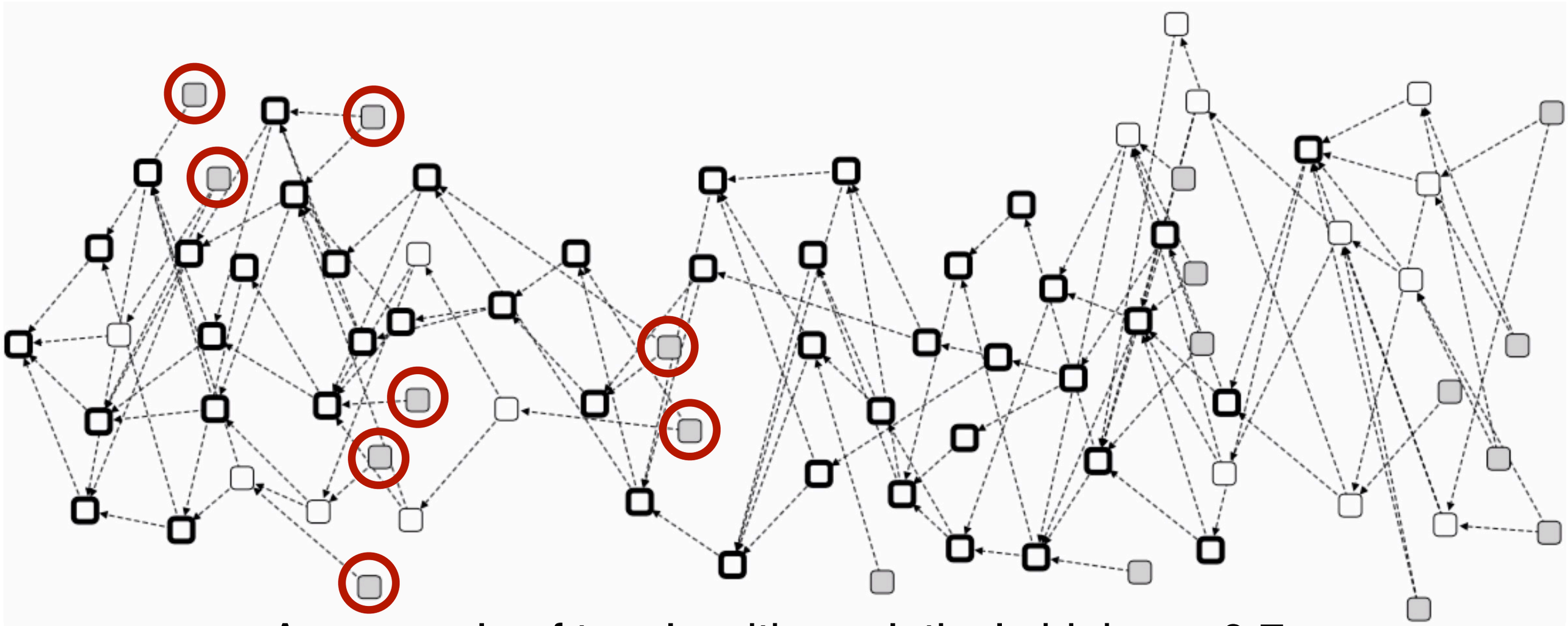
[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Splitting attack [1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

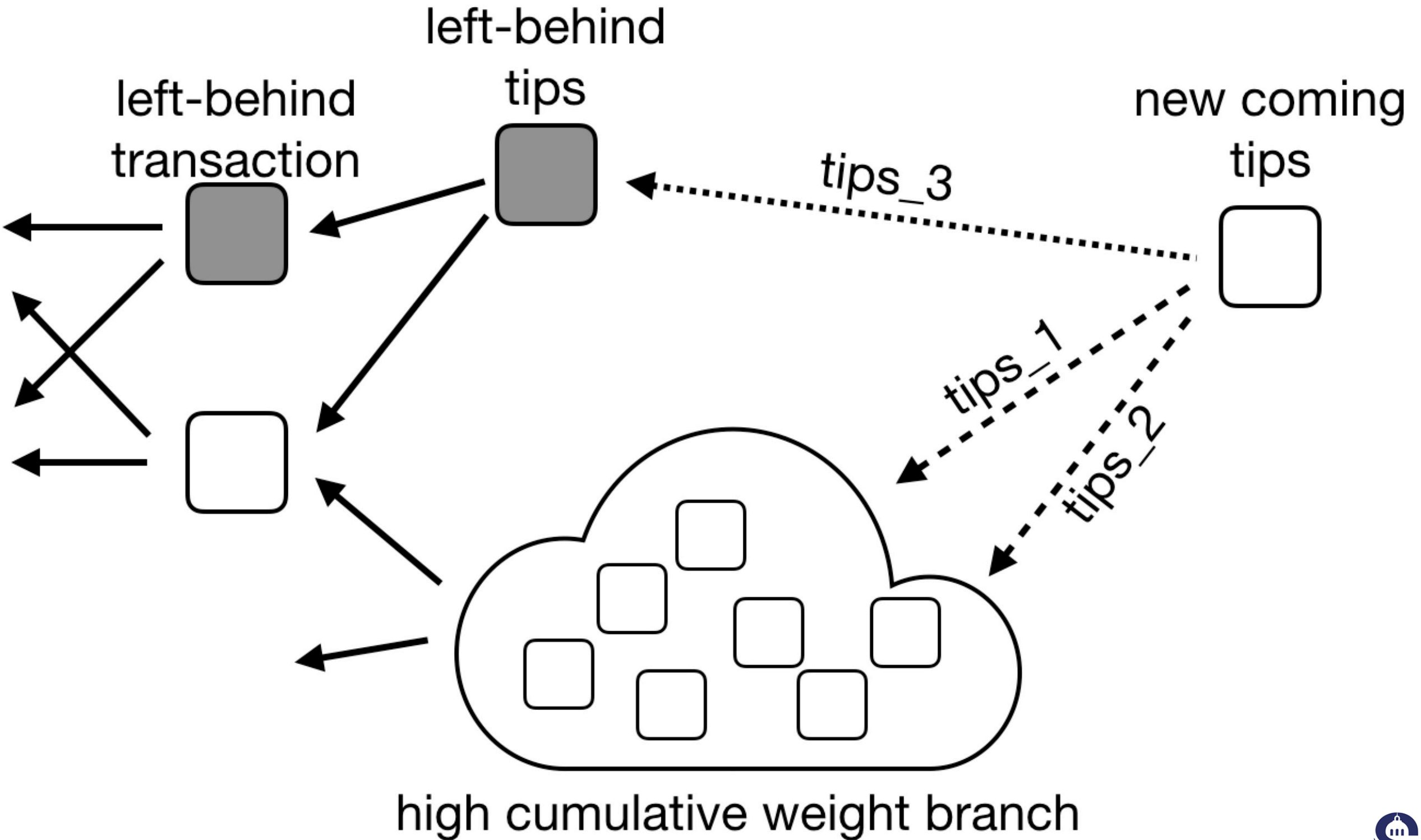
Fairness issue



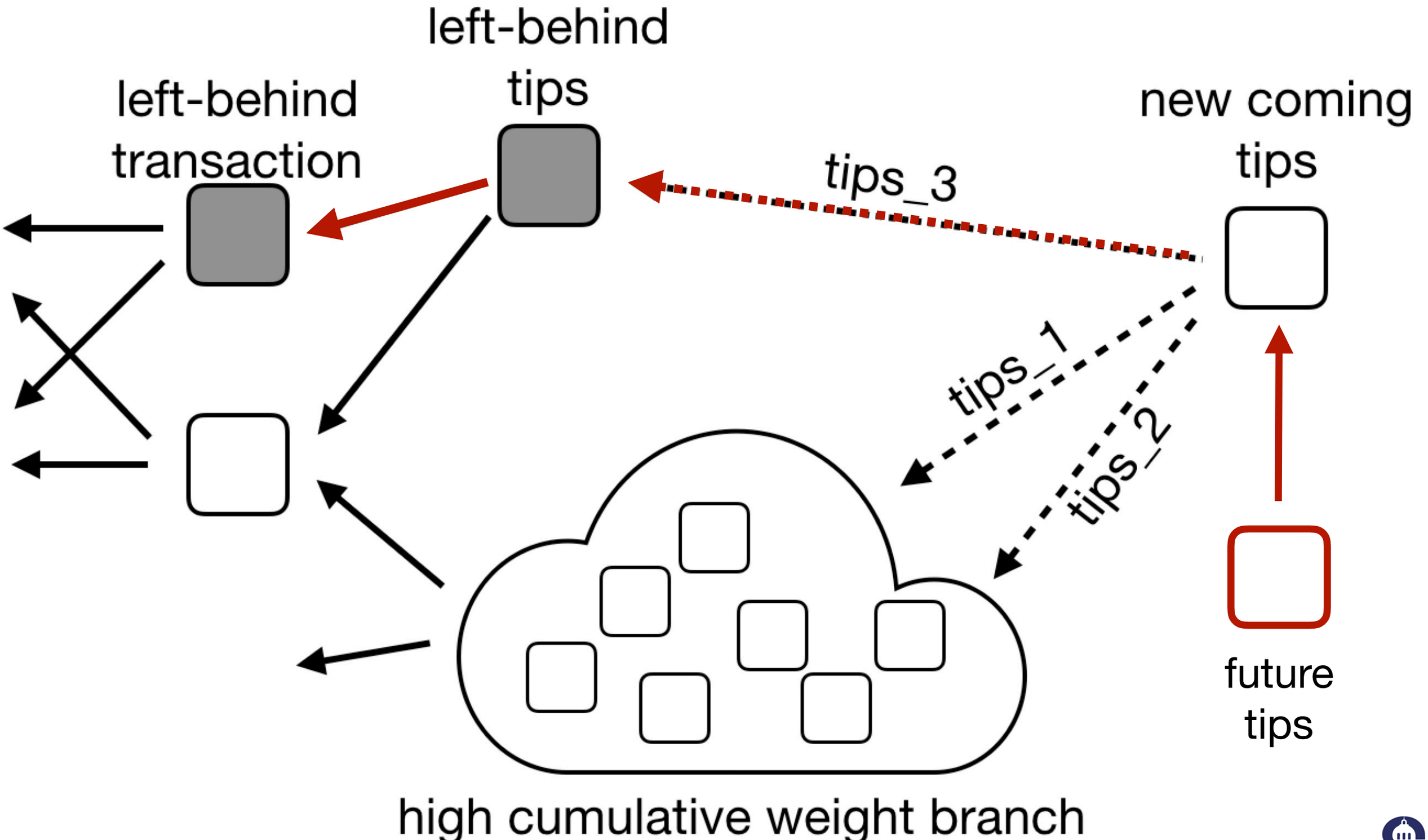
An example of tangle with a relatively high α = 0.7.

Many tips are left behind.

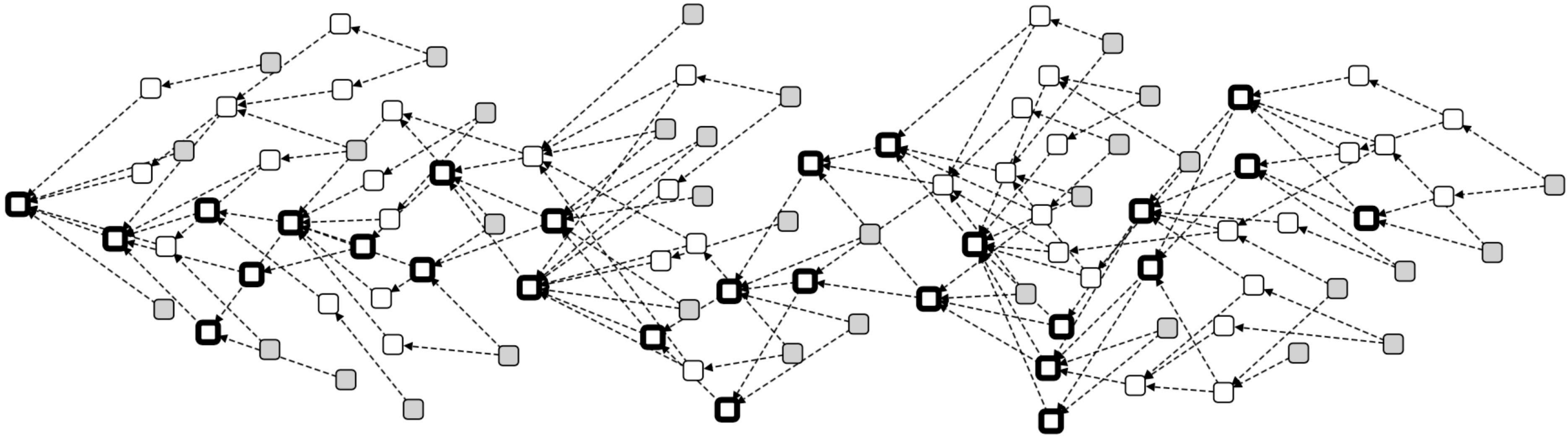
G-IOTA


left-behind
tips
left-behind
transaction
new coming
tips
tips_3
tips_1
tips_2
high cumulative weight branch

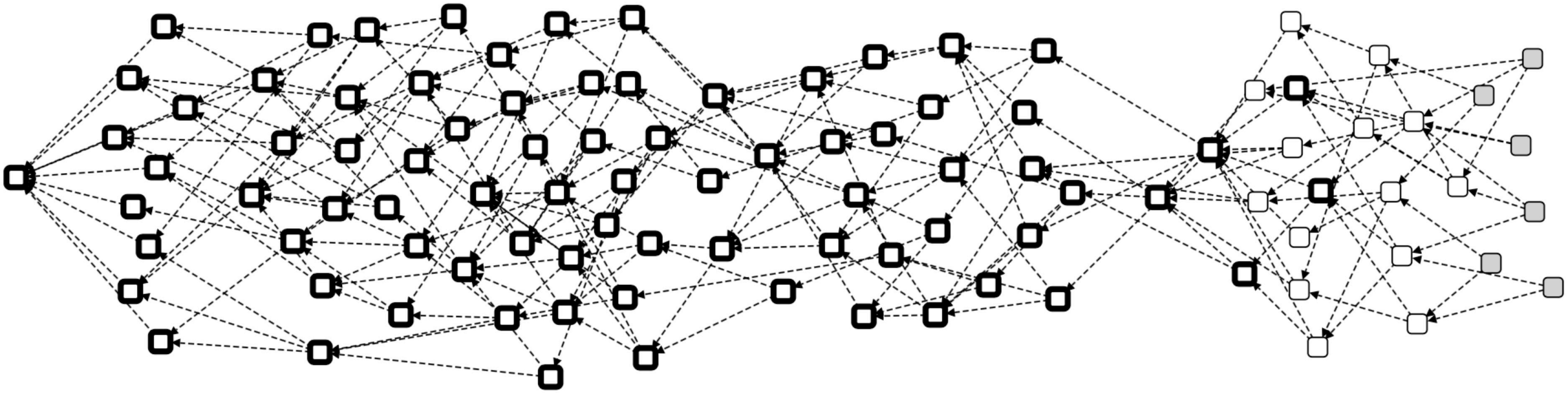
G-IOTA


left-behind
tips
left-behind
transaction
new coming
tips
tips_3
tips_1
tips_2
future
tips
high cumulative weight branch

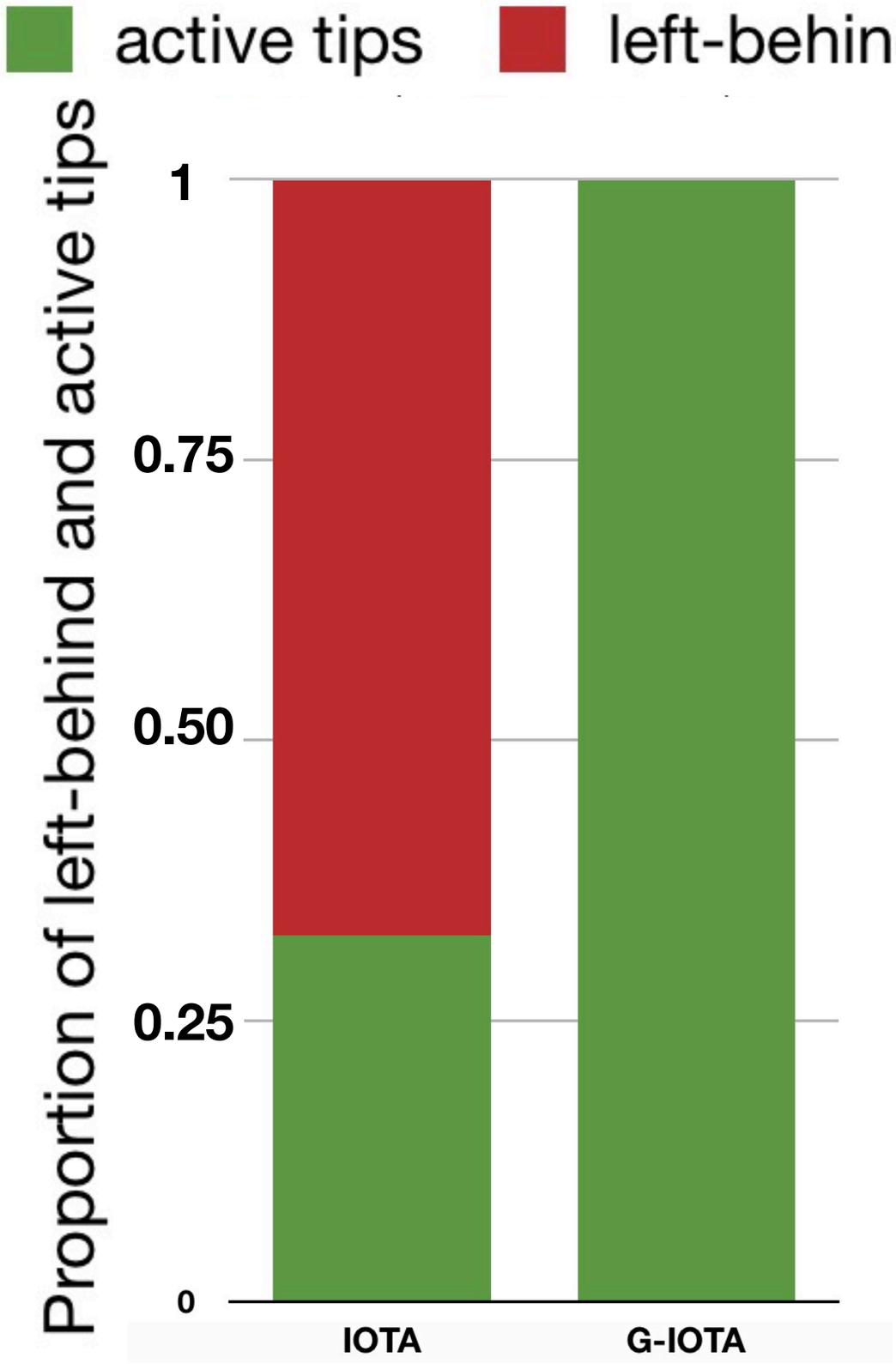
IOTA

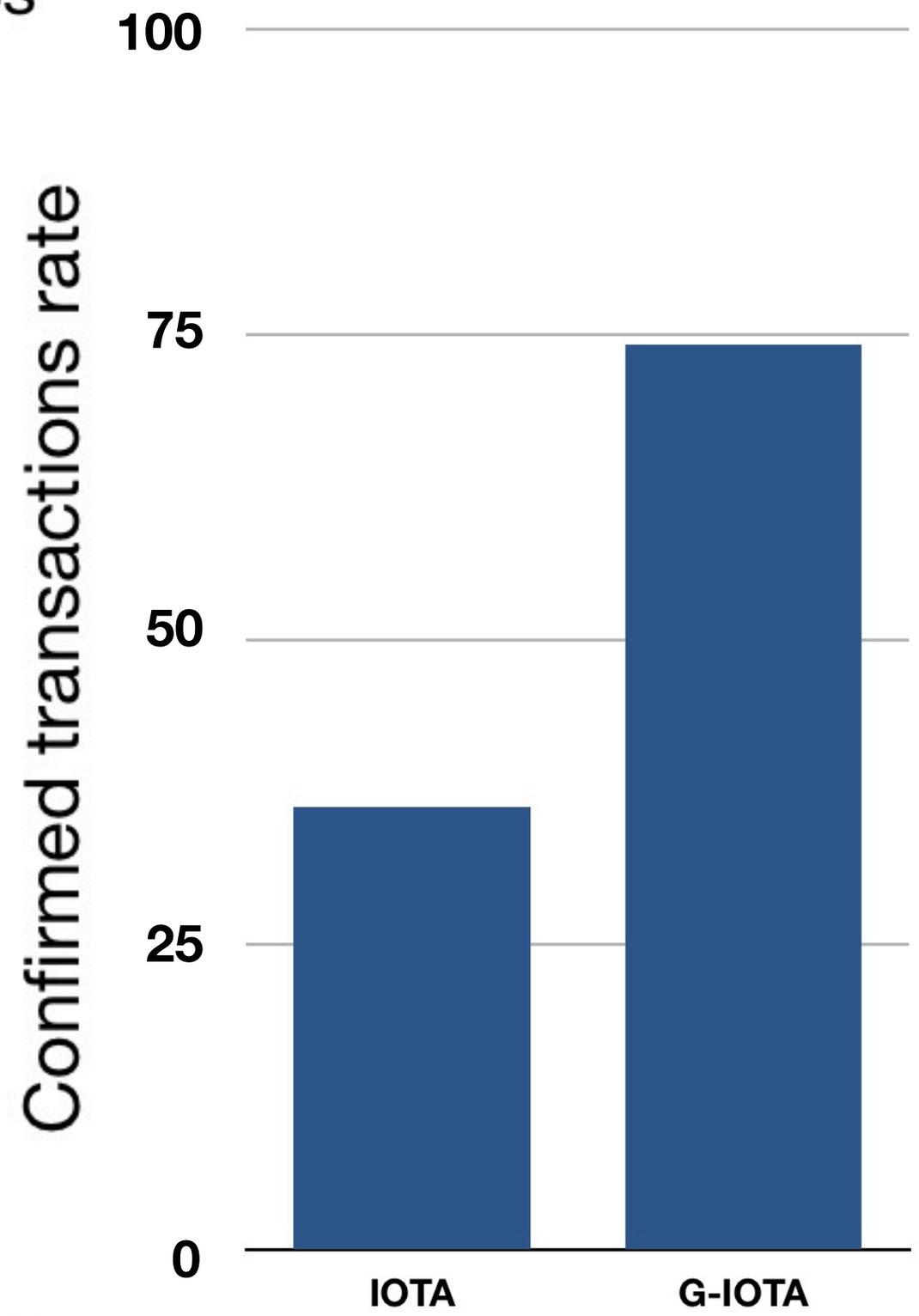


G-IOTA



G-IOTA vs IOTA

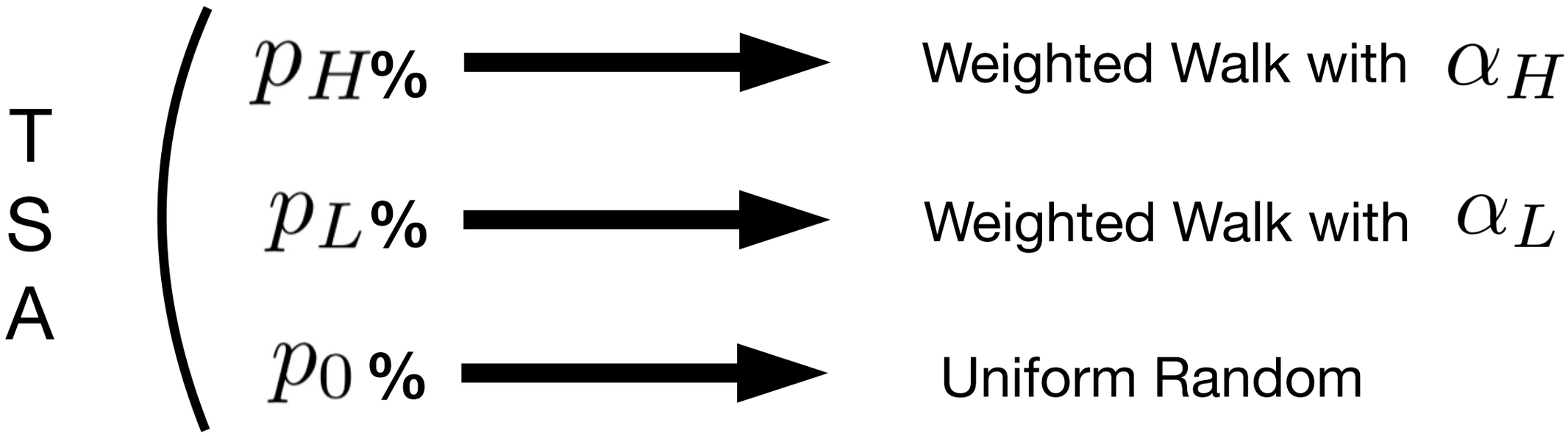




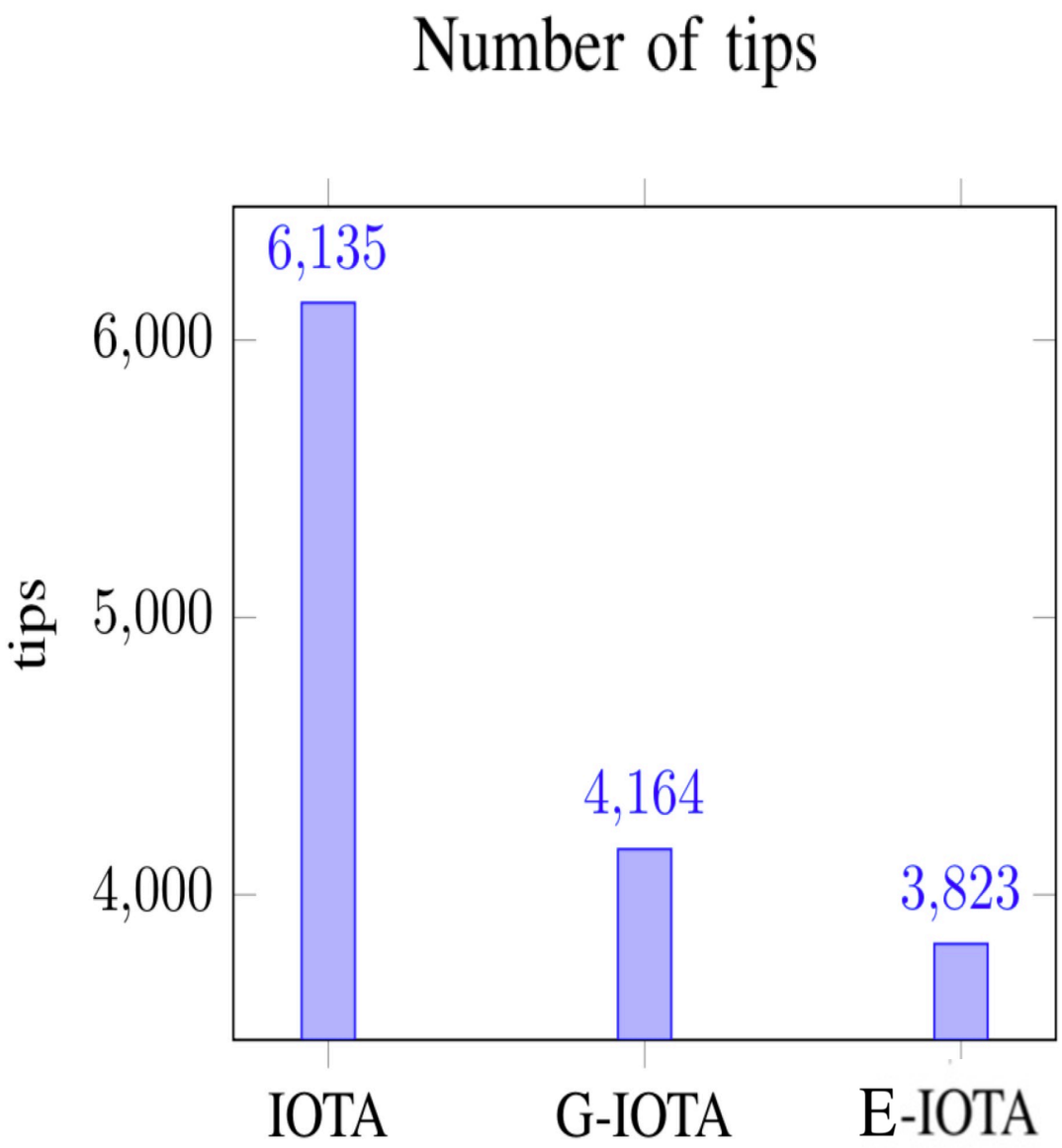
Is 3rd tips necessary?

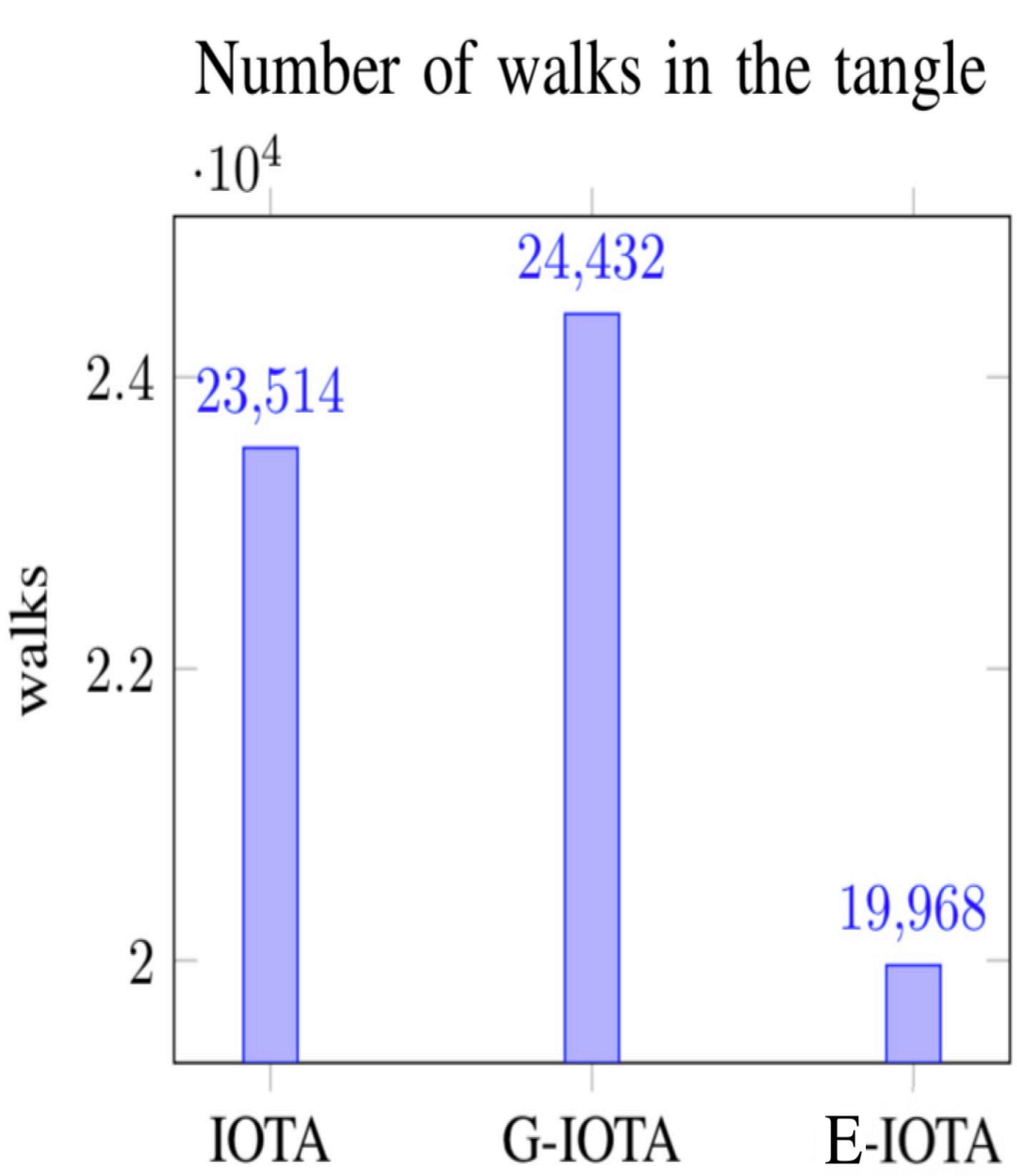
→ **E-IOTA**

E-IOTA : choosing two tips



VISA transaction case: 2000 tps, 8000 transactions





G-IOTA/E-IOTA

Large Weight Attack ✓

Parasite Chain Attack ✓

Splitting Attack ✓

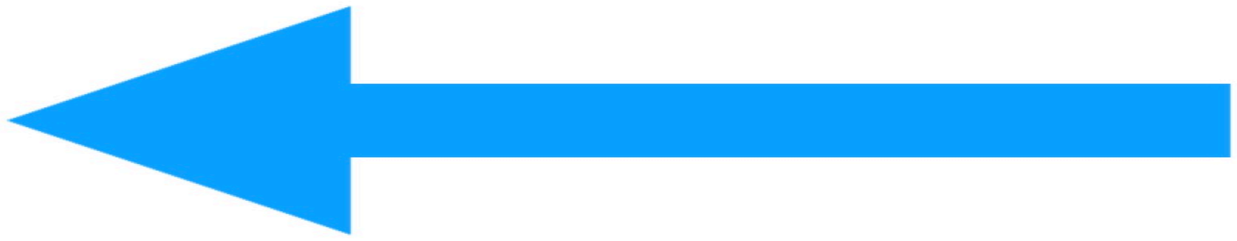
G-IOTA/E-IOTA
Fair and Efficient Aware Tangle

Thank you :)

BlockChain Day

12 Juin 2019

Registration

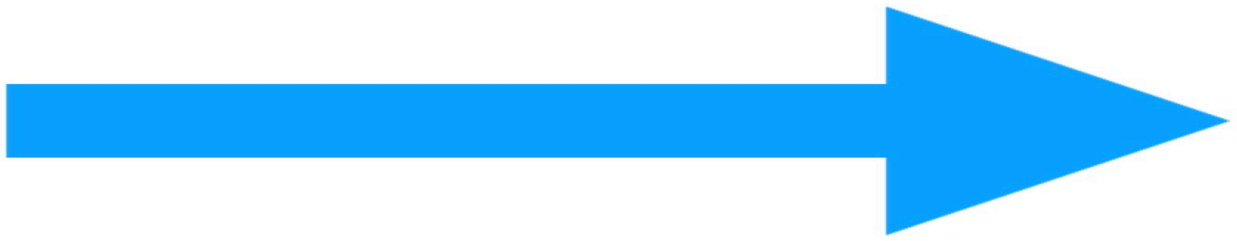


Institut Mines-Télécom · Inria INVENTEURS DU MONDE NUMÉRIQUE · NOKIA · SORBONNE UNIVERSITÉ CRÉATEURS DE FUTURS DEPUIS 1257 · SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE

BlockChain Day

12 Juin 2019

Registration



titut Mines-Télécom

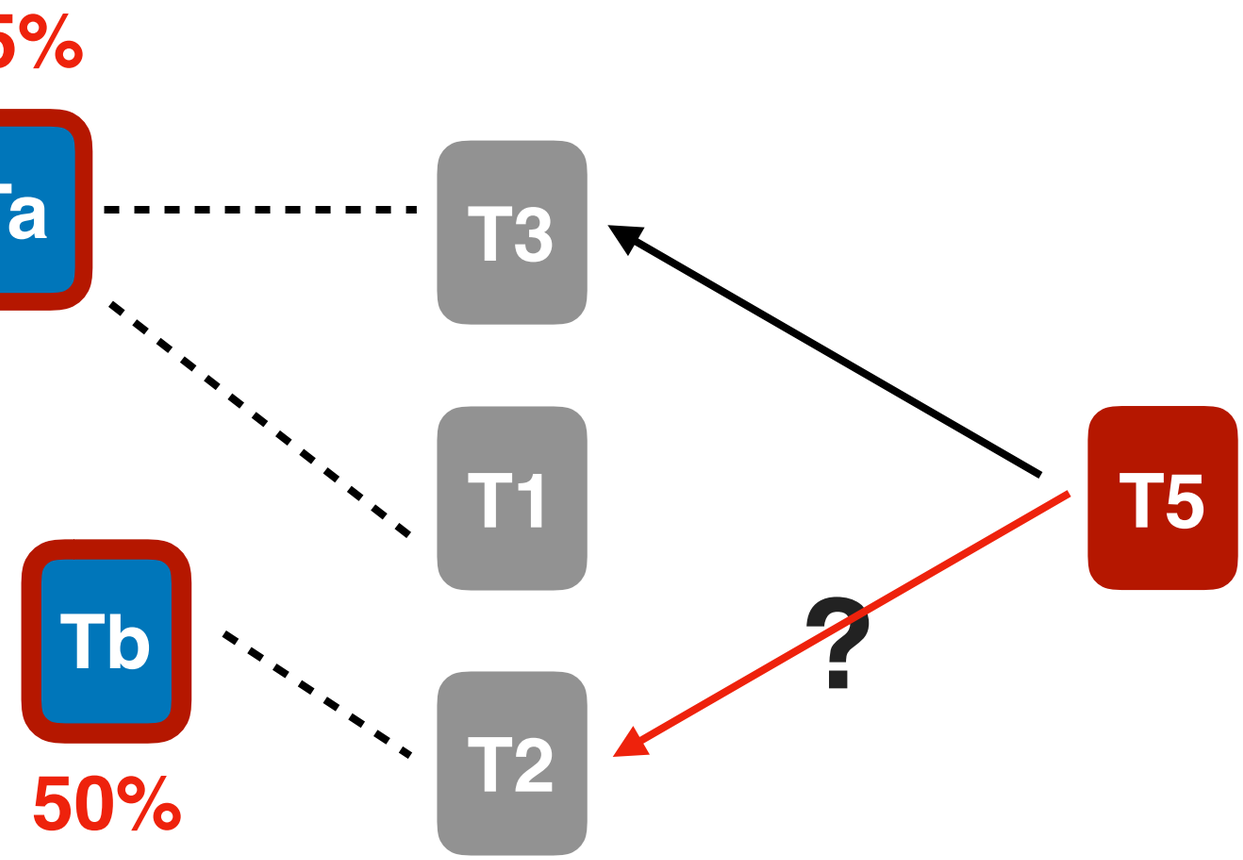
INVENTEURS DU MONDE NUMÉRIQUE

NOKIA

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

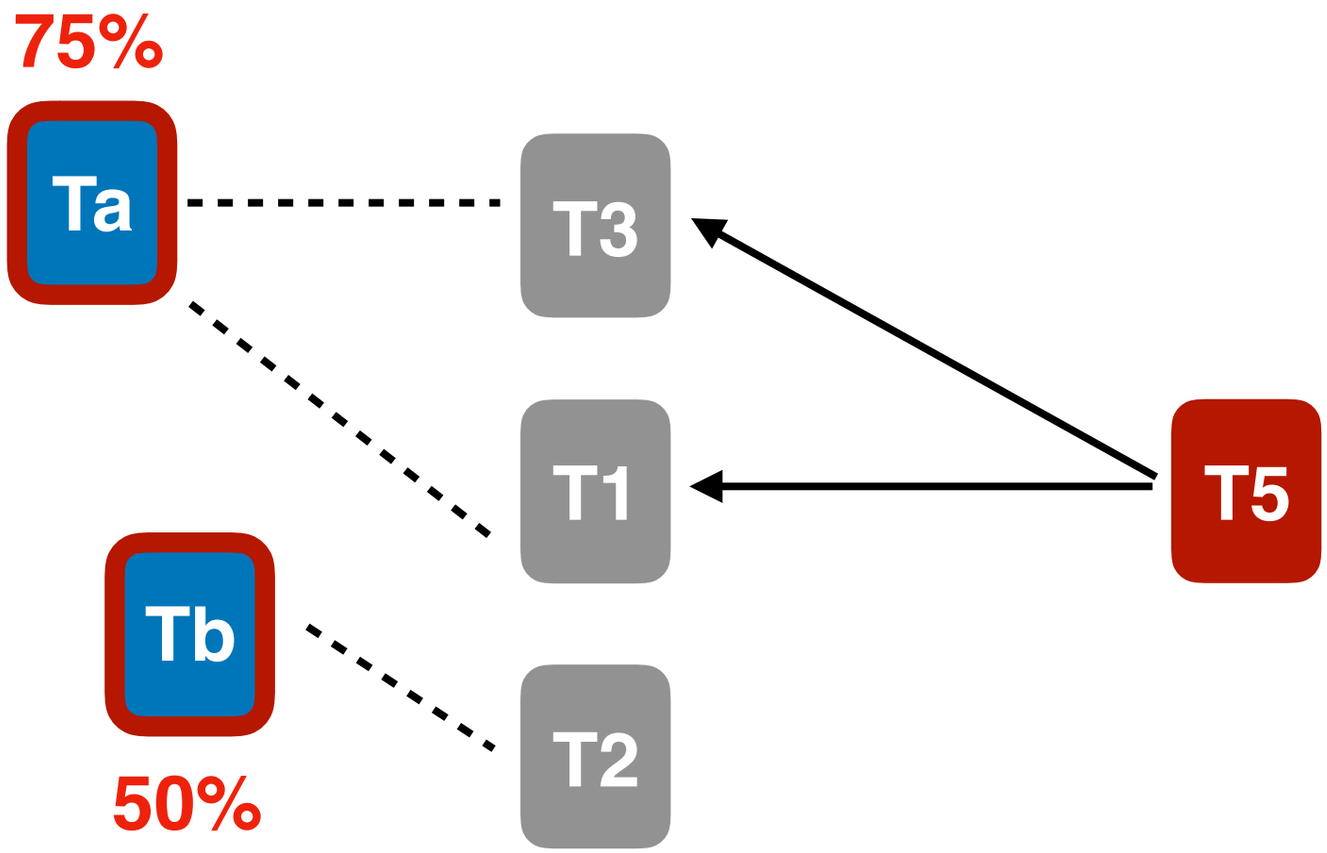
INSTITUT DE RECHERCHE TECHNOLOGIQUE

Conflicting Transactions[1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

Conflicting Transactions[1]



[1] Popov S. The tangle[J]. cit. on, 2016: 131.https://www.iota.org

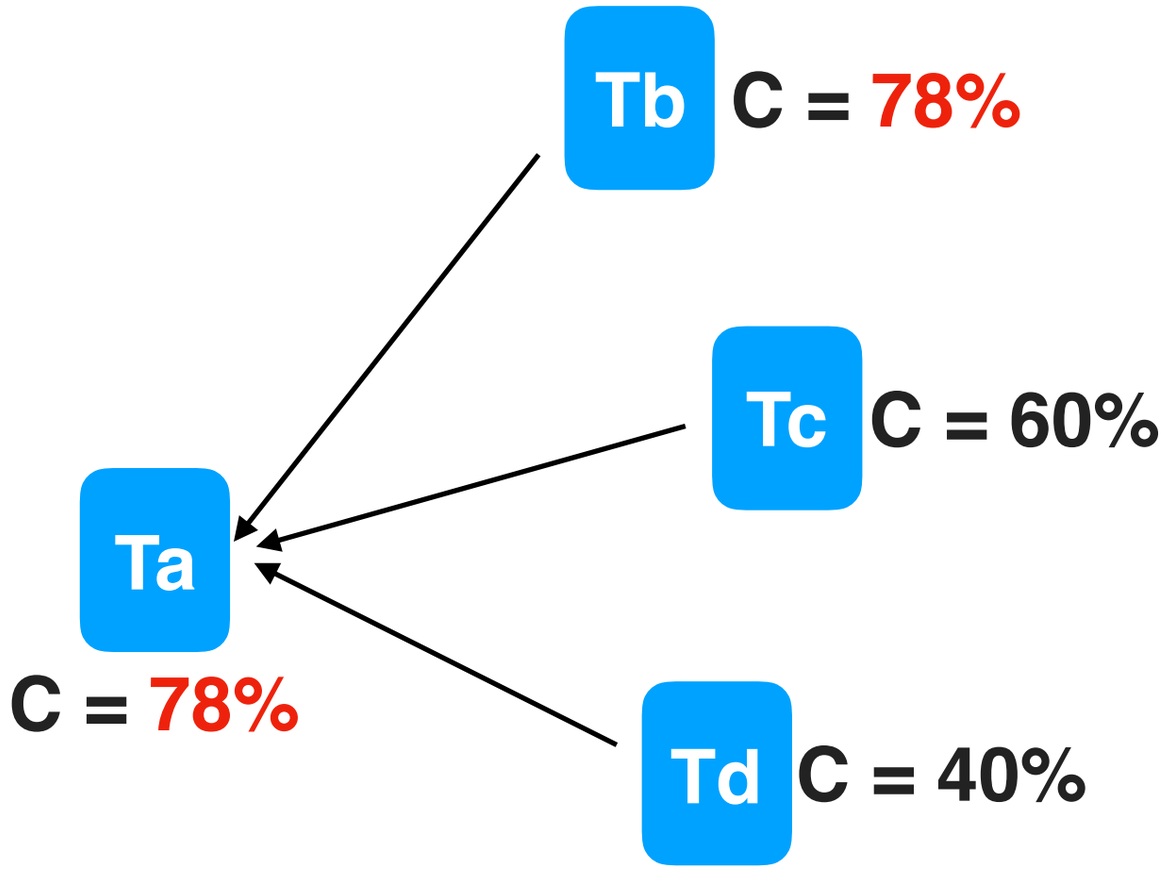
Fairness issue

Left-behind tips: tips who have not been approved for a time ***D_tips***.

Left-behind transactions: non-tips transactions who have not been confirmed for a time ***D_tran***.

Observation

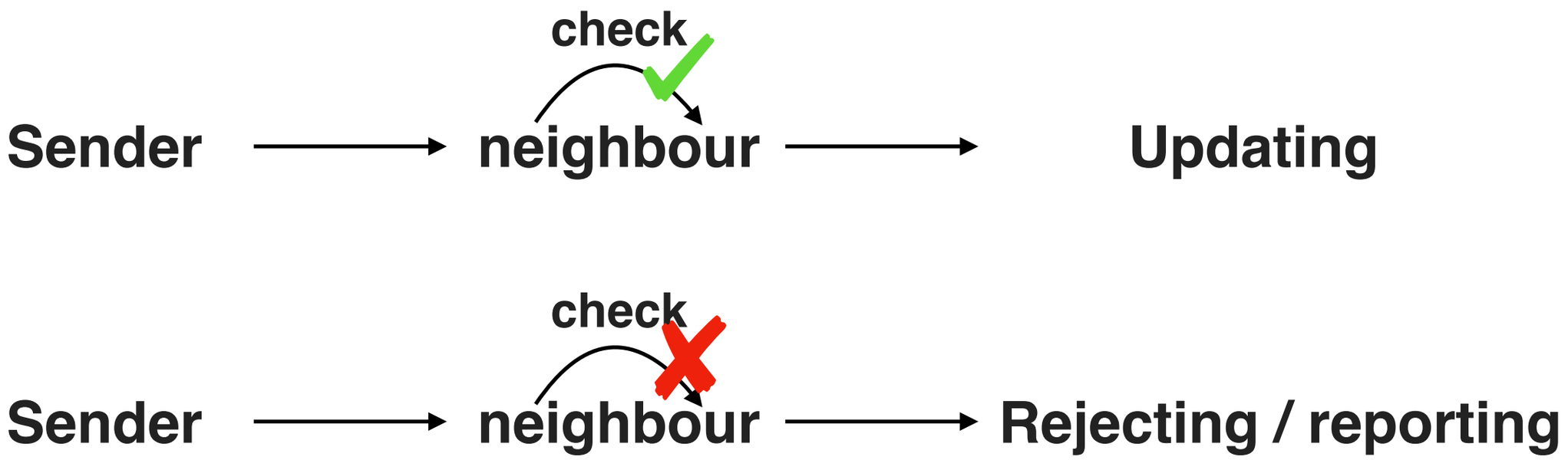
The confidence of a transaction is at least equal to the maximal confidence among all its son transactions.



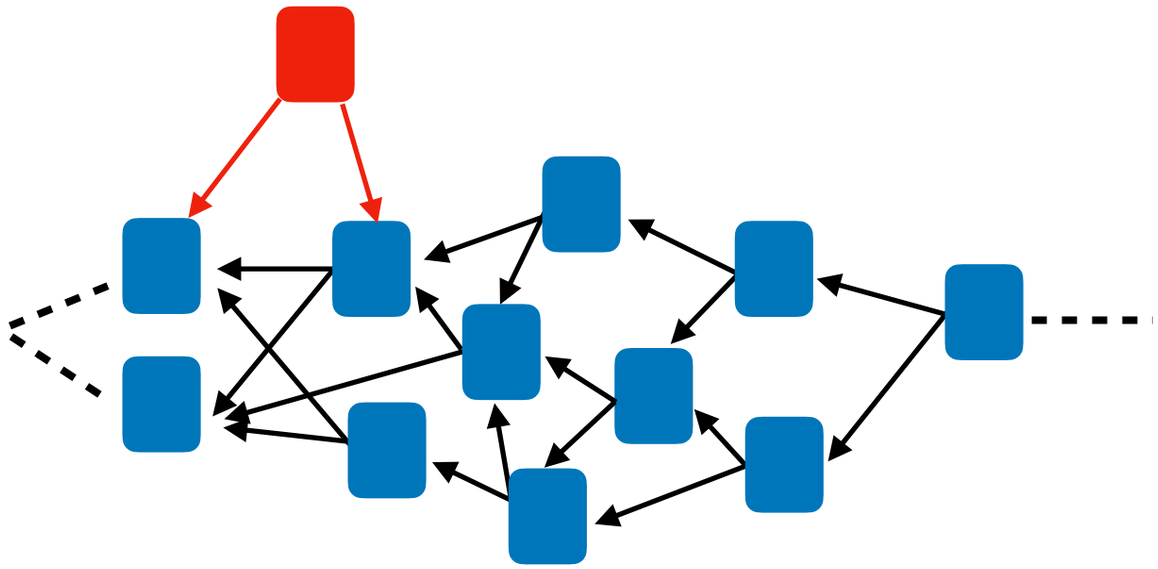
Mutual Supervision Mechanism

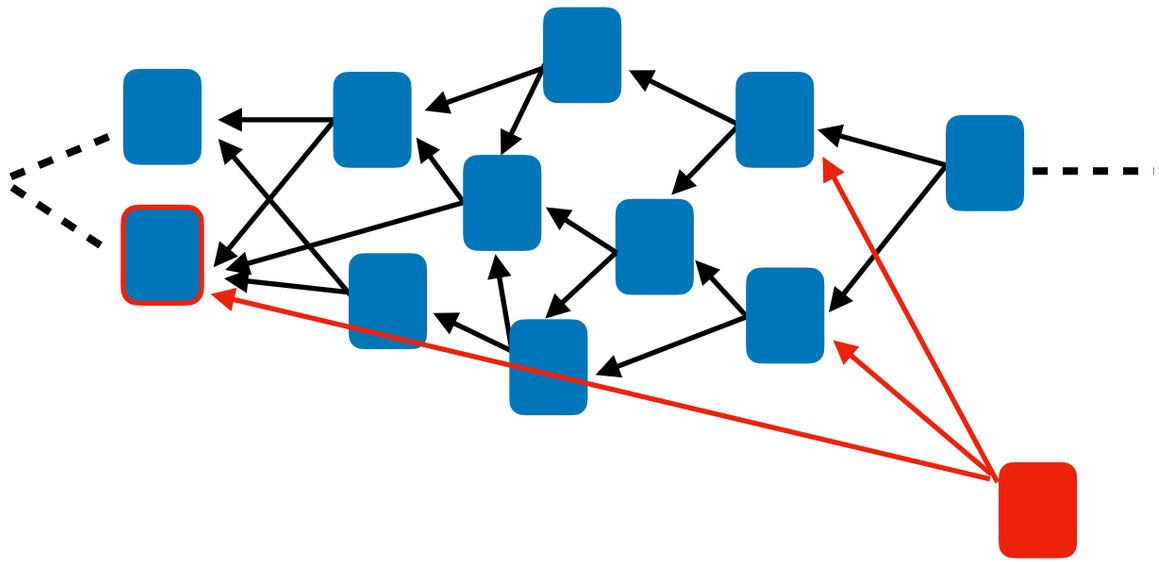
1) What if a speculative user always verifies a third tips, a non-left-behind tips, to pretend that it works hard for helping the others?

2) What if a lazy user only chooses old conformed transactions to verify and pretends his transaction has been left-left-behind and waits others saving his transaction?

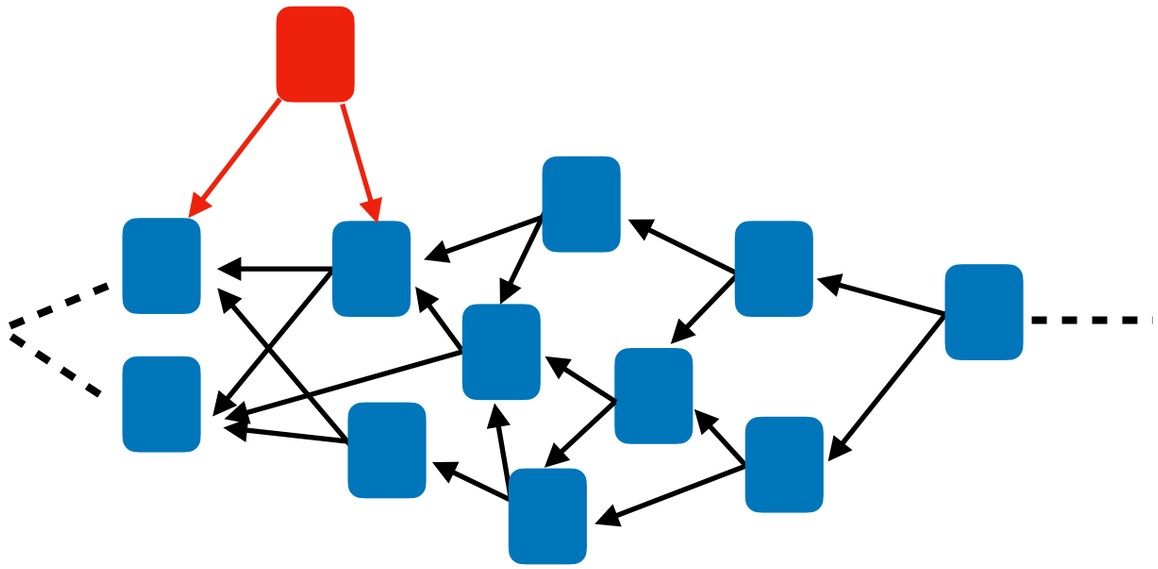


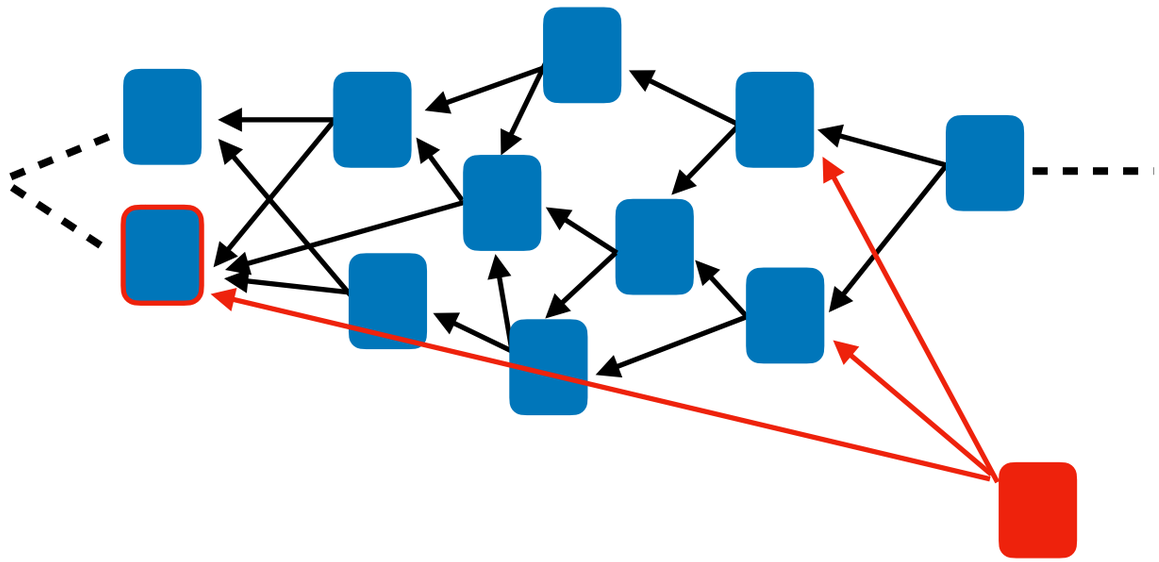
Mutual Supervision Mechanism





Mutual Supervision Mechanism





Networking layer effect

- **Benefit of choosing the 3nd tips**

  → **Game theory Proof**

- **G-IOTA has at lest the same security level than IOTA**

  → **Formal proof**

- **Is 3 tips necessary?**

  → **New deign**

IOTA	G-IOTA
Computation	More
Left Behind Tips	No

IOTA	G-IOTA	E-IOTA
Computation	More	Less
Left Behind Tips	No	No

E-IOTA

honest: *1* **unit** **attacker:** P_a**%**

Large Weight Attack

weight of a transaction is limited

Parasite Chain Attack

$$p_L + p_H > p_0$$

Splitting Attack

$$p_H > P_a$$