Parasite Chain Detection in the IOTA 1.0 Protocol

Andreas Penzkofer - Iota Foundation

Context
IOTA

permissionless

distributed

feeless

immutable

no miners

scalable

backbone for IoT

open-source

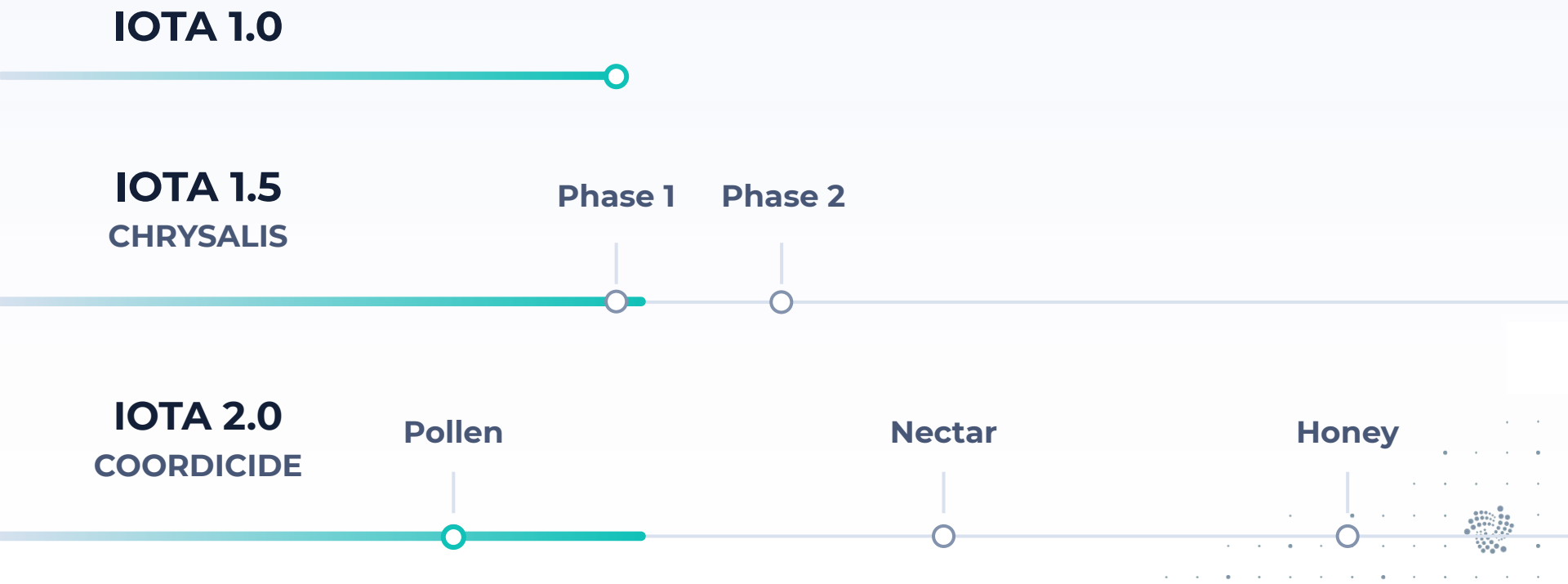
data and value transfer

Context
Stages of Mainnet

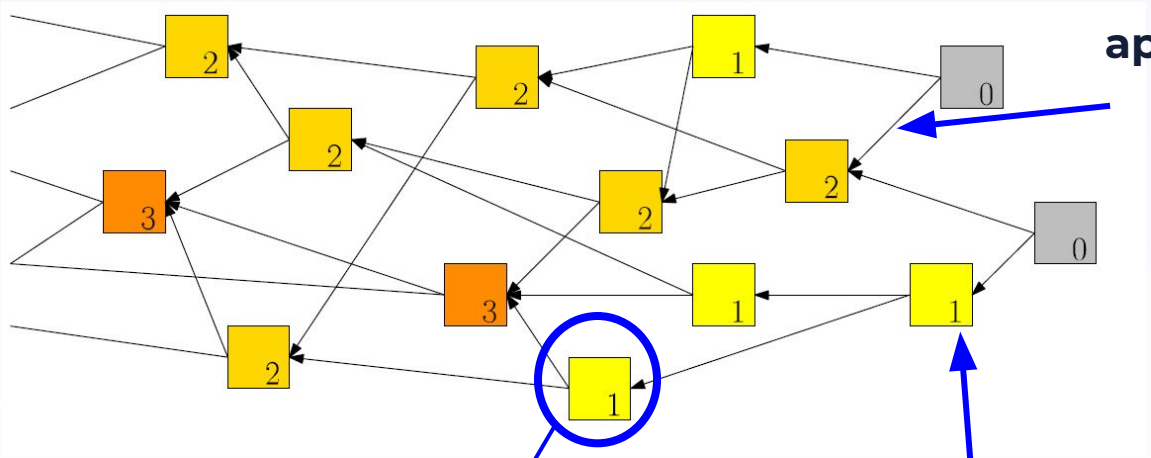
IOTA 1.0	IOTA 1.5 (Chrysalis)	IOTA 2.0 (Coordicide)
Network secured through PoW Majority of transaction issuers are honest Currently network also secured through checkpoints (issued by coordinator node)	Various modifications to the protocol: Improved tip selection Autopeering Atomic transactions UTXO Improved throughput Faster confirmations … https://roadmap.iota.org/chrysalis	Major changes to the protocol : Voting protocol Rate and Congestion Control Node bootstraping and syncing … https://coordicide.iota.org/

This presentation applies to the protocol version IOTA 1.0

Context
Stages of Mainnet



The Tangle
IOTA 1.0



Transaction approves tip and becomes tip

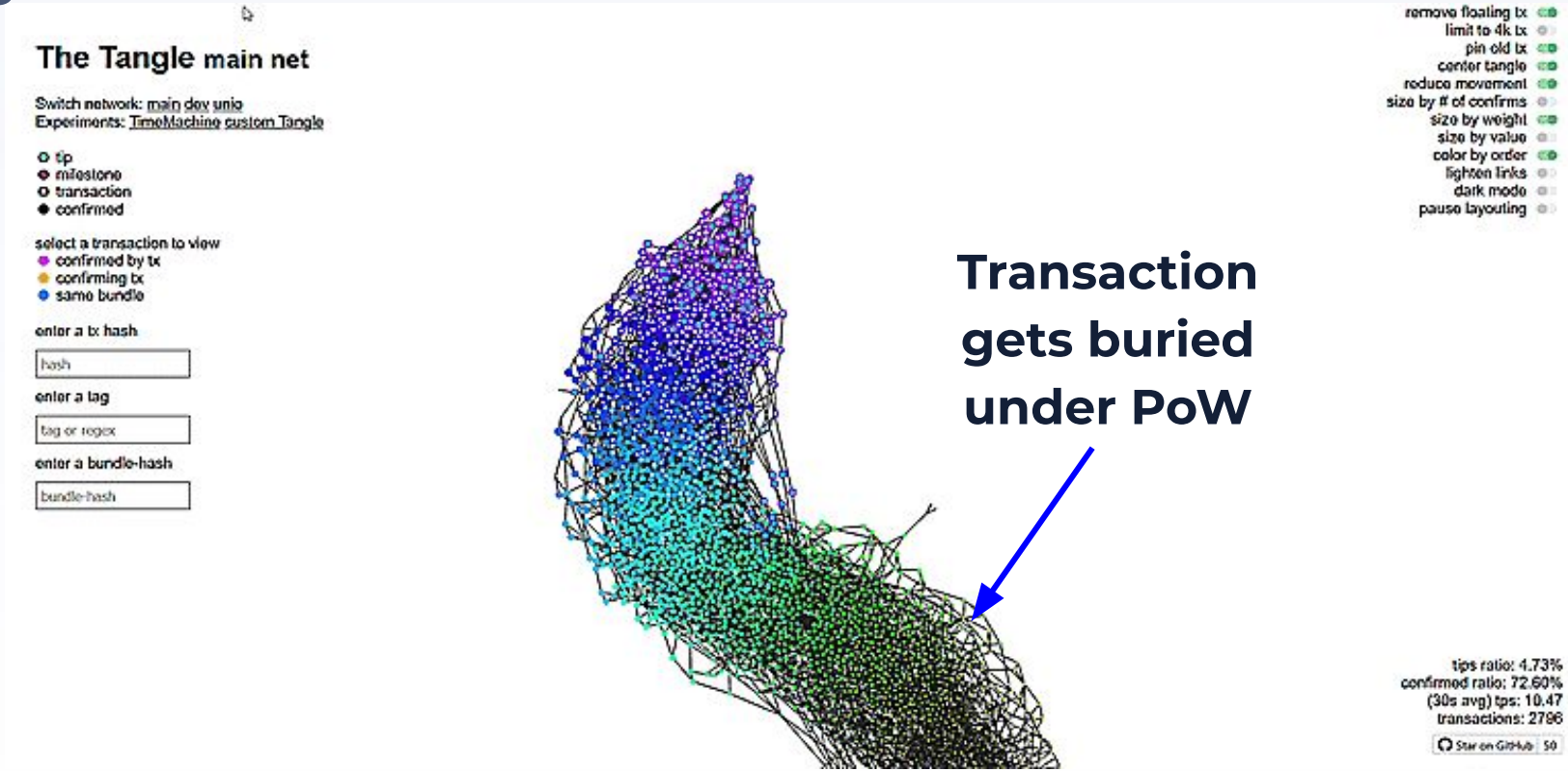
Transaction

Number of approvers

Ledger structure

- Directed Acyclic Graph (DAG)
- grows by each transaction referencing 2 previous transactions

The Tangle Mainnet



Tip selection methods

Nodes are FREE to choose which transactions to approve.

Considered tip selection algorithms

Tip selection methods

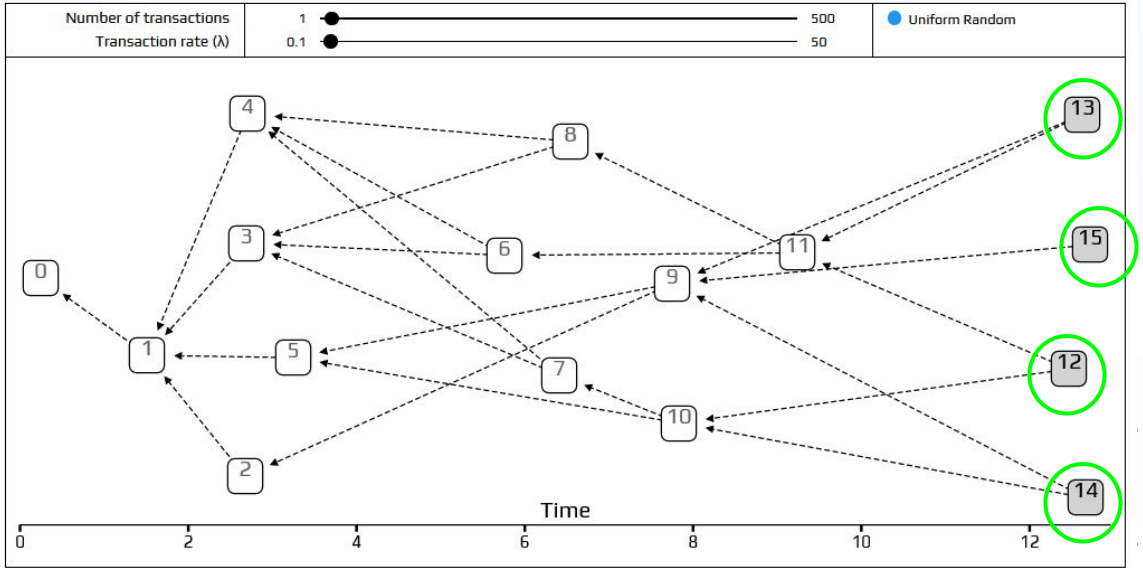
Nodes are <u>FREE</u> to choose which transactions to approve.

Considered tip selection algorithms

Uniform random (URTS) ⟷ **Unbiased random walk (URW)** ⟷ **Biased random walk (BRW)**

Procedure:

1) **Select tip at random**



Tip selection methods

Nodes are <u>FREE</u> to choose which transactions to approve.

Considered tip selection algorithms

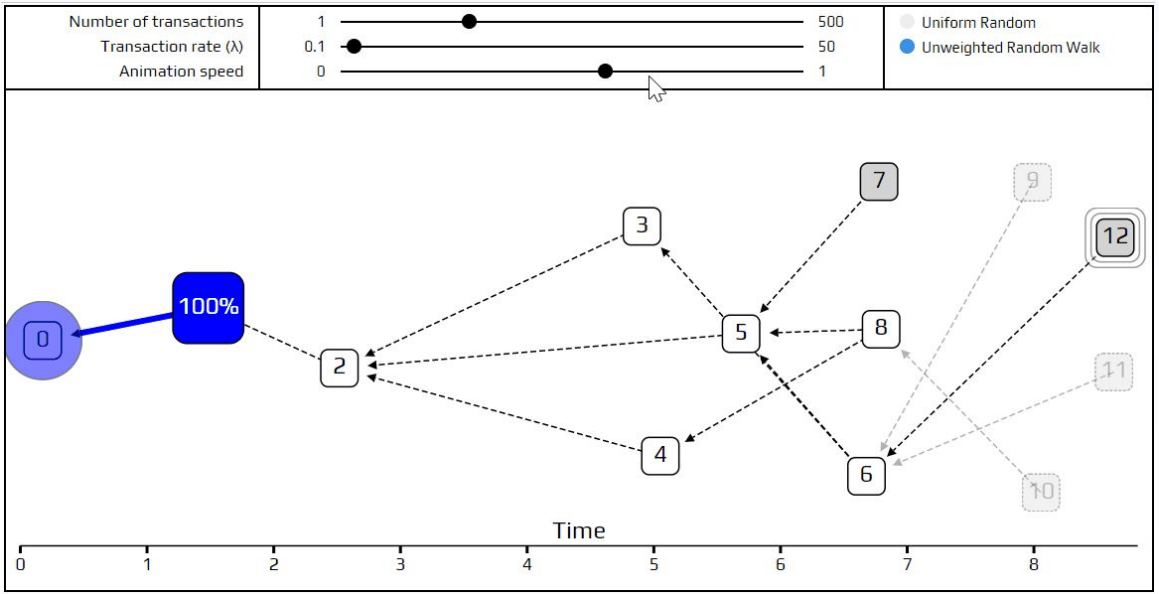
Uniform random (URTS) ⟷ **Unbiased random walk (URW)** ⟷ Biased random walk (BRW)

Procedure:

1) **start random walk deep in the Tangle**

2) **pick one of the children transactions with equal probability**

3) **repeat 2 - 4 until reaching a tip**



Tip selection methods

Nodes are FREE to choose which transactions to approve.

Considered tip selection algorithms

Uniform random (URTS) ⟺ Unbiased random walk (URW) ⟺ **Biased random walk (BRW)**

Procedure:

1) start random walk deep in the Tangle

2) for each step, calculate the transition probability P_{xy} to all children transactions

3) pick one of the children transactions with probability P_{xy}

4) repeat 2 - 4 until reaching a tip

$$P_{xy} = \frac{\exp(\alpha \mathcal{H}_y)}{\sum_{z:z\to x} \exp(\alpha \mathcal{H}_z)}$$

Biased random walk
Parameter choice

α

α small

same as uniform random tip selection

Allows for lazy tip selection

More vulnerable to attacks

suitable α

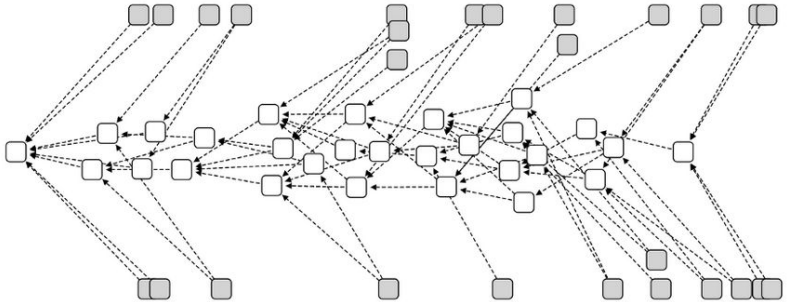
Value in IOTA 1.0 :
α = .001

α large

Transactions left behind (Orphanage)

Need for reattachments and promotions

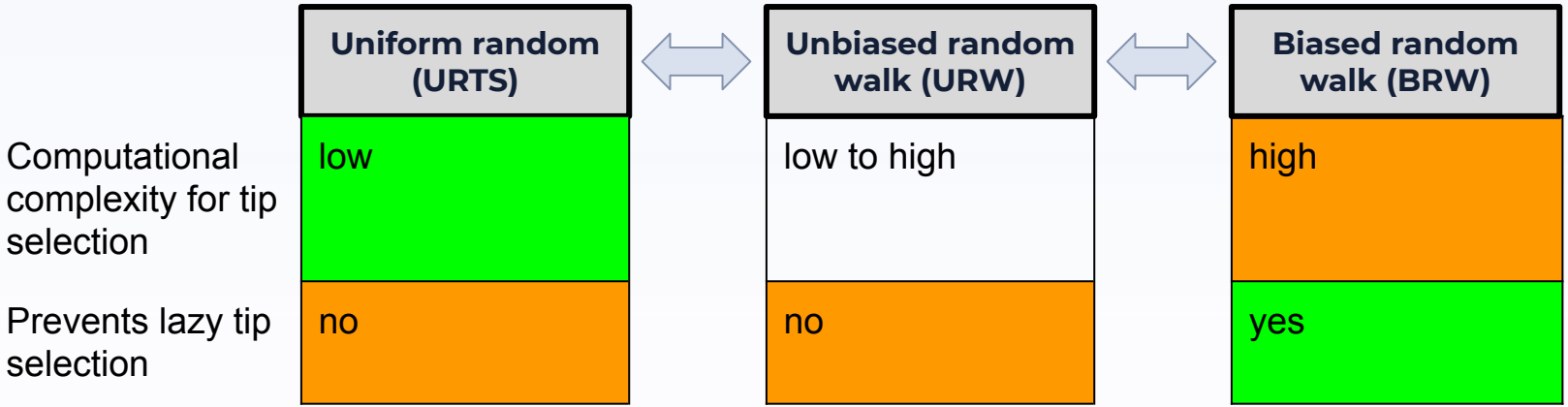
Decreased maximum throughput



Tip selection methods

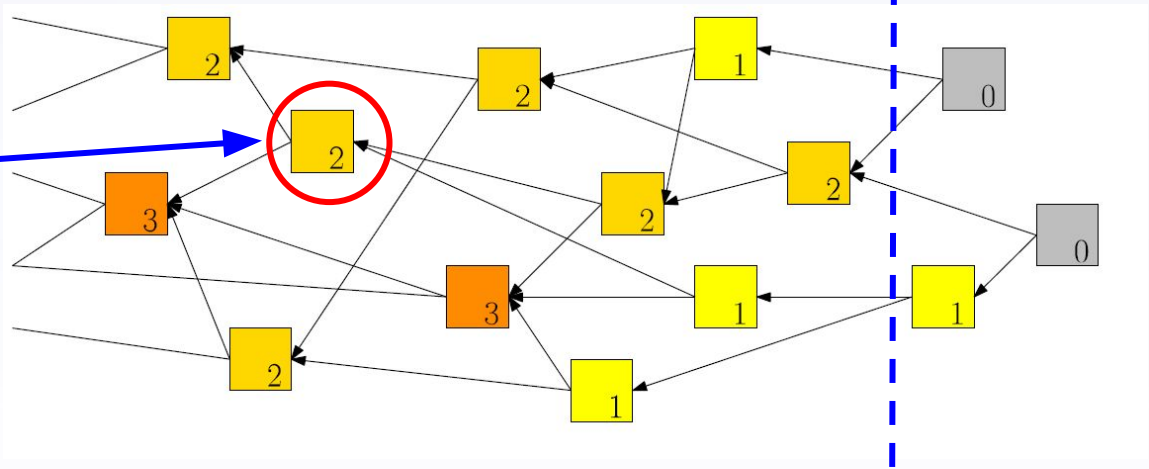
Nodes are FREE to choose which transactions to approve.

Considered tip selection algorithms



Parasite Chain attack
Concept

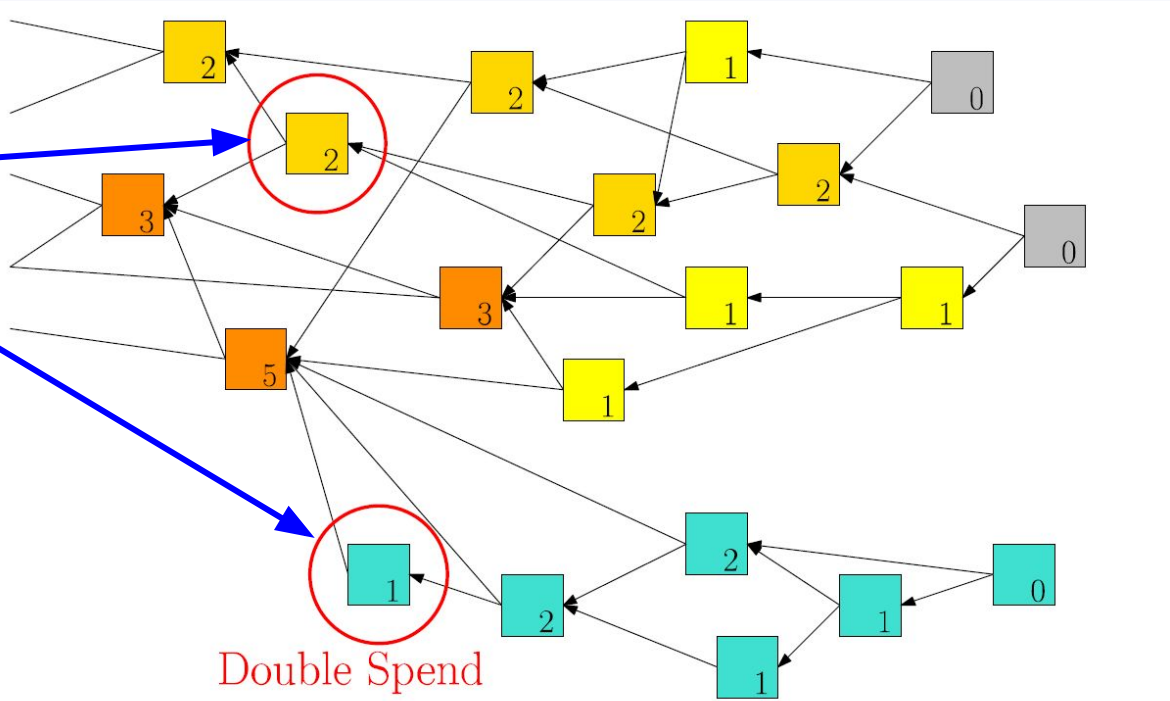
Attacker spends the funds



Sometime later the merchant accepts the funds

Parasite Chain attack
Concept

Spends the same funds



Tip selection methods

Nodes are <u>FREE</u> to choose which transactions to approve.

Considered tip selection algorithms

	Uniform random (URTS)	Unbiased random walk (URW)	Biased random walk (BRW)
Computational complexity for tip selection	low	low to high	high
Prevents lazy tip selection	no	no	yes
Attack to attempt double spend	Create many tips	PC by creating many links to the past	PC with high amount of PoW
Necessary PoW for attack	low	low	high

Uniform Random tip selection
Model

Number of tips

Transactions arrive through Poisson process: $P(\gamma, n) = e^{-\gamma}\frac{\gamma^n}{n!}$

Number of tips modelled by $L = 1 + 2\lambda$

Tx rate

Uniform Random tip selection
Model

Number of tips

Transactions arrive through Poisson process: $P(\gamma, n) = e^{-\gamma}\frac{\gamma^n}{n!}$

Number of tips modelled by $L = 1 + 2\lambda$

Number of approvers

$$N_i = 1 + Pois(\lambda_i)$$

$$\lambda_i = \lambda \int_{t_i}^{t_i+h} dt\ (\ 2p_i(t) - p_i(t)^2)$$

Uniform Random tip selection
Model

Number of tips

Transactions arrive through Poisson process:

$$P(\gamma, n) = e^{-\gamma}\frac{\gamma^n}{n!}$$

Number of tips modelled by $L = 1 + 2\lambda$

Number of approvers

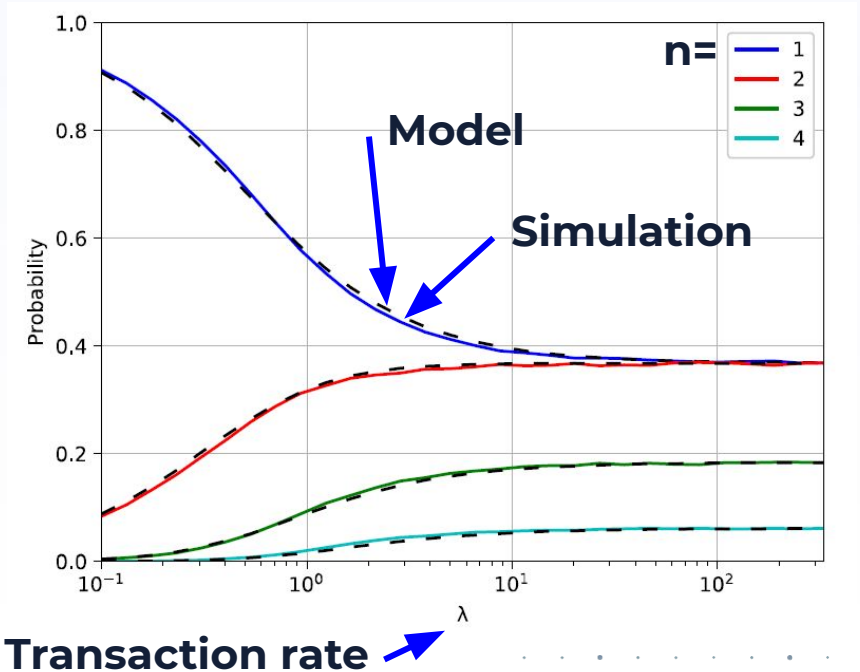
$$N_i = 1 + Pois(\lambda_i)$$

$$\lambda_i = \lambda \int_{t_i}^{t_i+h} dt\ (2p_i(t) - p_i(t)^2)$$

Probability for n approver

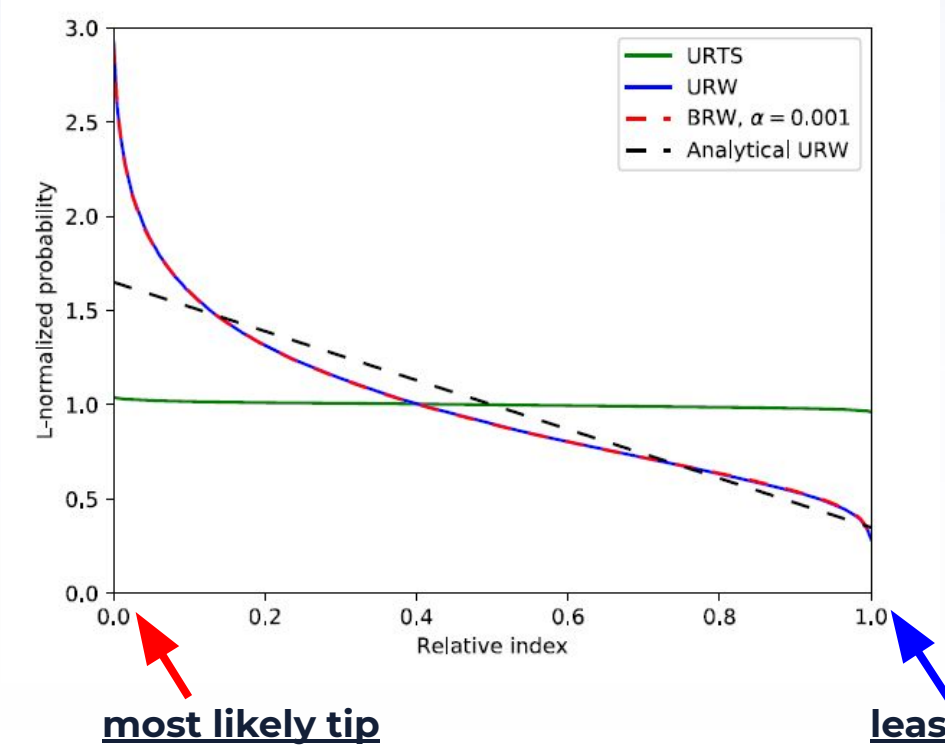
Poisson distribution $P(\lambda_U, n-1)$

$$\lambda_U = 2\lambda L^{-1}(1 - 0.5L^{-1})$$



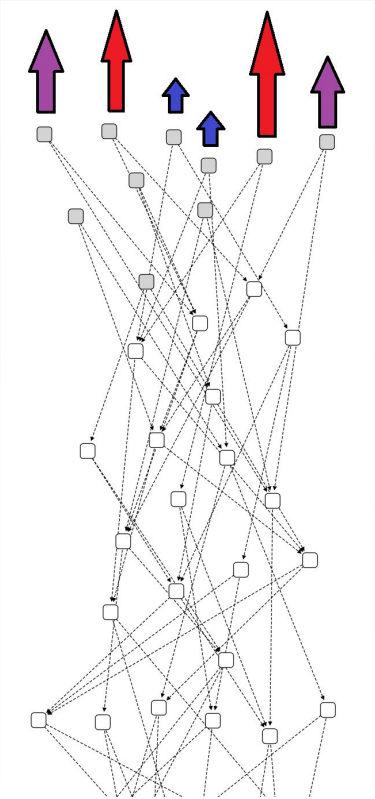
Unbiased Random Walk tip selection Model

Exit probability



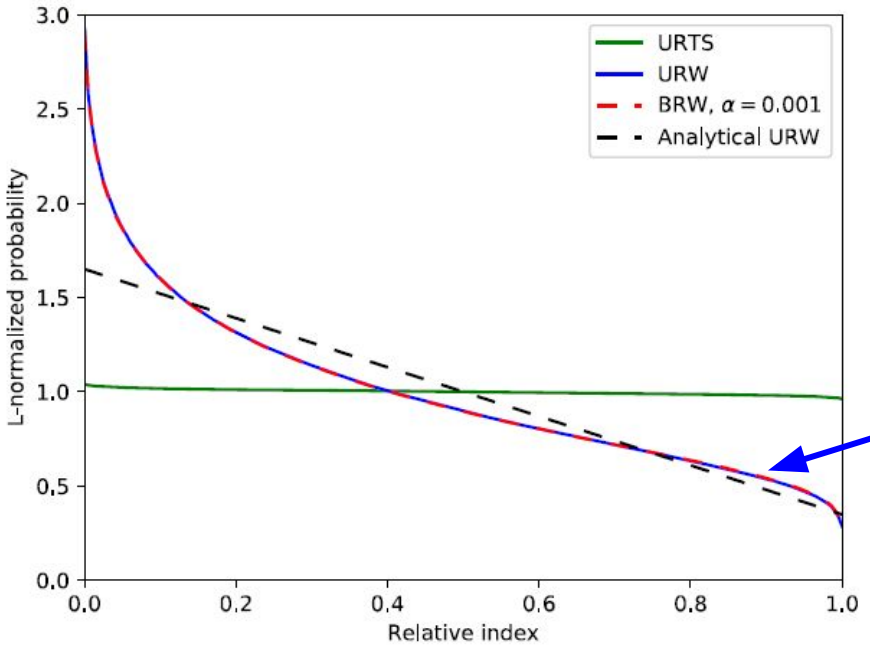
most likely tip

least likely tip



Unbiased Random Walk tip selection
Model

Exit probability



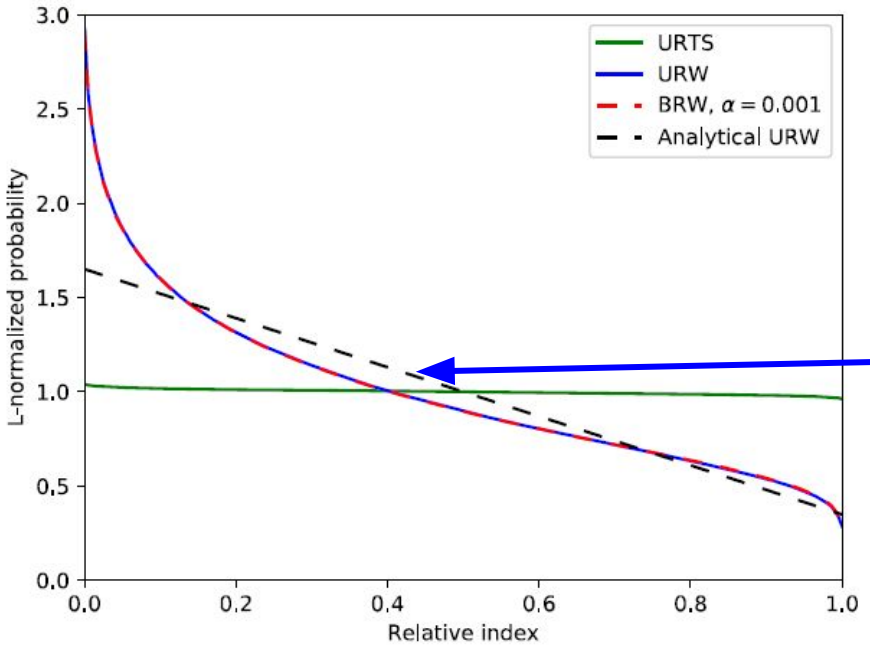
At the time of paper submission :

α = .001
PoW time = 4.1s
Tx rate = 5tps

For this setting the exit probabilities of BRW and URW are almost identical.

Unbiased Random Walk tip selection
Model

Exit probability



Relative index exit probability

$$e(x) = 1 + f(x)$$

Probability to have n approvers
(Integral over relative index space)

$$P_{URW}(n) = P_U(n) \int_0^1 dx\, e^{-f(x)\lambda_U} (1 + f(x))^{n-1}$$

Linear approach

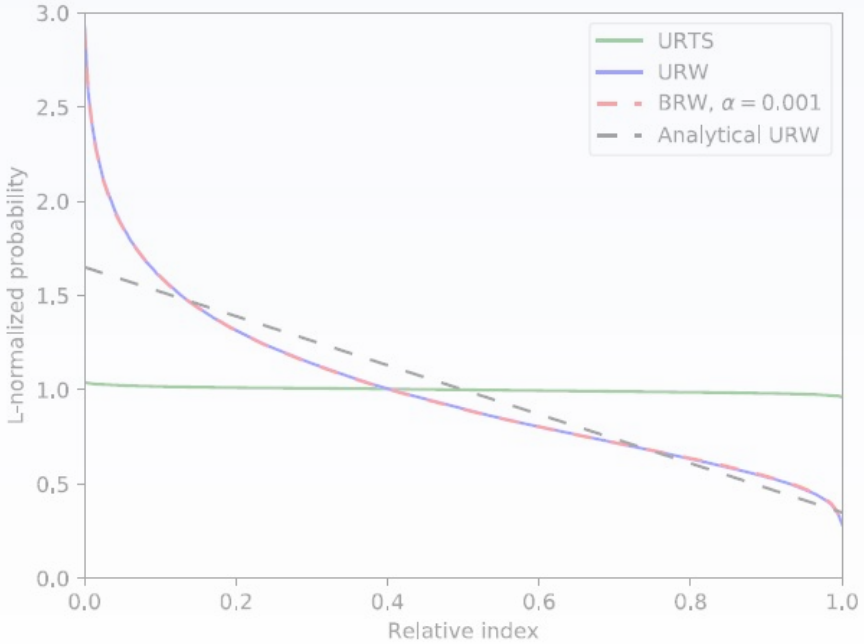
$$P_{URW}(n) = P_U(n) g(n-1)$$

$$g(n) = \frac{1}{a} \sum_{j=0}^{n} \lambda_U^{-j-1} \frac{n!}{(n-j)!} \left[e^{-y\lambda_U} (1+y)^{n-j} \right]_{0.5a}^{-0.5a}$$

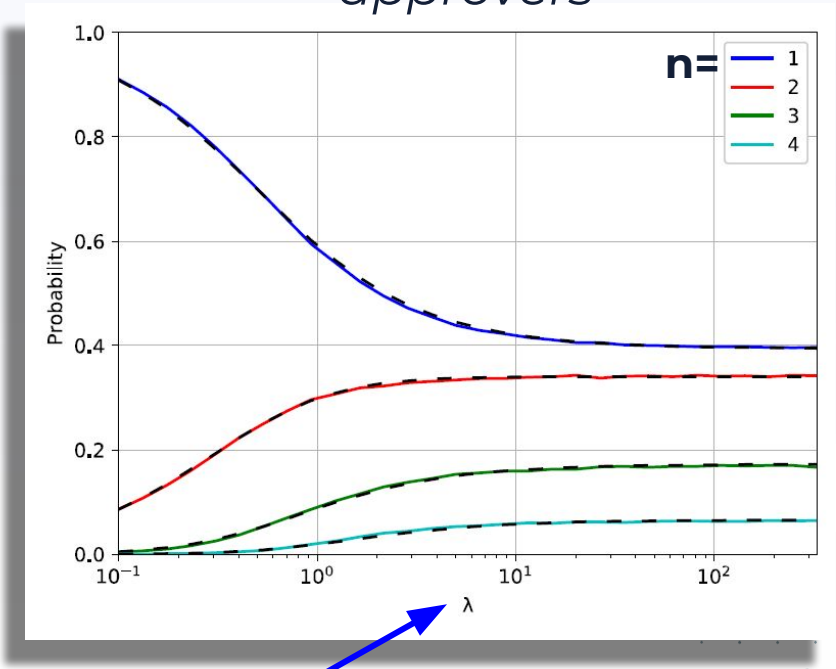
Unbiased Random Walk tip selection

Expected number of approvers

Exit probability

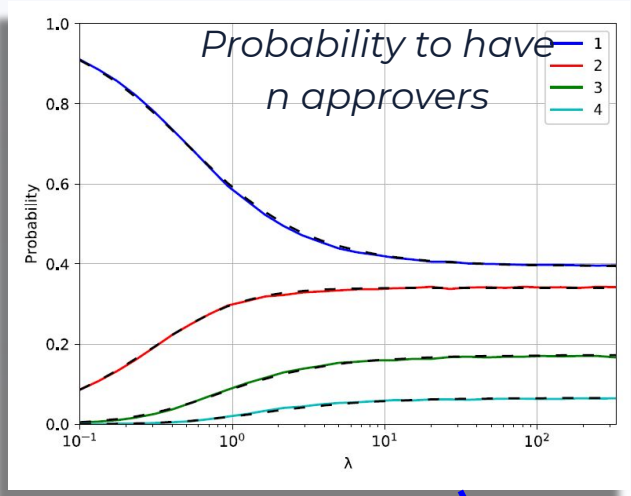


Probability to have n approvers



Transactions rate

Parasite Chain detection

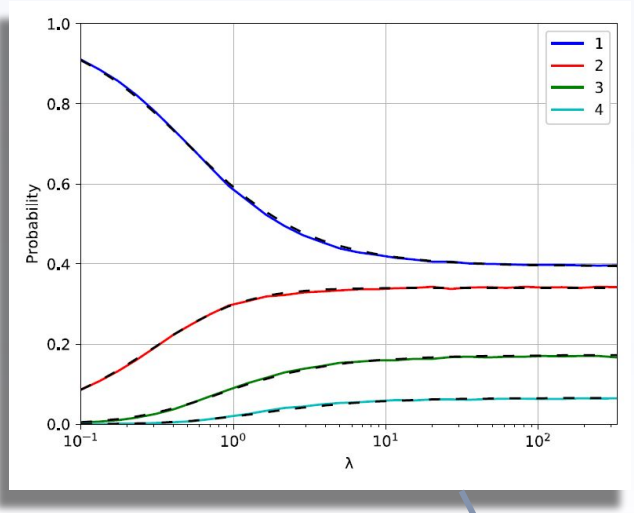


Expected distribution Random Walk

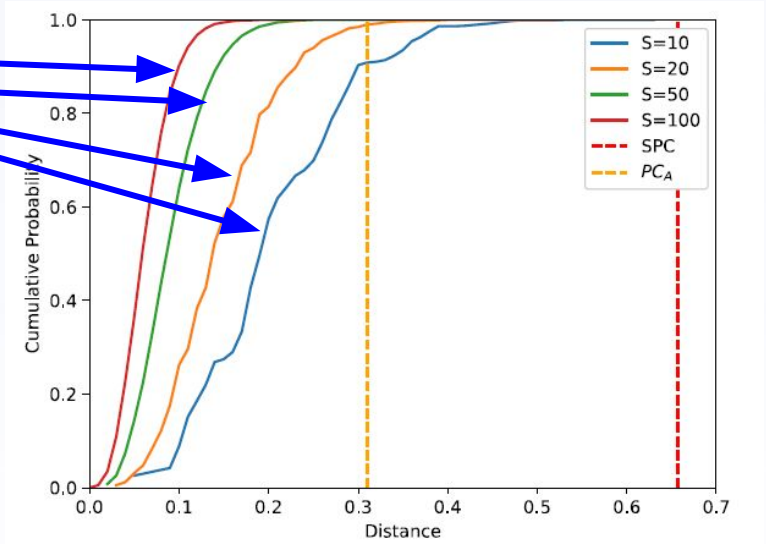
Perform Random Walk sample

$$d_P = \frac{1}{2}\sum_{n=0}^{\infty} |P(n,S) - P_{ref}(n)|$$

Parasite Chain detection



Main Tangle



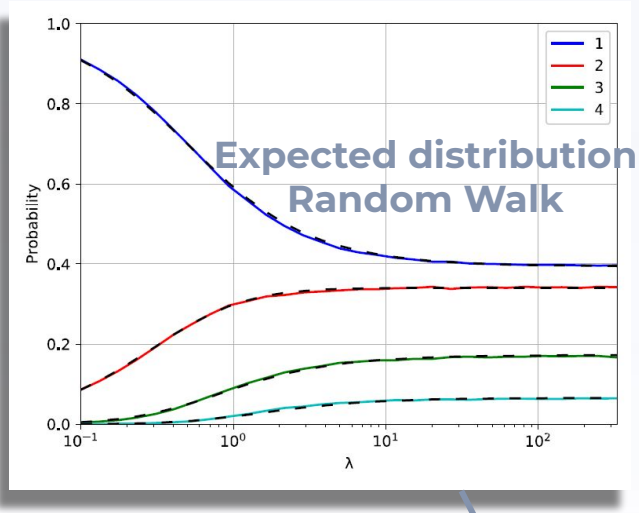
a) Distance metric d_P

Expected distribution
Random Walk

Perform
Random Walk
sample

$$d_P = \frac{1}{2} \sum_{n=0}^{\infty} |P(n, S) - P_{ref}(n)|$$

Parasite Chain detection

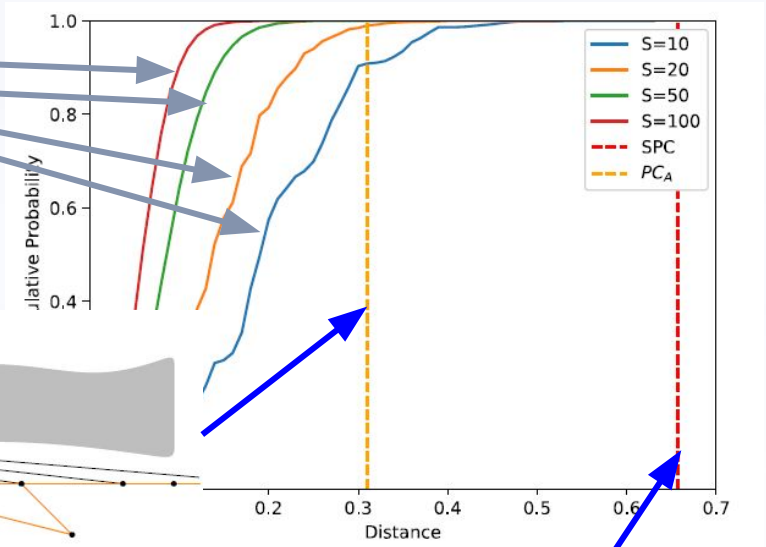


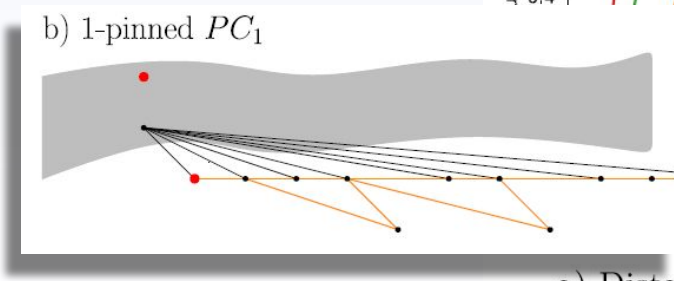
Expected distribution
Random Walk

Perform
Random Walk
sample

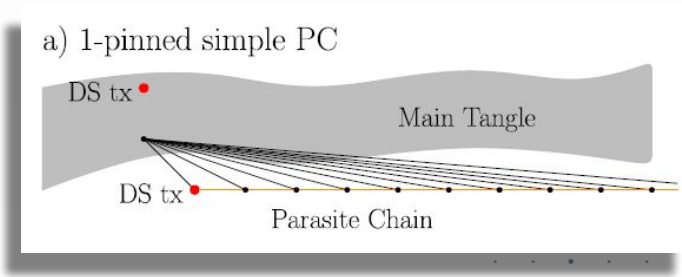
$$d_P = \frac{1}{2}\sum_{n=0}^{\infty} |P(n,S) - P_{ref}(n)|$$

Main Tangle





a) Distance metric d_P



Remarks

- **Counter measures upon successful detection**
  - rerun BRW from start (with increased α),
    e.g. “IOTA-based Directed Acyclic Graphs without Orphans” https://arxiv.org/abs/1901.07302
    by P. Ferraro, C. King, and R. Shorten
  - revert several steps to exit the Parasite Chain,
  - introduce probability to go step backwards
  - etc..

- **Improvements**
  - expensive to build a Parasite Chain with high number of approvers
    ⇒ The difference $|P(n, S) - P_{ref}(n)|$ is larger for higher n
    ⇒ Reward having many approvers, change distance metric $Q(n) = \sum_{m=n}^{\infty} P(m)$
  - Future cone detection :
    - average number of approvers in PC is lower than in main tangle
    - computationally expensive (requires traverse algorithm to collect sample)
    - can e.g. be employed when Parasite Chain is suspected
      (increase confirmation certainty)

IOTA

Parasite Chain Detection
in the IOTA 1.0 Protocol

Thank You!

Andreas Penzkofer
Research Scientist, IOTA Foundation