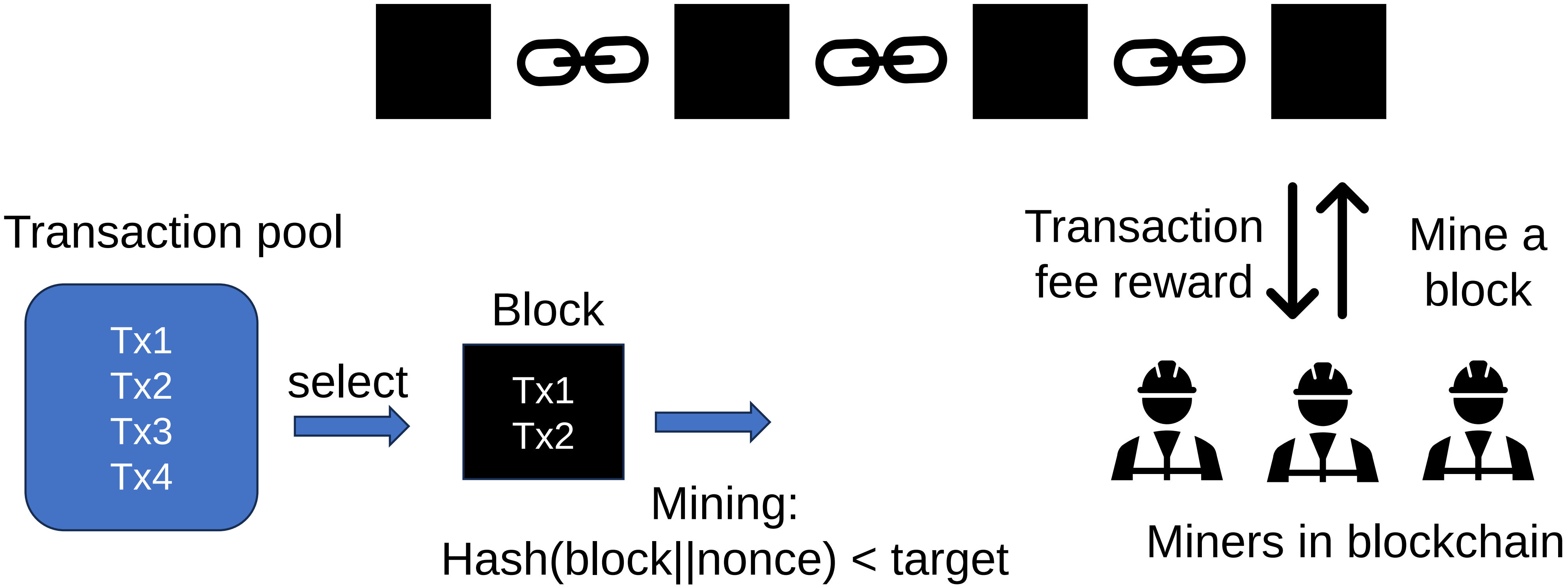
We-TIPS: Weak-Block-Based Transaction Inclusion Protocol with Signaling in DAG-based Blockchain

Canhui Chen and Zhixuan Fang

Institute for Interdisciplinary Information Science,

Tsinghua University

Blockchain System



Transaction pool

Tx1
Tx2
Tx3
Tx4

select

Block

Tx1
Tx2

Mining:
Hash(block||nonce) < target

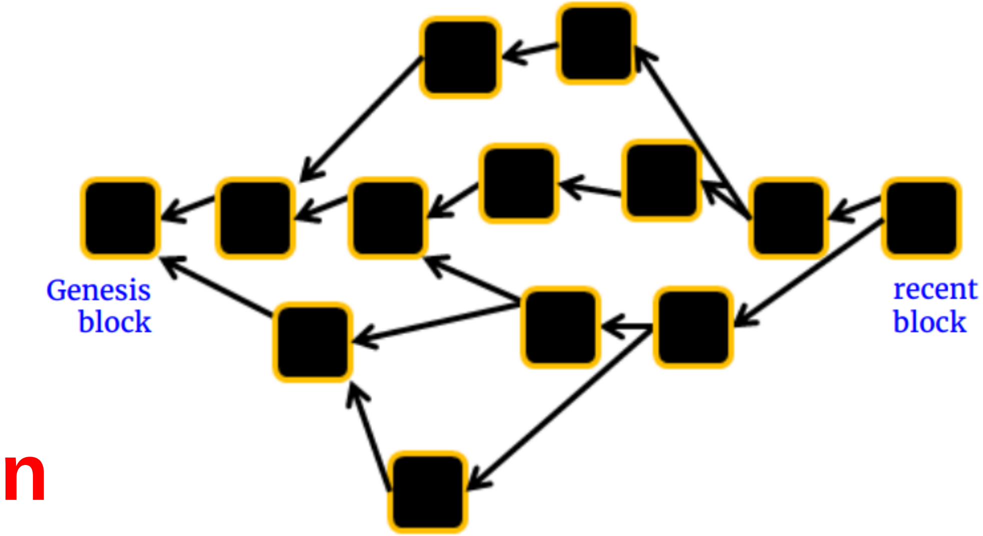
Transaction fee reward

Mine a block

Miners in blockchain

DAG-based Blockchain

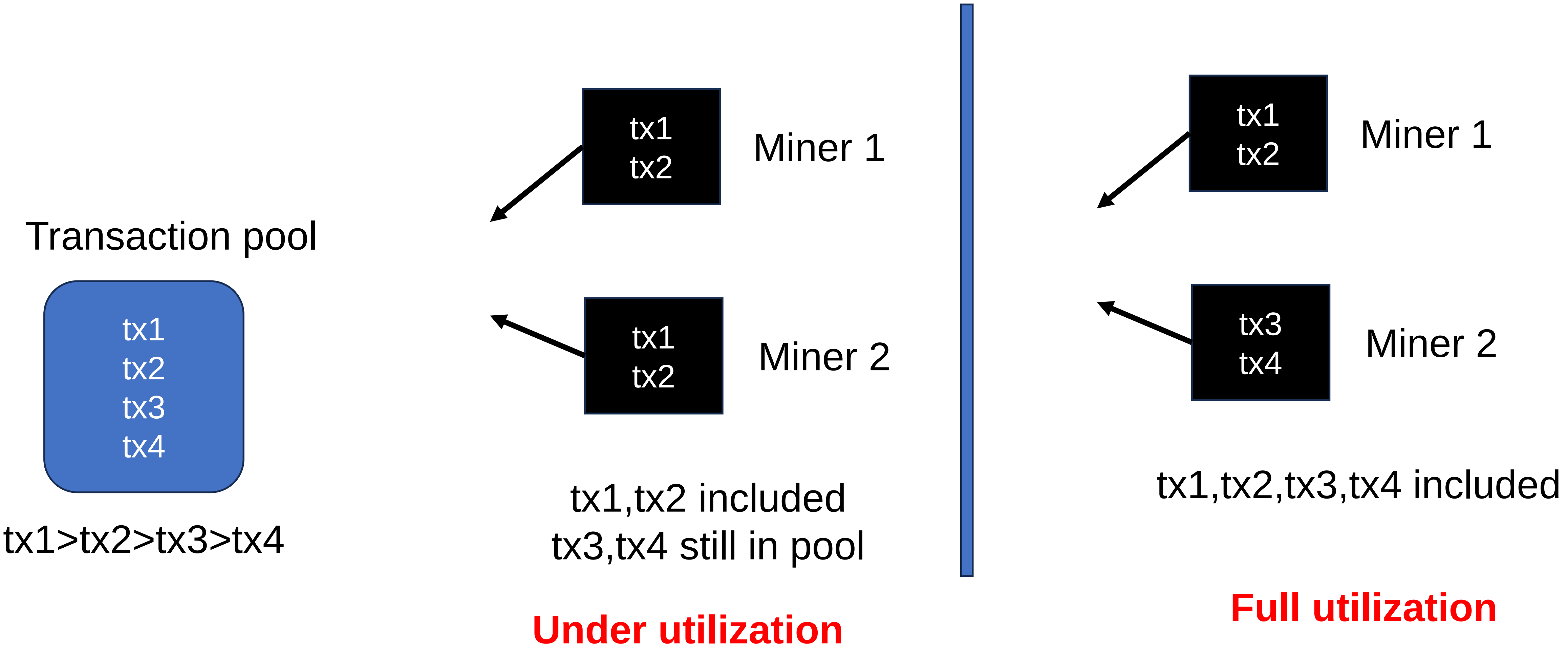
- Directed Acyclic Graph (DAG) structure:
  - Maintain entire graph
  - Consider all blocks
  - High throughput



Key Challenge:
Transaction Inclusion Collision

[1] Lewenberg, Yoad, Yonatan Sompolinsky, and Aviv Zohar. "Inclusive block chain protocols." *Financial Cryptography and Data Security: 19th International Conference, FC 2015.*

Transaction Inclusion Collision in DAG



Transaction pool

tx1
tx2
tx3
tx4

tx1>tx2>tx3>tx4

tx1
tx2

Miner 1

tx1
tx2

Miner 2

tx1,tx2 included
tx3,tx4 still in pool

Under utilization

tx1
tx2

Miner 1

tx3
tx4

Miner 2

tx1,tx2,tx3,tx4 included

Full utilization

Transaction Inclusion Game

Player: miner 1 and miner 2

	Miner 2 chose tx1	**Miner 2 chose tx2**
Miner 1 chose tx1	(0.5*tx1, 0.5*tx1)	(tx1, tx2)
Miner 1 chose tx2	(tx2, tx1)	(0.5*tx2, 0.5*tx2)

Transaction inclusion collision

Equilibrium Strategy

Equilibrium strategy in transaction inclusion game [1]:

- miners are incentivized to avoid selecting the same transactions

Equilibrium Strategy is not enough!

Can only achieve ~70% utilization

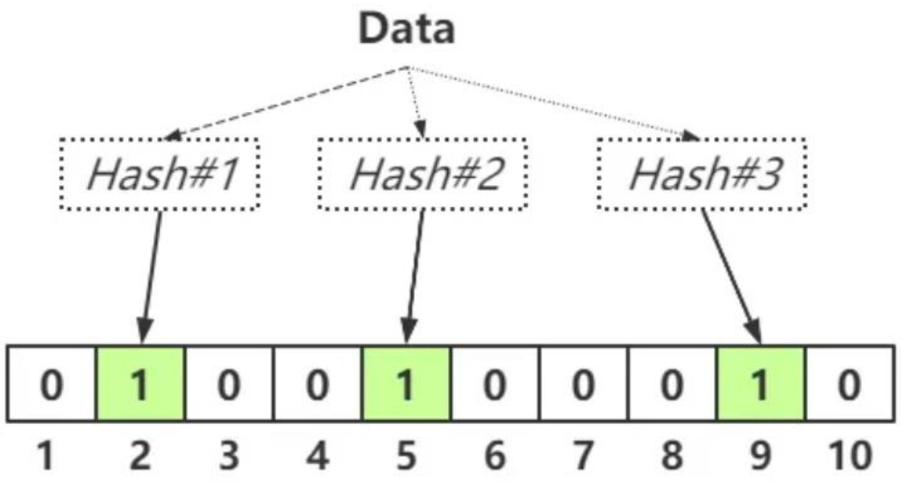
[1] Lewenberg, Yoad, Yonatan Sompolinsky, and Aviv Zohar. "Inclusive block chain protocols." *Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19*. Springer Berlin Heidelberg, 2015.

Signal can help!

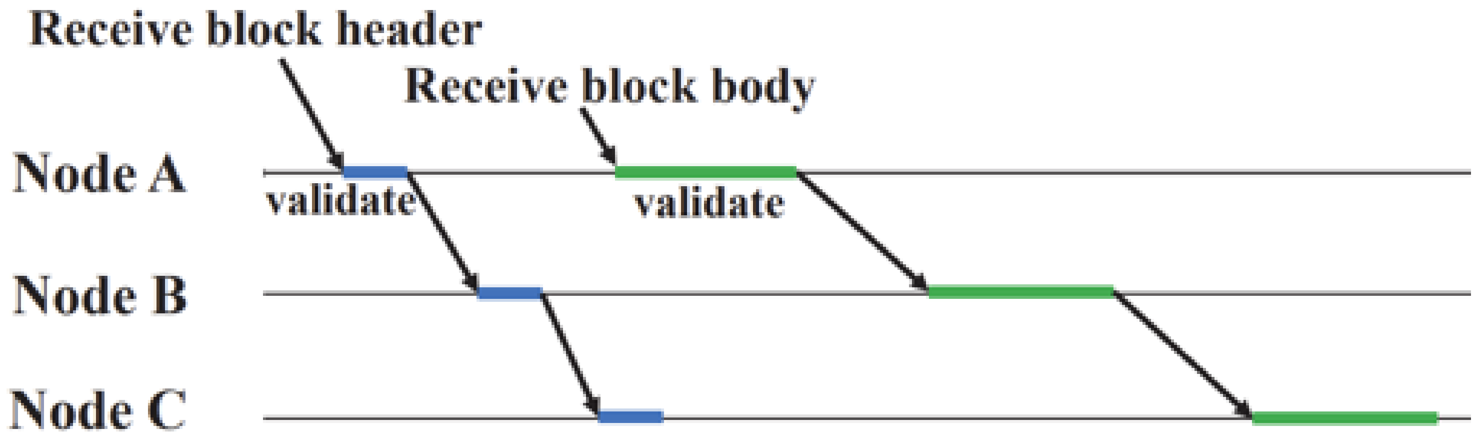
- Why collision?
  - The collision occurs because the miners can not access to the up-to-date information!
  - Waiting for block propagation. (long)
- How to improve?
  - Broadcast a small signal indicating the transaction inclusion in the block.
  - Waiting for signal propagation. (short)

TIPS: Transaction Inclusion Protocol with Signaling

- TIPS introduces a signal to indicate the transactions included in the block using Bloom Filter.
- TIPS broadcast the signal earlier than the whole block.



1	2	3	4	5	6	7	8	9	10
0	1	0	0	1	0	0	0	1	0



[1] Canhui Chen, Xu Chen and Zhixuan Fang, “TIPS: Transaction Inclusion Protocol with Signaling in DAG-Based Blockchain,” IEEE Journal on Selected Areas in Communications (JSAC), volume 40, 2022.

TIPS: Transaction Inclusion Protocol with Signaling

- TIPS introduces a signal to indicate the transactions included in the block using Bloom Filter.
- TIPS broadcast the signal earlier than the whole block.

TIPS can achieve ~90% utilization!
Can we do better?

[1] Canhui Chen, Xu Chen and Zhixuan Fang, “TIPS: Transaction Inclusion Protocol with Signaling in DAG-Based Blockchain,” IEEE Journal on Selected Areas in Communications (JSAC), volume 40, 2022.

Limitation of TIPS & Motivation of We-TIPS

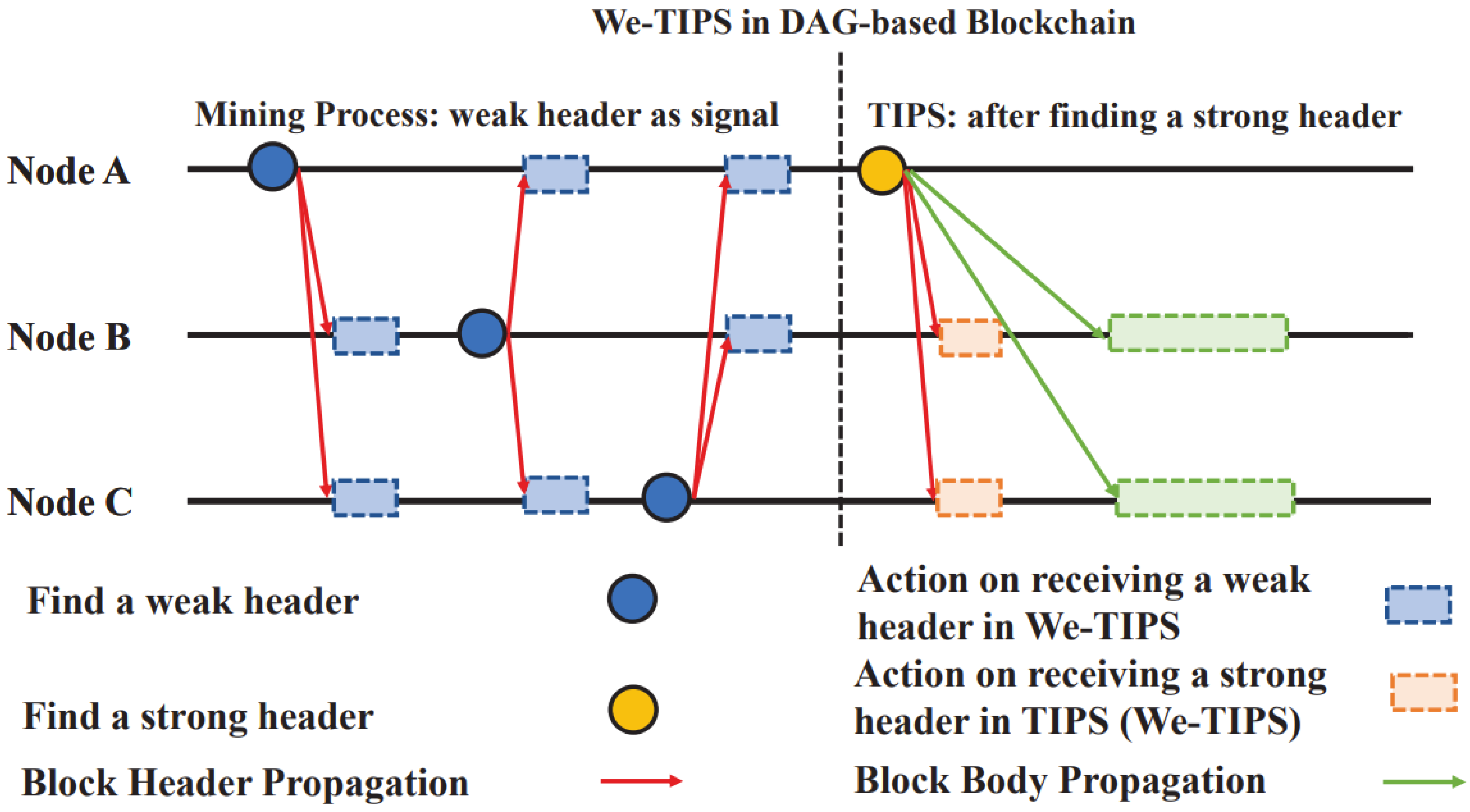
- TIPS only signals other miners when a new block is mined.
- We-TIPS: the weak-block-based transaction inclusion protocol
- We-TIPS can signal the miners during the mining process using weak block header.

Weak Block

- Mining: hash value h of a block header small enough
- Strong target: T_s (corresponds to mining difficulty)
- Strong header: $h < T_s$ (A valid header in PoW)
- Weak target: T_w
- Weak header: $T_s \leq h < T_w$
- Weak block ratio: $\beta = T_w / T_s$
- $\beta = 1$ indicates the scenario without weak blocks, where We-TIPS degenerates to TIPS

- Weak block contains partial PoW => can not be easily forged
- Each strong block => expected β weak blocks

System Model of We-TIPS


We-TIPS in DAG-based Blockchain
Mining Process: weak header as signal
TIPS: after finding a strong header
Node A
Node B
Node C
Find a weak header
Find a strong header
Block Header Propagation
Action on receiving a weak header in We-TIPS
Action on receiving a strong header in TIPS (We-TIPS)
Block Body Propagation

We-TIPS Property

- The weak block would not affect the miner’s reward.
- When the miners are homogeneous, the reward on the specific transaction is only related to the number of miners that select this transaction.

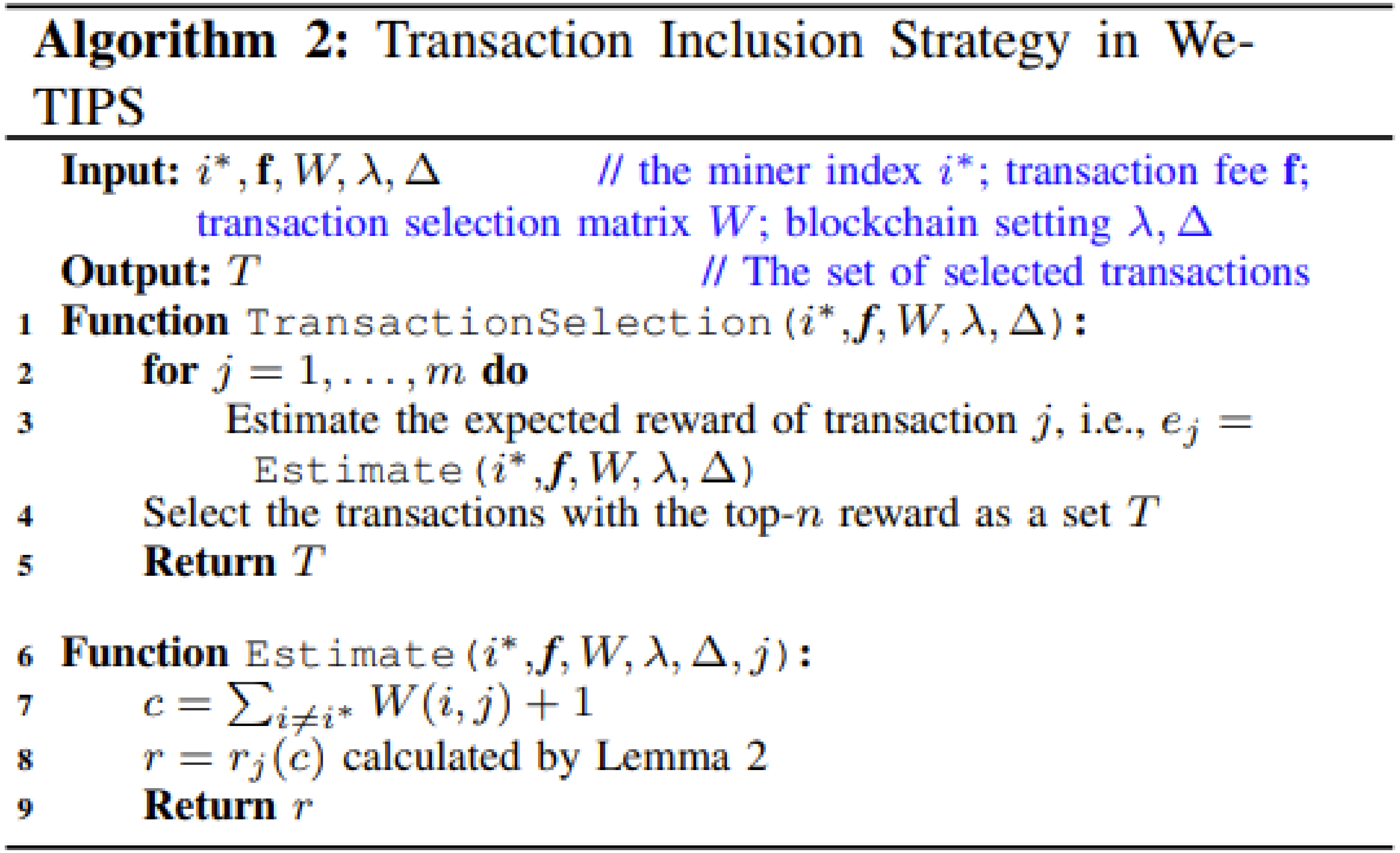
Similar to the Congestion Game / Potential Game

Transaction Inclusion Game in We-TIPS

- **Theorem 1**. *The transaction inclusion game in We-TIPS is a potential game.*

- Potential game => a pure strategy Nash equilibrium

Transaction Inclusion Strategy

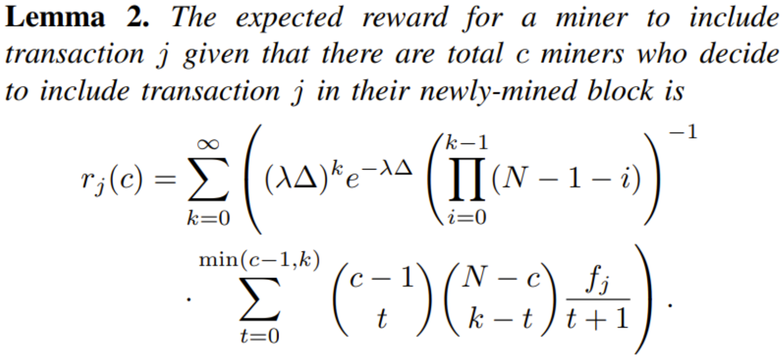


Algorithm 2: Transaction Inclusion Strategy in We-TIPS

```
Input: $i^*$, $\mathbf{f}$, $W$, $\lambda$, $\Delta$        // the miner index $i^*$; transaction fee $\mathbf{f}$;
        transaction selection matrix $W$; blockchain setting $\lambda$, $\Delta$
Output: $T$                                  // The set of selected transactions
Function TransactionSelection($i^*$,$f$, $W$, $\lambda$, $\Delta$):
    for $j = 1, \ldots, m$ do
        Estimate the expected reward of transaction $j$, i.e., $e_j$ =
         Estimate($i^*$,$f$, $W$, $\lambda$, $\Delta$)
    Select the transactions with the top-$n$ reward as a set $T$
    Return $T$

Function Estimate($i^*$,$f$, $W$, $\lambda$, $\Delta$, $j$):
    $c = \sum_{i \neq i^*} W(i, j) + 1$
    $r = r_j(c)$ calculated by Lemma 2
    Return $r$
```

Myopic Strategy in We-TIPS

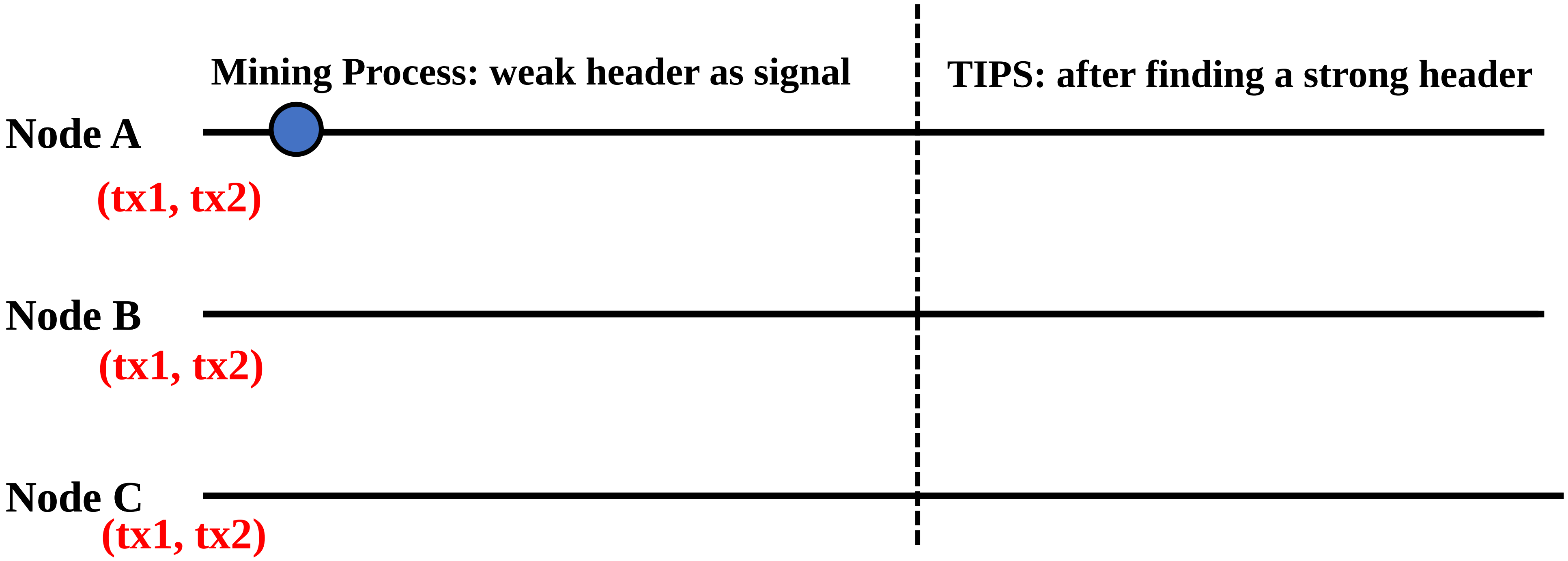


Lemma 2. *The expected reward for a miner to include transaction j given that there are total c miners who decide to include transaction j in their newly-mined block is*

$$r_j(c) = \sum_{k=0}^{\infty} \left((\lambda\Delta)^k e^{-\lambda\Delta} \left(\prod_{i=0}^{k-1} (N-1-i) \right)^{-1} \cdot \sum_{t=0}^{\min(c-1,k)} \binom{c-1}{t} \binom{N-c}{k-t} \frac{f_j}{t+1} \right).$$

Transaction Inclusion Strategy

Transaction pool: tx1>tx2>tx3>tx4>tx5>tx6



Mining Process: weak header as signal

TIPS: after finding a strong header

Node A

(tx1, tx2)

Node B

(tx1, tx2)

Node C

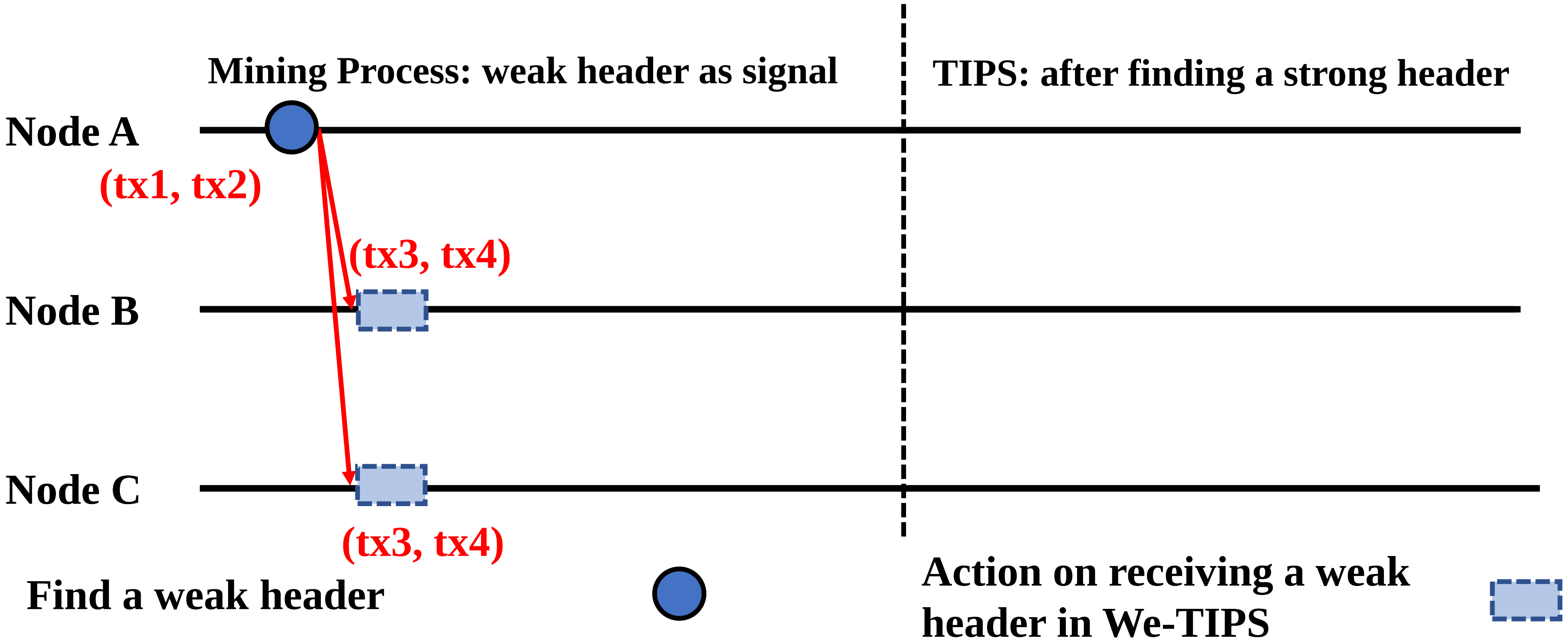
(tx1, tx2)

Find a weak header ●

Action on receiving a weak header in We-TIPS ▨

Transaction Inclusion Strategy

Transaction pool: tx1>tx2>tx3>tx4>tx5>tx6



Mining Process: weak header as signal

TIPS: after finding a strong header

Node A

(tx1, tx2)

(tx3, tx4)

Node B

Node C

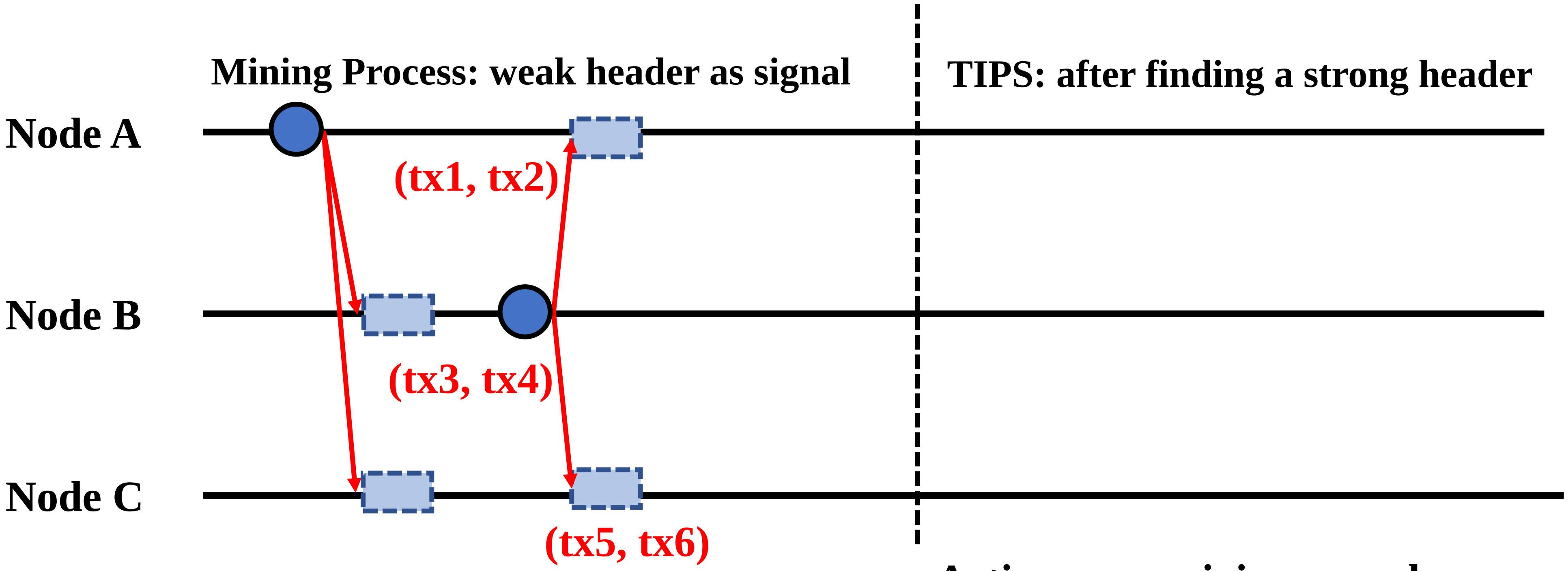
(tx3, tx4)

Find a weak header ●

Action on receiving a weak header in We-TIPS ▭

Transaction Inclusion Strategy

Transaction pool: tx1>tx2>tx3>tx4>tx5>tx6



Mining Process: weak header as signal

TIPS: after finding a strong header

Node A

Node B

Node C

(tx1, tx2)

(tx3, tx4)

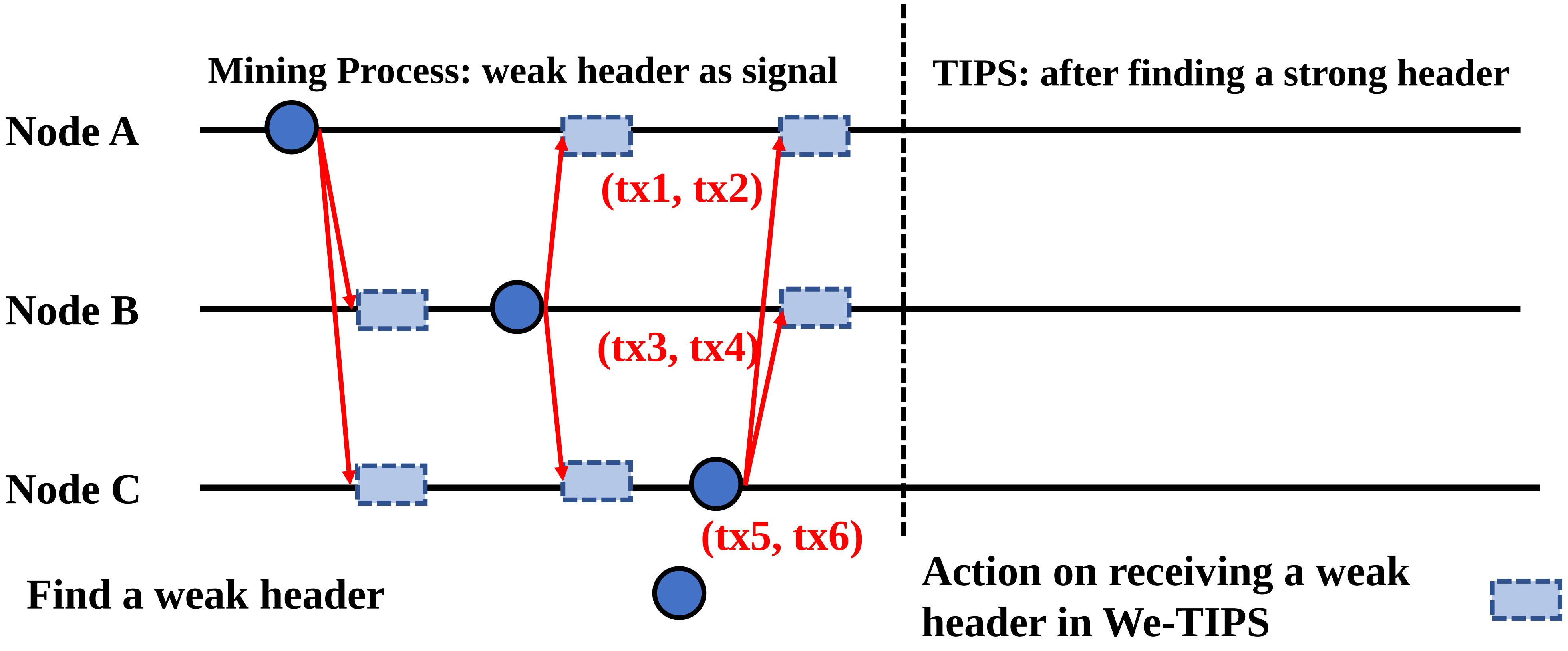
(tx5, tx6)

Find a weak header ●

Action on receiving a weak header in We-TIPS ▨

Transaction Inclusion Strategy

Transaction pool: tx1>tx2>tx3>tx4>tx5>tx6



Mining Process: weak header as signal

TIPS: after finding a strong header

Node A

(tx1, tx2)

Node B

(tx3, tx4)

Node C

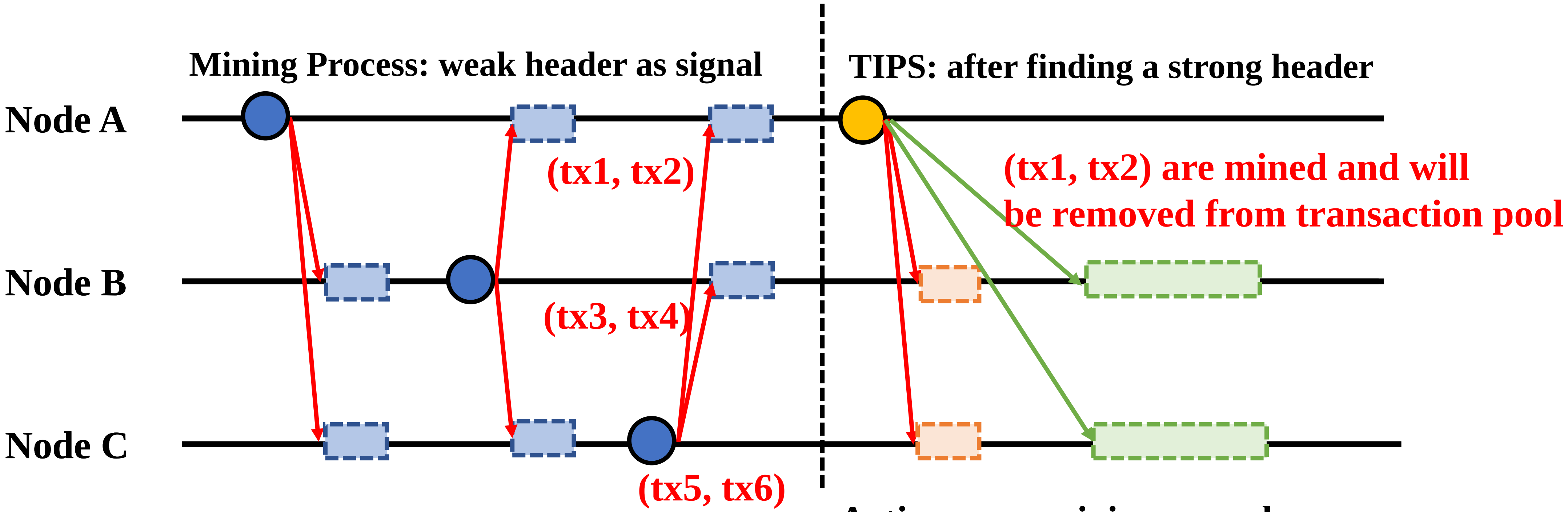
(tx5, tx6)

Find a weak header ●

Action on receiving a weak header in We-TIPS ▨

Transaction Inclusion Strategy

Transaction pool: tx1>tx2>tx3>tx4>tx5>tx6



Mining Process: weak header as signal

TIPS: after finding a strong header

Node A

Node B

Node C

(tx1, tx2)

(tx3, tx4)

(tx5, tx6)

(tx1, tx2) are mined and will be removed from transaction pool

Find a weak header ●

Action on receiving a weak header in We-TIPS ▨

Equilibrium Analysis

- **Theorem 2**. *Algorithm 2 can achieve the η- approximate Nash equilibrium, where*

$$\eta = O\left(\beta^{-1} N^2 \log N \sum_{j=1}^{n} f_j\right)$$

A larger β ⇒
A smaller η

- **Theorem 3**. *When the weak block ratio β is large enough, i.e., $\beta \to \infty$, Algorithm 2 is guaranteed to achieve the pure strategy Nash equilibrium with probability 1.*

Empirical Results of Conflux

- Conflux adopts the random transaction inclusion strategy with transaction fee priority $\frac{p_1}{f_1} = \frac{p_2}{f_2} = \cdots = \frac{p_m}{f_m}$.
- We have collected the blocks in 1000 epochs (from 32289102-th epoch to 32290102-th epoch), which includes 5584 transactions but only 4043 unique transactions
- The block capacity utilization of Conflux is 72.40%
- 27.60% block capacity is wasted due to the transaction inclusion collision.

Experiment

- We conduct the experiment in a DAG-based blockchain simulator with the implementation of the PHANTOM [1]
  - The miners are homogeneous.
  - The size of transaction pool is $m = 10000$, each block can contain at most $n = 2000$ transactions.
  - The propagation delay for the whole block is a random variable following the normal distribution with the expectation as $\Delta = 10$, and the propagation delay for the signal is a random variable following the normal distribution with the expectation as $\tau = 1$.

- [1] Sompolinsky, Yonatan, and Aviv Zohar. "Phantom." *IACR Cryptology ePrint Archive, Report 2018/104* (2018).

Weak Block Ratio Design

- Weak block ratio: $\beta = T_w / T_s$
- $\beta = 1$ indicates the scenario without weak blocks

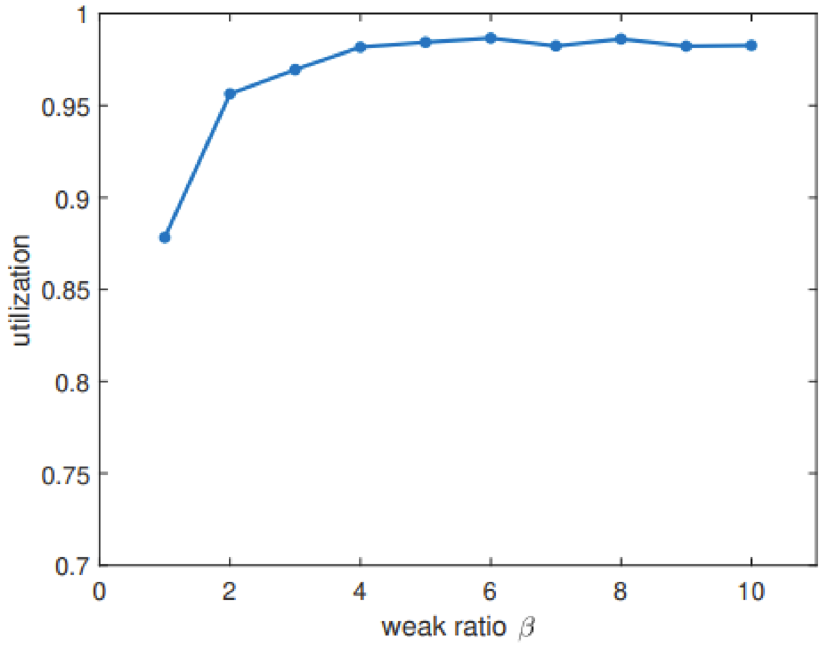


Fig. 2. Utilization of We-TIPS with different ratios β

Performance Results

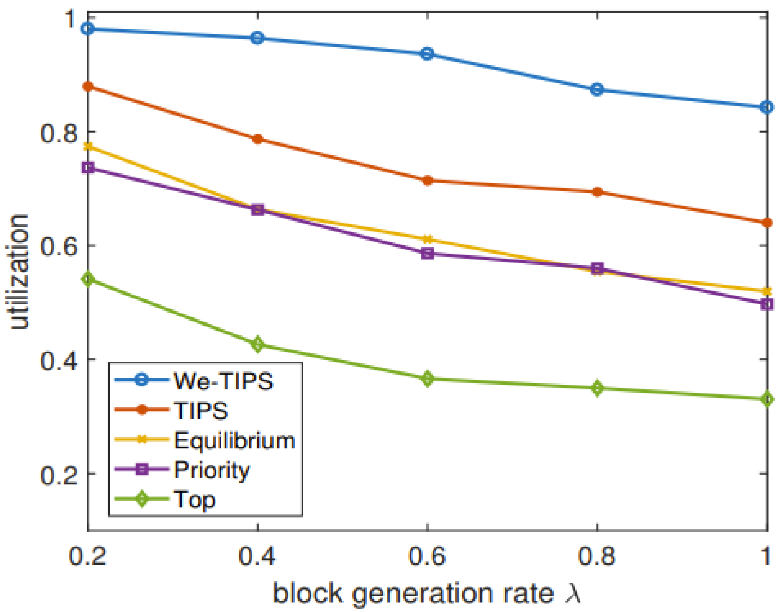


Fig. 3. Utilization of different transaction inclusion protocols

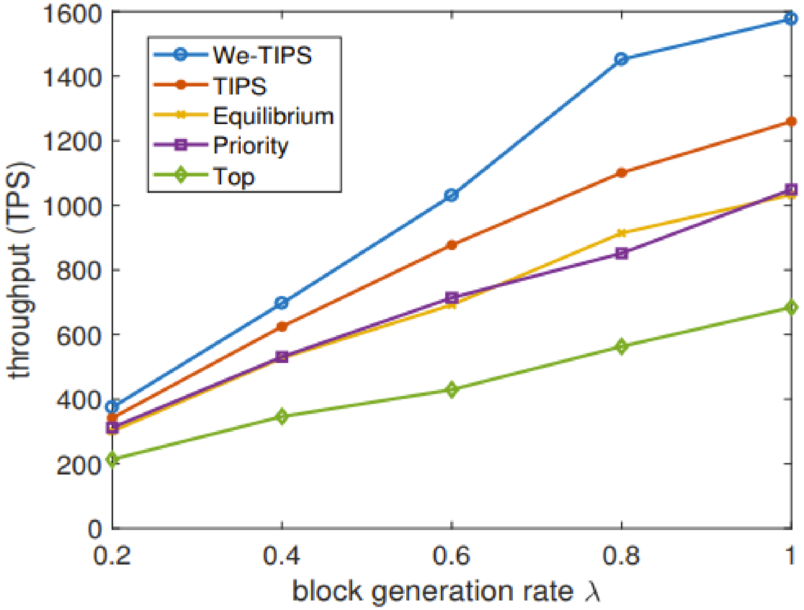


Fig. 4. TPS of different transaction inclusion protocols

Conclusion

- We propose We-TIPS, which allows miners to broadcast their weak headers as signals during the mining process.
- We investigate the transaction inclusion game in We-TIPS, and show that it is a potential game and further propose a decentralized transaction inclusion algorithm.
- We demonstrate the high performance of We-TIPS with intensive experiments.

Thanks~

Canhui Chen

Email: chen-ch21@mails.tsinghua.edu.cn