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

Canhui Chen
Institute for Interdisciplinary Information Science
Tsinghua University
Beijing, China
chen-ch21@mails.tsinghua.edu.cn

Zhixuan Fang
Institute for Interdisciplinary Information Science
Tsinghua University Beijing, China
Shanghai Qi Zhi Institute Shanghai, China
zfang@mail.tsinghua.edu.cn

***Abstract*—DAG-based blockchain faces the key challenge of transaction inclusion collision due to the high concurrency and network delay. In this paper, we propose "We-TIPS", the weak-block-based transaction inclusion protocol with signaling to tackle this key challenge. In We-TIPS, during the mining process, the miner can broadcast their weak block header as a signal, which can indicate the miner's current transaction inclusion. With the prompt broadcast of the signal, the miner can effectively avoid the transaction inclusion collision and thus greatly boost the system performance. Besides, we develop a transaction inclusion game in We-TIPS to model miners' interaction and further show that it is a potential game. We propose a decentralized transaction inclusion algorithm that can achieve the approximate Nash equilibrium. Finally, we conduct intensive experiments to demonstrate the superior performance of the We-TIPS.**

***Index Terms*—blockchain network, performance analysis, game theory**

I. Introduction

The Internet of Things (IoT) and wireless networks are rapidly transforming the way we interact with our environment, leading to a vast and interconnected network of devices, sensors, and services [1], [2]. With the increased connectivity, security, and reliability of these networks, there is a growing need for a distributed and decentralized approach to managing the vast amounts of data generated by IoT devices [3]. This is where blockchain technology comes into play [4]. Blockchain technology has emerged as a potential solution to address the challenges of IoT data management by providing a secure and decentralized platform for data exchange [5]–[7]. However, the traditional blockchain architecture requires the explicit confirmation of each block, which can result in delays and inefficiencies in wireless networks with low bandwidth and high latency. To overcome these limitations, a new type of blockchain architecture has emerged, called the Directed Acyclic Graph (DAG)-based blockchain [8]. The DAG-based blockchain ensures that multiple transactions can be processed simultaneously without the need for globally confirmed, which is important for IoT applications.

While DAG-based blockchains offer many advantages for wireless networks and IoT applications, one of the key challenges they face is transaction inclusion collision [9]. This occurs due to high concurrency and network delays, as miners may not have access to the most up-to-date information about the blockchain, especially in wireless networks with low bandwidth and high latency. As a result, the same transactions may be included in concurrent blocks, leading to redundant records in the blockchain. This collision in transaction inclusion can waste block capacity and severely degrade system performance, posing a significant challenge for the effective implementation of DAG-based blockchains in wireless networks and IoT applications [10].

Faced with this challenge, authors in [11] propose "TIPS", a transaction inclusion protocol with signaling in the DAG-based blockchain. TIPS [11] includes a Bloom filter in the block header which can indicate the included transactions, and broadcast the block header as a signal when a miner successfully mines a new block. Since the size of the signal is small enough, the signal can be broadcast to the whole blockchain network in a short time and effectively help the miners to avoid transaction inclusion and thus significantly improve the system performance. However, we notice that TIPS only signals other miners when a new block is successfully mined, which limits its performance improvement. To address this problem, we propose "We-TIPS", the weak-block-based transaction inclusion protocol with signaling in DAG-based blockchain, which can signal the miners during the mining process to avoid transaction inclusion collision.

Before successfully mining a new block (i.e. finding the solution to the hashing puzzle), the miner may find several weak solutions that do not satisfy the full mining difficulty requirement but also reflect a valid partial proof-of-work (PoW). The block with the weak solution is called "weak block". This is similar to the partial proof-of-work, i.e., "shares" in mining pools [12]. Similar to TIPS [11], we include the Bloom filter into the block header so that a block header can serve as a signal indicating the transactions included in the block. Differently, instead of broadcasting the signal only when a new block is mined, We-TIPS allows the miner to broadcast the weak block header as a signal during the mining process. With the prompt broadcast of the signal in the weak block header, the miner can know other miners' current transaction inclusion strategies, based on which, the miner can adjust his mining strategy to avoid transaction inclusion collision. Besides, to model the miners' interaction in We-TIPS, we develop a transaction inclusion game. We

show that the transaction inclusion game in We-TIPS is a potential game. We further propose a decentralized transaction inclusion algorithm that can achieve the approximate Nash equilibrium. Both the theoretical analysis and experimental validation support the high efficiency of the We-TIPS.

The key contributions of the paper are listed as follows:

- We propose a novel weak-block-based transaction inclusion protocol with signaling (We-TIPS) in the DAG-based blockchain. We-TIPS allows miners to broadcast their weak block header as a signal during the mining process, which can indicate the miners' current transaction inclusion strategies and help the miners to avoid the transaction inclusion.
- We adopt a game-theoretic framework to model the miners' interaction in We-TIPS. We show that the transaction inclusion game in We-TIPS can be modeled as a potential game. Besides, we propose a decentralized transaction inclusion algorithm that can achieve the approximate Nash equilibrium.
- We provide some empirical results of the existing DAG-based blockchain to demonstrate how transaction inclusion collision degrades the system performance in reality. Besides, we develop a DAG-based blockchain simulator and conduct intensive experiments. The experiment results show that We-TIPS can achieve the nearly-optimal performance. Specifically, We-TIPS can achieve more than 98% utilization, while "TIPS" can achieve 90% utilization and the current popular protocol "Conflux" only achieve 72% utilization.

The rest of the paper is organized as follows. In Section II, we introduce the system model of We-TIPS. In Section III, we develop the transaction inclusion game in We-TIPS, and propose a transaction inclusion algorithm to achieve the approximate Nash equilibrium. In Section IV, we conduct intensive experiments to demonstrate the efficiency of We-TIPS. In Section V, we review related literature. Section VI concludes the paper with the final remark.

II. System Model

In this section, we introduce the system model of "We-TIPS", i.e., the weak-block-based transaction inclusion protocol with signaling in the DAG-based blockchain. The key feature of We-TIPS is that the miners in We-TIPS can broadcast the signal using a weak block header indicating their current transaction selection during the mining process, by which the miners can coordinate their transaction inclusion strategies to avoid transaction inclusion collision.

A. Model Overview

Figure 1 demonstrates the system model of We-TIPS. In We-TIPS, during the mining process, each miner may find some weak headers, which is a partial solution to the mining puzzle. There is a Bloom filter [13] in the header, which can indicate the transactions that the miner is currently mining on. Therefore, the weak header can serve as a signal during the mining process. Once a miner finds a weak header, he will broadcast his weak header to other nodes. And when receiving weak headers from other nodes, the miner will adjust his transaction inclusion strategy to avoid transaction inclusion collision. Once a miner successfully solves the mining puzzle (finds a strong header), he will follow the TIPS protocol [11], that is, he will broadcast the strong header first to further avoid transaction inclusion collision.

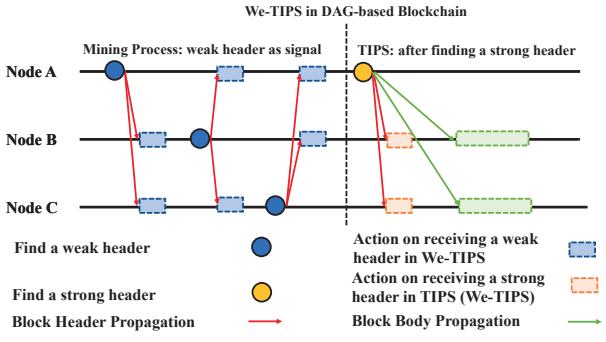

Fig. 1. System model of We-TIPS

B. Block Layout

In the PoW-based blockchain system, every miner tries to solve a PoW puzzle by computing the hash function over a newly created header. The header is constantly being changed by modifying its nonce field, until a valid hash value is found. Consistent with the definitions of [14], we denote the block header that solves the PoW puzzle as a "strong header" with its hash value h smaller than the strong target (mining difficulty) T_s. The "weak header" is a block header whose hash value does not meet the strong target T_s, but still are low enough to prove a significant PoW, i.e. $T_s \leq h < T_w$, where $T_w > T_s$ and T_w is the weak target. For convenience, we denote $\beta = T_w/T_s \geq 1$ as the weak block ratio in We-TIPS, which demonstrates the expected number of weak/strong block headers corresponding to each strong block header. Specially, $\beta = 1$ indicates the scenario without weak blocks, where the proposed We-TIPS degenerates to TIPS [11]. Similar to TIPS [11], we insert the Bloom filter in the block header. A Bloom filter is a space-efficient probabilistic data structure, conceived by Burton Howard Bloom in 1970 [13], which is used to test whether an element is a member of a set. We can consider the block header with the Bloom filter as a signal in our system, where the Bloom filter can indicate the selected transactions in the block. As discussed in TIPS [11], the size of the Bloom filter is small enough so that the block header can be propagated through the whole network in a short time.

C. Mining Process

The mining process is shown in Algorithm 1. During the mining process in We-TIPS, the miners' behaviors of mining and receiving the strong block header and block body are consistent with those in TIPS. And the miner's behaviors on weak block headers are summarized as follows:

- When a miner finds a weak block header, it only needs to broadcast the weak block header.

Algorithm 1: Mining process in We-TIPS

```
on MineBlock:
    for nonce ∈ {0, 1, 2, ···} do
        header ← createHeader(nonce)
        hash ← H(header)
        if hash < T_s then
            // strong header
            broadcast(header)
            broadcast(body)
            return
        end
        if hash < T_w then
            // weak header
            broadcast(header)
        end
    end

on ReceiveBlockHeader⟨header⟩
    hash ← H(header)
    assert(validHeader(header) and hash < T_w)
    BF ← getBloomFilter(header)
    // Select the transactions hitting BF from transaction pool
    TX ← getTransactionSet(BF, txpool)
    if hash < T_s then
        // strong header
        Update transaction pool based on TIPS [11]
    end
    if hash < T_w then
        // weak header
        Update the selecting transactions based on Algorithm 2
    end

on ReceiveBlockBody⟨body⟩
    header ← getBlockHeader(body)
    hash ← H(header)
    // We only handle the block body with strong header
    assert(validBody(body) and hash < T_s)
    Update transaction pool based on TIPS [11]
```

- When a miner receives a weak block header, it needs to check the validation of the weak block header. If the weak block header is valid, the miner will update his transaction inclusion strategy to avoid transaction inclusion collision, which will be discussed in Section III.

Note that the weak block header does not change the consensus protocol in the DAG-based blockchain system. Thus We-TIPS can be used as an "add-on" component, and can be applied to most of the current DAG-based blockchain protocols.

D. Security Discussion

We consider the following two possible security threats in We-TIPS, and show that We-TIPS can maintain system security in long term.

- **No-broadcasting the weak block header**: In We-TIPS, miners are not forced to broadcast the newly-mined weak block header. However, broadcasting the newly-mined weak block header can avoid other miners from selecting the same transaction set, and thus improve the mining revenue. No-broadcasting the weak block header does not affect the system consensus, but will degrade the miner's revenue. Therefore, a rational miner will always broadcast his weak block header.
- **Constructing the misleading weak block header**: A miner can construct a misleading weak block header that does not include the transactions he wants to mine. However, each weak block header contains a partial PoW, and the effort of constructing a misleading signal is at least equal to that of honest mining. Therefore, it is not profitable for a miner to construct a misleading signal.

III. Transaction Inclusion Strategy

In this section, we investigate the miners' transaction inclusion strategies in We-TIPS. We first show that the miners' interactions can be modeled as a multi-agent Markov decision process (MMDP). To model the miner's rationality, we investigate the miner's transaction inclusion strategy from a game-theoretical perspective. We show that the transaction inclusion game in We-TIPS is a potential game and further propose a transaction inclusion algorithm that can achieve the approximate Nash equilibrium with a good system performance.

A. Blockchain Modeling

We consider a DAG-based blockchain system with N miners, where the block generation process follows the Poisson process with a rate λ. We denote the effective network propagation delay as Δ. Each miner maintains a transaction pool containing at most m transactions. Due to the block size limit, each block can contain at most n transactions. Without loss of generality, we assume that the transactions in the memory pool are sorted in descending order by their transaction fees, and the transaction fee of the transaction i is denoted as f_i. Each miner is rational and will choose his transaction inclusion strategy to maximize his utility, which forms a transaction inclusion game in We-TIPS.

B. Miners' Behaviors Modeling

Since the block generation process follows the Poisson process, which satisfies the memorylessness property, the miners' behavior can be modeled as a multi-agent Markov decision process (MMDP).

1) Multi-agent Markov Decision Process: The multi-agent Markov decision process (MMDP) of the mining process can be represented as a tuple $< \mathcal{N}, \mathcal{S}, (A_i)_{i\in\mathcal{N}}, P, (R_i)_{i\in\mathcal{N}} >$, where $\mathcal{N}$ denotes the set of N miners in the DAG-based blockchain system, with x_i denoting the hash rate of miner i and $\mathbf{x} = [x_1, \ldots, x_N]$ denoting the normalized hash rate vector, i.e., $\sum_{i=1}^{N} x_i = 1, x_i \in [0, 1]$; $\mathcal{S}$ is a set of states, each state $s \in \mathcal{S}$ can be represented as a tuple $< \mathbf{f}, W, \mathbf{b} >$, where $\mathbf{f} \in \mathbb{R}^{1\times m}$ denotes the transaction fees of m transactions in the memory pool, and $W \in \mathbb{R}^{N\times m}$ is a matrix denoting the miners' transaction selections in their previous weak headers. Specially, $W(i, j) = 1$ denotes that the latest weak header mined by miner i contains transaction j [1], otherwise $W(i, j) = 0$. The symbol $\mathbf{b} \in \mathbb{R}^{N\times 1}$ denotes the mining results. $b_i = 1$ implies that the miner i successfully solves the PoW puzzle, i.e., finds the strong block header. Otherwise $b_i = 0$. The symbol $A_i \in \mathbb{R}^{1\times m}$ denotes the action of miner i. Specially, $A_{i,j} = 1$ implies that the miner i includes the

[1]When we say the block header contains transaction j, it implies that the transaction j hits the Bloom Filter in the block header.

transaction j in a block and mines on that. Otherwise, we have $A_{i,j} = 0$. Since there are at most n transactions in a block, we have $||A_i||_1 = \left(\sum_{j=1}^{m} A_{i,j}\right) \leq n, \forall i \in \mathcal{N}$, where $||\cdot||_1$ is the Manhattan norm of a vector. Typically, we consider the case when $||A_i||_1 = n, \forall i \in \mathcal{N}$. Furthermore, the joint actions of miners can be represented as $A = A_1 \times \ldots \times A_N \in \mathbb{R}^{N \times m}$. $R_i(s, A)$ is the reward of miner i at state s with the joint actions A. P is the probability transition function that describes state transition, conditioned on the past states s and joint actions A. This game satisfies the Markov property due to the memorylessness of the mining process, i.e., $P[s_{t+1}|s_t, A_t, \ldots, s_0, a_0] = P[s_{t+1}|s_t, A_t]$.

2) Reward: Since the coinbase transaction reward is independent of the miner's transaction selection, for simplicity, we only consider the transaction fee reward in the miner's revenue. And the miner can obtain the transaction fee reward only when he successfully mines a strong block. Thus, the weak block header in We-TIPS only serves as a signal, and miners cannot get any reward from mining a weak block header. Besides, if there exist ι miners who have successfully mined a strong block with the same transaction i during the network propagation period Δ, we assume that the expected reward for any one of these miners on the transaction i is f_i/ι, i.e., assuming an equal network advantage for all miners. Note that such a model of probabilistic and homogeneous network advantage during the propagation period is common in the previous study (e.g., [9], [15]).

3) State Transition: We consider the state that at least one of the miners successfully solves the PoW puzzle and finds the strong block header as the final state, i.e., $s^* =< \mathbf{f}, W, \mathbf{b} >$ where $\mathbf{b} \neq \vec{\mathbf{0}}$ is a final state. The game ends at the final states without any further state transitions and will restart at the next step. We call the other states with $\mathbf{b} = \vec{\mathbf{0}}$ as processing states. With $\beta = T_w/T_s$ denoting the difficulty ratio of mining a strong block and weak block, the probability of transition from the processing states to the final states is $1/\beta$, and the probability of transition from the processing states to other processing states is $1 - 1/\beta$. Specially, the probability of miner i mining a weak header, and the state transfer from the processing state $s =< \mathbf{f}, W, \vec{\mathbf{0}} >$ to the processing state $s^{(i)} =< \mathbf{f}, W^{(i)}, \vec{\mathbf{0}} >$ is

$$P\left(< \mathbf{f}, W^{(i)}, \vec{\mathbf{0}} > | < \mathbf{f}, W, \vec{\mathbf{0}} >, A\right) = \left(1 - \frac{1}{\beta}\right) x_i,$$

where

$$W^{(i)}(j,k) = \begin{cases} W(j,k), & j \neq i, \\ A(i,k), & j = i. \end{cases}$$

The probability that at least one of the miners solves the PoW puzzle and mines a strong block, and the state transfer from the processing state $s =< \mathbf{f}, W, \vec{\mathbf{0}} >$ to the final state $s^* =< \mathbf{f}, W, \mathbf{b} >$ is formulated in the following lemma:

Lemma 1. *The probability that the state transfers from the processing state $s =< \boldsymbol{f}, W, \vec{\boldsymbol{0}} >$ to the final state $s^* =< \boldsymbol{f}, W, \boldsymbol{b} >$ is*

$$P\left(s^*|s, A\right) = \frac{1}{\beta}\left(\frac{(\lambda\Delta)^{||\boldsymbol{b}||_1 - 1}}{(||\boldsymbol{b}||_1 - 1)!} e^{-\lambda\Delta}\right) \sum_{\pi \in \mathcal{P}^{\mathcal{K}}} \prod_{i=1}^{|\mathcal{K}|} \frac{x_{k_{\pi(i)}}}{1 - \sum_{j=1}^{i-1} x_{k_{\pi_j}}},$$

where $\mathcal{K} = \{i | b_i = 1\}$ denotes the set of miners who generates a new block at the final state s^*.

Proof. At the final state $s^* =< \mathbf{f}, W, \mathbf{b} >$, there are $||\mathbf{b}||_1$ blocks generated in the blockchain system. Then $(||\mathbf{b}||_1 - 1)$ blocks are generated during the block propagation time Δ. Since the block generation process follows the Poisson process with a rate λ, the probability that $(||\mathbf{b}||_1 - 1)$ blocks are generated during the block propagation time Δ is $\frac{(\lambda\Delta)^{||\mathbf{b}||_1 - 1}}{(||\mathbf{b}||_1 - 1)!} e^{-\lambda\Delta}$. Denote the set $\mathcal{K} = \{i | b_i = 1\}$ as the set of miners who generates a new block at the final state s^*, and we have $|\mathcal{K}| = ||\mathbf{b}||_1$ and $\mathcal{K} \subset \mathcal{N}$. Then the problem of calculating the probability that the miners in $\mathcal{K}$ mine new blocks given the condition that $|\mathcal{K}|$ blocks will be generated is equivalent to the sampling problem with varying probability without replacement [16], where the normalized miners' hash rates $\mathbf{x}$ corresponds to their weights. Let $\mathcal{P}^{\mathcal{K}}$ denote the set of all permutations of the elements of $\mathcal{K}$. Then the probability that the miners in $\mathcal{K}$ mine new blocks given the condition that $|\mathcal{K}|$ blocks will be generated is

$$\Pr(\mathcal{K}) = \sum_{\pi \in \mathcal{P}^{\mathcal{K}}} \prod_{i=1}^{|\mathcal{K}|} \frac{x_{k_{\pi(i)}}}{1 - \sum_{j=1}^{i-1} x_{k_{\pi_j}}}. \tag{1}$$

Since the probability of transition from the processing states to the final states is $1/\beta$, the probability that the state transfer from the processing state $s =< \mathbf{f}, W, \vec{\mathbf{0}} >$ to the final state $s^* =< \mathbf{f}, W, \mathbf{b} >$ is

$$P\left(s^*|s, A\right) = \frac{1}{\beta}\left(\frac{(\lambda\Delta)^{||\mathbf{b}||_1 - 1}}{(||\mathbf{b}||_1 - 1)!} e^{-\lambda\Delta}\right) \sum_{\pi \in \mathcal{P}^{\mathcal{K}}} \prod_{i=1}^{|\mathcal{K}|} \frac{x_{k_{\pi(i)}}}{1 - \sum_{j=1}^{i-1} x_{k_{\pi_j}}}.$$

The proof is thus completed. □

C. Game Analysis

For simplicity, in the following discussion, we assume that the miners are homogeneous to enable tractable analysis. We further show that the transaction inclusion game in We-TIPS is a potential game.

When the miners are homogeneous, we know that the expected reward for a miner to include a certain transaction depends on the number of miners who also select the same transaction, which is formulated in the following lemma.

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*

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

Proof. Denote the set $\mathcal{K}$ as the set of miners (except itself) who generates a new block during the block propagation time Δ. Since the block generation process follows the Poisson process with a rate λ, the probability that k blocks are generated during the block propagation time Δ is

$$\Pr(|\mathcal{K}| = k) = \frac{(\lambda\Delta)^k}{k!} e^{-\lambda\Delta}.$$

Then the probability that the miners in $\mathcal{K}$ mine new blocks given the condition that $|\mathcal{K}|$ blocks will be generated can be calculated using equation (1). As miners are homogeneous, they have the same hash rate, i.e., $x_i = 1/N, \forall i \in \mathcal{N}$. Then equation (1) can be simplified as

$$\Pr(\mathcal{K} \mid |\mathcal{K}| = k) = k! \left(\prod_{i=0}^{k-1} (N-1-i) \right)^{-1}.$$

Denote the set $\mathcal{C}$ as the set of miners (except itself) who decide to include transaction j in their newly-mined block, then we have $|\mathcal{C}| = c - 1$ and $\mathcal{C} \subset \mathcal{N}$. Therefore, at the final state s^*, there will be $|\mathcal{K} \cap \mathcal{C}|$ miners who include transaction j in their newly-mined block. Then the expected reward for these miners on transaction j is $f_j / (|\mathcal{K} \cap \mathcal{C}| + 1)$. Let $t = |\mathcal{K} \cap \mathcal{C}|$, then the number of combinations that leads to the expected reward of $f_j / (t+1)$ is

$$\begin{aligned} \#\text{Comb}(t) &= \binom{|\mathcal{C}|}{|\mathcal{K} \cap \mathcal{C}|} \cdot \binom{|\mathcal{N} - \mathcal{C}| - 1}{|\mathcal{K}| - |\mathcal{K} \cap \mathcal{C}|} \\ &= \binom{c-1}{t} \cdot \binom{N-c}{k-t} \end{aligned} \tag{2}$$

Therefore, the expected reward for a miner to include transaction j given that there are total k miners who decide to include transaction j in their newly-mined block is

$$\begin{aligned} r_j(c) &= \sum_{k=0}^{\infty} \left(\Pr(|\mathcal{K}| = k) \cdot \Pr(\mathcal{K}) \cdot \sum_{t=0}^{\min(c-1,k)} \#\text{Comb}(t) \right) \\ &= \sum_{k=0}^{\infty} \left(\frac{(\lambda\Delta)^k}{k!} e^{-\lambda\Delta} \cdot k! \left(\prod_{i=1}^{k-1} (N-1-i) \right)^{-1} \right. \\ &\quad \left. \cdot \sum_{t=0}^{\min(c-1,k)} \binom{c-1}{t} \binom{N-c}{k-t} \frac{f_j}{t+1} \right). \end{aligned}$$

The proof is thus completed. □

With the expected reward analysis, we can further show that the transaction inclusion game in We-TIPS is a potential game.

Theorem 1. *The transaction inclusion game in We-TIPS is a potential game, where the utility for the miner i with joint action A is*

$$u_i(A) = \sum_{j \in \{k | A_{i,k} = 1\}} r_j(c_j(A)),$$

where $c_j(A)$ denotes the number of miners including the transaction j given the joint action A, and $r_j(c)$ denotes the expected reward on transaction j given that there are totally c miners selecting the transaction j, which is formulated in Lemma 2, and the potential function is

$$\Phi(A) = \sum_{j=1}^{m} \sum_{k=1}^{c_j(A)} r_j(k),$$

where m is the number of transactions in the transaction pool.

Proof. Consider the case where a single miner changes its strategy from A_i to B_i. Let Δu_i be the change in its cost caused by the change in strategy, then we have

$$\begin{aligned} \Delta u_i &= u_i(B_i, A_{-i}) - u_i(A_i, A_{-i}) \\ &= \sum_{j \in \{k | B_{i,k} = 1 \wedge A_{i,k} = 0\}} r_j(c_j(A) + 1) - \sum_{j \in \{k | B_{i,k} = 0 \wedge A_{i,k} = 1\}} r_j(c_j(A)) \end{aligned}$$

Let $\Delta\Phi$ be the change in the potential caused by the change in strategy, then we have

$$\begin{aligned} \Delta\Phi &= \Phi(B_i, A_{-i}) - \Phi(A_i, A_{-i}) \\ &= \sum_{j \in \{k | B_{i,k} = 1 \wedge A_{i,k} = 0\}} r_j(c_j(A) + 1) - \sum_{j \in \{k | B_{i,k} = 0 \wedge A_{i,k} = 1\}} r_j(c_j(A)) \end{aligned}$$

Thus we can conclude that $\Delta u_i = \Delta\Phi$. And thus the transaction inclusion game in We-TIPS is a potential game. The proof is thus completed. □

Since the transaction inclusion game in We-TIPS is a potential game, it always has a pure strategy Nash equilibrium and the finite improvement property [17]. This implies that any asynchronous better response update process is guaranteed to reach a pure strategy Nash equilibrium. This motivates the algorithm design in the following section.

D. Transaction Inclusion Strategy in We-TIPS

The transaction inclusion strategy in We-TIPS is shown in Algorithm 2. The miner will analyze other miners' transaction selection strategy based on the weak block headers they broadcast, where $\sum_{i \neq i^*} W(i,j)$ in line 7 in Algorithm 2 denotes the number of miners who select the transaction j in their latest weak block header. After knowing other miners' transaction selection strategies, the miner will estimate the expected reward for each transaction based on Lemma 2 (line 8). Based on the estimation of each transaction, the miner will adopt a myopic strategy and select the transactions with the highest expected reward (line 1-5). In this way, the miner will adopt the best response to other miners' behaviors.

We first show that Algorithm 2 can achieve the η-approximate Nash equilibrium in the following theorem.

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

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

Proof. We will show that Algorithm 2 will find a ϵ-approximate Nash equilibrium with the potential function:

$$\Phi(A) = \sum_{j=1}^{m} \sum_{k=1}^{c_j(A)} r_j(k) \leq \sum_{j=1}^{m} n_j(A) r_j(1) \leq N \sum_{j=1}^{n} f_j.$$

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 λ, Δ
Output: T // The set of selected transactions

Function `TransactionSelection` $(i^*, \boldsymbol{f}, W, \lambda, \Delta)$**:**
  for $j = 1, \ldots, m$ **do**
    Estimate the expected reward of transaction j, i.e., $e_j =$ `Estimate` $(i^*, \boldsymbol{f}, W, \lambda, \Delta)$
  Select the transactions with the top-n reward as a set T
  Return T

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

When the miners are homogeneous, each miner has the same probability $1/N$ to generate a new block. When a new weak block is mined, the corresponding miner can publish his latest transaction selection set. If the miner changes his transaction inclusion strategy, we decrease the potential function Φ with a least η. Otherwise, we have reached the η-approximate Nash equilibrium. Similar to the Coupon collector's problem [18], the expected number of rounds before each miner generates a weak block is $\theta(N \log N)$, where N is the number of miners. Therefore, before reaching the η-approximate equilibrium, each $\theta(N \log N)$ rounds will decrease Φ with a least η. Then the expected number of rounds is at most

$$\frac{\Phi(a)\theta(N \log N)}{\eta} \leq \epsilon^{-1} N^2 \log N \sum_{j=1}^{n} f_j.$$

Besides, the game ends when a strong block is mined. With $\beta = T_w/T_s$ denoting the difficulty ratio of mining a strong block and weak block, the expected number of weak blocks in each round is β. Therefore, we have that

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

Thus, we have

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

The proof is thus completed. □

According to Theorem 2, we can find that a larger weak block ratio β indicates a smaller η. Specially, we can show that when β is large enough, i.e., $\beta \to \infty$, Algorithm 2 is guaranteed to achieve the pure strategy Nash equilibrium.

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.*

Proof. Since the potential game has the finite improvement property, we assume that after χ better response update, it can reach the pure strategy Nash equilibrium. According to the Coupon collector's problem, the probability that there is no better response update in r rounds (each weak block corresponds to a single round) is that $\Pr(r) \leq \left(1 - \frac{1}{N}\right)^r \leq e^{-r/N}$. And the probability that there will be χ better response update within $\chi \cdot r$ rounds is that $\Pr(\chi) \geq \left(1 - e^{-r/N}\right)^{\chi}$. The game ends when a strong header is mined with the probability $1/\beta$. And the number of total rounds in the game follows the geometric distribution with the expected value $\mu = \beta$ and variance $\sigma^2 = \beta^2 - \beta$. Using Chebyshev's inequality, the probability that there will be at least $\chi \dot{r}$ rounds is

$$\Pr(\chi \cdot r) = 1 - \sum_{i=1}^{\chi \cdot r} (1 - \frac{1}{\beta})^i \frac{1}{\beta} \geq \frac{\beta^2 - \beta}{(\beta - \chi r)^2}$$

Let $r = \frac{\sqrt{\beta}}{\chi}$, then the probability that Algorithm 2 will achieve the pure strategy Nash equilibrium is

$$\Pr(\text{NE}) = \Pr(\chi \cdot r) \cdot \Pr(\chi) \geq \frac{\beta^2 - \beta}{(\beta - \sqrt{\beta})^2} \cdot \left(1 - e^{-\frac{\sqrt{\beta}}{N}}\right)^{\chi}$$

Thus we have $\lim_{\beta \to \infty} \Pr(\text{NE}) = 1$, which implies that we can achieve the pure strategy Nash equilibrium with probability 1 when $\beta \to \infty$. The proof is thus completed. □

Consistent with the equilibrium analysis in TIPS, when the effective network propagation delay Δ is small enough, Algorithm 2 in We-TIPS is guaranteed to achieve the unique Nash equilibrium as in TIPS.

Theorem 4. *Selecting the transactions with the top-n transaction fee is the unique Nash equilibrium in this transaction inclusion game when $\Delta \leq \frac{1}{\lambda} \varphi\left(\frac{f_{n+1}}{f_n}\right)$ and Algorithm 2 is guaranteed to achieve the unique Nash equilibrium.*

Proof. Since $\Delta \leq \frac{1}{\lambda} \varphi\left(\frac{f_{n+1}}{f_n}\right)$ is equivalent to $\frac{1 - e^{-\lambda\Delta}}{\lambda\Delta} \geq \frac{f_{n+1}}{f_n}$. We are going to prove that when $\frac{1 - e^{-\lambda\Delta}}{\lambda\Delta} \geq \frac{f_{n+1}}{f_n}$, the unique Nash equilibrium in this transaction inclusion game is to always include the transactions with the highest transaction fee, i.e., the top n transactions. Initially, according to Algorithm 2, all the miners will choose to include the transactions with the highest transaction fee, and thus achieve the Nash equilibrium and will not change their transaction inclusion strategy.

Denote the transaction set $\mathbb{A} = \{1, 2, \cdots, n\}$ as the top n transactions with the highest fee, and transaction set $\mathbb{B} = \{n+1, \cdots, m\}$ as the set of the remaining transactions. Then according to Lemma 2, the expected reward for the transaction in $\mathbb{A}$ is

$$r_j = r_j(N) = \frac{1 - e^{-\lambda\Delta}}{\lambda\Delta} f_j, \forall j \in \mathbb{A},$$

and the expected reward for transaction in $\mathbb{B}$ is

$$r_j = r_j(1) = f_j, \forall j \in \mathbb{B}.$$

Then we have that

$$\min_{j \in \mathbb{A}} r_j = r_n = \frac{1 - e^{-\lambda\Delta}}{\lambda\Delta} f_n.$$

and that $\max_{j\in\mathbb{B}} r_j = r_{n+1} = f_{n+1}$. Since $\frac{1-e^{-\lambda\Delta}}{\lambda\Delta} \geq \frac{f_{n+1}}{f_n}$, we have that $\min_{j\in\mathbb{A}} \geq \max_{j\in\mathbb{B}}$, therefore transactions in $\mathbb{A}$ are always the transactions with the highest expected reward, none of the miners have the incentive to choose other transactions, which reaches the equilibrium. The proof is thus completed. □

IV. Performance Evaluation

In this section, we first provide empirical results of Conflux [19], one of the most popular DAG-based blockchain systems, and show how transaction inclusion collision degrades its system performance. Then we conduct experiments to demonstrate the performance of We-TIPS, and further validate our analysis.

A. Empirical Results of Conflux

Conflux is one of the most popular DAG-based blockchain systems. To avoid transaction inclusion collision, Conflux adopts the random transaction inclusion strategy with transaction fee priority, that is, the miner will include the transaction i in his block with probability p_i, where $\frac{p_1}{f_1} = \frac{p_2}{f_2} = \cdots = \frac{p_m}{f_m}$.

We set up a full node of Conflux on a server with one AMD Ryzen 5950X (16 cores 32 HT) CPU and 32 GB memory to pull the latest blocks from the mainnet of Conflux. We have collected the blocks in 1000 epochs (from 32289102-th epoch to 32290102-th epoch), which includes total of 5584 transactions but only 4043 unique transactions, implying that the block capacity utilization of Conflux is around 72.40%. This implies that around 27.60% block capacity is wasted due to the transaction inclusion collision.

B. Experiment Configuration

We develop a DAG-based blockchain simulator in Python using Simpy [20]. The experimental configuration is as follows. We set the block size to 1MB, which is the current block size limitation in Bitcoin. With the average transaction size being 500 bytes, we put 2000 transactions in one block, i.e., $n = 2000$. Besides, we assume the size of the transaction pool to be $m = 10000$. The propagation delay for the whole block is a random variable following the normal distribution with the expectation of $\Delta = 10$, and the propagation delay for the signal is a random variable following the normal distribution with the expectation of $\tau = 1$. The block generation rate of the DAG-based blockchain system λ ranges from 0.1 to 1.

C. Weak Block Ratio Design

Since the weak block ratio β will directly affect the performance of We-TIPS as shown in Theorem 2, we first investigate the impact of the weak block ratio β. Figure 2 demonstrates the block utilization of We-TIPS with different weak block ratios β. Specially, when $\beta = 1$, the We-TIPS degenerates to TIPS. We can find that block utilization increases with the weak block ratio. This is because a large β can provide more accurate information for miners to avoid transaction inclusion collision. However, due to the propagation delay of the weak block header, when β is large, too many weak block headers may be generated during the mining process, resulting in an intensive network load. And some weak block headers may not be broadcast to all the miners in time, leading to insignificant improvement. As shown in Figure 2, $\beta = 4$ is the "elbow" where the insignificant increase in the utilization is no longer worth the additional increase on β. Thus, we take $\beta = 4$ in our experiment.

D. Performance Results

To compare and further demonstrate the performance of We-TIPS, we consider the following baselines in DAG-based blockchain systems:

- "TIPS": stands for transaction inclusion protocol in [11].
- "Priority": stands for the random strategy with transaction fee priority adopted by Conflux [19].
- "Equilibrium": stands for the equilibrium strategy in the standard DAG-based blockchain system [9].
- "Top": stands for the top-n strategy in the standard DAG-based blockchain system, where the miners always include the transactions with the highest transaction fees.
- "We-TIPS": stands for our proposed weak-block-based transaction inclusion protocol with signaling.

Figure 3 shows the block capacity utilization of different transaction inclusion protocols. We can find that We-TIPS always achieves the highest utilization compared to TIPS and the other protocols. Specially, when $\lambda = 0.2$, the "Priority" strategy can achieve 77% utilization, the "Equilibrium" strategy can achieve 79% utilization, TIPS can achieve 90% utilization, while We-TIPS can achieve the astonishing 98% utilization. This implies that We-TIPS can effectively avoid transaction inclusion collision. Figure 4 shows the system throughput (TPS) of different transaction inclusion protocols, which shows that We-TIPS also always achieves the highest system throughput compared to TIPS and the other protocols.

V. Related Work

In the inclusive blockchain protocols [9], the authors model the transaction selection as a non-cooperative game with incomplete information and propose a myopic strategy. Conflux [19] models the transaction selection as a cooperative game and distributes the transaction fee based on Shapley value [21]. In [11], the authors propose "TIPS", which introduces a "signal" in the transaction selection game, and help to improve the system performance by avoiding transaction inclusion collision after finding a new block. However, TIPS only signals other miners when a new block is successfully mined, which limits its performance improvement. Faced with this limitation, we propose "We-TIPS", the weak-block-based transaction inclusion protocol with signaling in DAG-based blockchain, which can signal the miners to avoid transaction inclusion collision even during the mining process.

Employing weak solutions (and their variations) in Bitcoin is an idea circulating on Bitcoin forums for many years [22], [23]. Initial proposals leverage weak solutions (i.e., weak blocks) for faster transaction confirmations [24], [25] and fork selection rule [26]. Rizun proposes Subchains [27], where

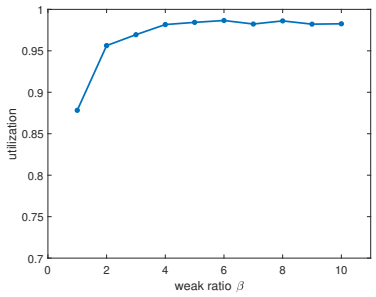

Fig. 2. Utilization of We-TIPS with different ratios β

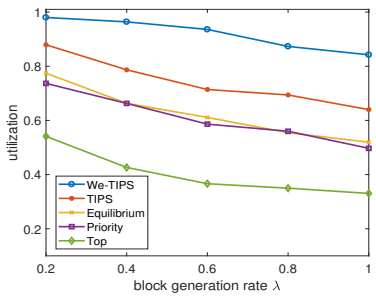

Fig. 3. Utilization of different transaction inclusion protocols

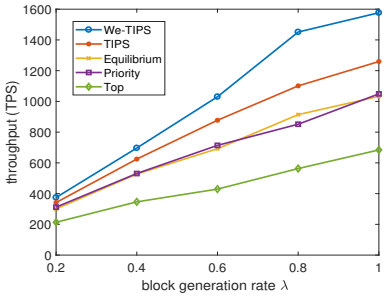

Fig. 4. TPS of different transaction inclusion protocols

a chain of weak blocks bridging each pair of subsequent strong blocks is created. In [14], the authors propose the StrongChain based on the idea of the weak block to make the mining process more transparent and collaborative. However, the previous work mainly focuses on the application of weak blocks in the linear blockchain. Along a different line, we apply the weak block in DAG-based blockchain system and design a novel signaling protocol.

VI. Conclusion

In this paper, we proposed a novel weak-block-based transaction inclusion protocol with signaling, We-TIPS, which effectively avoids the transaction inclusion collision and achieves near-optimal performance while maintaining system security. Both the theoretical analysis and experiment results significantly demonstrate the high efficiency of We-TIPS.

Multi-agent reinforcement learning (MARL) is an ideal tool to capture the feature of the mining process in We-TIPS after modeling the system as a multi-agent Markov decision process (MMDP). Using MARL to explore a more efficient transaction inclusion strategy will be one of our future works.

References

[1] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2019.

[2] L. Duan, L. Huang, C. Langbort, A. Pozdnukhov, J. Walrand, and L. Zhang, "Human-in-the-loop mobile networks: A survey of recent advancements," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 4, pp. 813–831, 2017.

[3] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into iot for security: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 452–10 473, 2021.

[4] M. Swan, J. Potts, S. Takagi, F. Witte, and P. Tasca, *Blockchain economics: implications of distributed ledgers: markets, communications networks, and algorithmic reality*. World Scientific Publishing Co. Pte. Ltd., 2019.

[5] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding characteristics and system implications of DAG-based blockchain in IoT environments," *IEEE Internet of Things Journal*, 2021.

[6] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, 2019.

[7] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG blockchain enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT," *IEEE Internet of Things Journal*, 2021.

[8] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "Sok: Diving into dag-based blockchain systems," *arXiv preprint arXiv:2012.06128*, 2020.

[9] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 528–547.

[10] H. Gupta and D. Janakiram, "CDAG: A serialized blockdag for permissioned blockchain," *arXiv preprint arXiv:1910.08547*, 2019.

[11] C. Chen, X. Chen, and Z. Fang, "Tips: Transaction inclusion protocol with signaling in dag-based blockchain," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3685–3701, 2022.

[12] B. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Web and Internet Economics: 13th International Conference, WINE 2017, Bangalore, India, December 17–20, 2017, Proceedings 13*. Springer, 2017, pp. 205–218.

[13] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[14] P. Szalachowski, D. Reijsbergen, I. Homoliak, and S. Sun, "Strongchain: Transparent and collaborative proof-of-work consensus," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 819–836.

[15] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International conference on financial cryptography and data security*. Springer, 2014, pp. 436–454.

[16] B. Rosen, "Asymptotic theory for successive sampling with varying probabilities without replacement, i," *The Annals of Mathematical Statistics*, pp. 373–397, 1972.

[17] J. N. Webb, *Game theory: decisions, interaction and Evolution*. Springer Science & Business Media, 2007.

[18] I. Adler, S. Oren, and S. M. Ross, "The coupon-collector's problem revisited," *Journal of Applied Probability*, vol. 40, no. 2, pp. 513–518, 2003.

[19] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. C.-C. Yao, "A decentralized blockchain with high throughput and fast confirmation," in *2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, 2020, pp. 515–528.

[20] N. Matloff, "Introduction to discrete-event simulation and the simpy language," *Davis, CA. Dept of Computer Science. University of California at Davis. Retrieved on August*, vol. 2, no. 2009, pp. 1–33, 2008.

[21] A. E. Roth, *The Shapley value: essays in honor of Lloyd S. Shapley*. Cambridge University Press, 1988.

[22] K. Rosenbaum. (2016) Weak blocks – the good and the bad. [Online]. Available: https://popeller.io/index.php/2016/01/19/weak-blocks-the-good-and-the-bad/

[23] G. Andresen. (2015) [bitcoin-dev] weak block thoughts. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-September/011157.html

[24] T. Nolan. (2013) Decoupling transactions and POW. [Online]. Available: https://bitcointalk.org/index.php?topic=179598.0

[25] P. Todd. (2013) [bitcoin-development] near-block broadcasts for proof of tx propagation. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-September/003275.html

[26] T. Nolan. (2013) [bitcoin-development] distributing low pow headers. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-July/002976.html

[27] P. R. Rizun, "Subchains: A technique to scale Bitcoin and improve the user experience," *Ledger*, vol. 1, pp. 38–52, 2016.