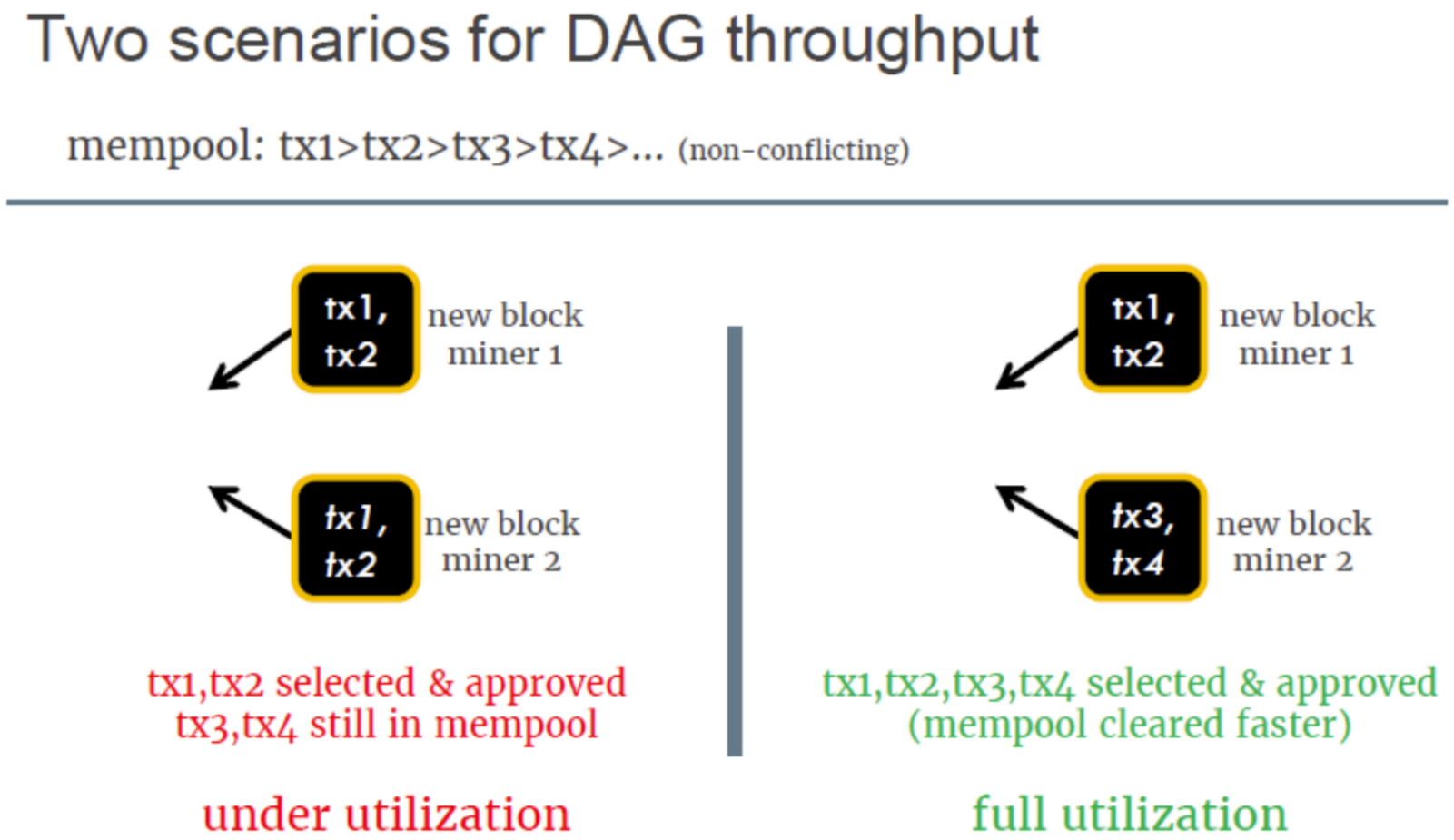
TIPS: Transaction Inclusion Protocol with Signaling in DAG-based Blockchain

Canhui Chen →

Background


Two scenarios for DAG throughput
mempool: tx1>tx2>tx3>tx4>... (non-conflicting)
tx1, tx2
new block miner 1
tx1, tx2
new block miner 2
tx1,tx2 selected & approved
tx3,tx4 still in mempool
under utilization
tx1, tx2
new block miner 1
tx3, tx4
new block miner 2
tx1,tx2,tx3,tx4 selected & approved
(mempool cleared faster)
full utilization

Transaction Inclusion Game

- The block generation process follows the Poisson process with a rate λ.
- we denote the maximum network propagation delay for a block as Δ.
- There are m transactions in the pool and each block will contain n transactions.

We denote a miner's transaction inclusion strategy as $\mathbf{p} \in \mathbb{P}$. Here $\mathbb{P} = \{\mathbf{p} | 0 \leq p_i \leq 1 \text{ and } \sum_{i=1}^{m} p_i = n\}$ denotes the set of transaction inclusion strategies, and p_i denotes the probability of including the transaction i in the new block. Without loss of generality, we sort the transactions in the transaction pool in descending order by their transaction fees, where the transaction fee of the transaction i is denoted as f_i. Then we have $f_1 \geq f_2 \geq \cdots \geq f_m$. As examples, we show below three typical transaction inclusion strategies:

- Random inclusion ($\mathbf{p}^{\text{rand}}$): $p_1 = p_2 = \cdots = p_m = \frac{n}{m}$.
- Random inclusion with priority ($\mathbf{p}^{\text{priority}}$): $p_1 \geq p_2 \geq \cdots \geq p_m$ and $\frac{p_1}{f_1} = \frac{p_2}{f_2} = \cdots = \frac{p_m}{f_m}$.
- Top n ($\mathbf{p}^{\text{top}}$): $p_1 = p_2 = \cdots = p_n = 1$ and $p_{n+1} = p_{n+2} = \cdots = p_m = 0$.

Equilibrium in Transaction Inclusion Game

Theorem 1. With the network propagation delay for the whole block as Δ, the symmetric equilibrium strategy of the transaction inclusion game is $p^*(\Delta)$, where

$$p_i^*(\Delta) = \begin{cases} \min\{r^{-1}\left(\frac{c_{l^*}}{f_i}|\Delta\right), 1\}, & 1 \leq i \leq l^*, \\ 0, & l^* < i \leq m. \end{cases}$$

Also, we have

$$F_l(c) = \sum_{i=1}^{l} \min\{r^{-1}(c/f_i|\Delta), 1\} - n, \quad \forall 1 \leq l \leq m,$$

$$l^* = \max\{l \leq m | \forall i \leq l : F_i\left(f_i\right) \leq 0\},$$

$$c_{l^*} \text{ is the root of } F_{l^*}.$$

Revenue Dilemma Analysis

Theorem 2. The random strategy, i.e., $\mathbf{p}^{\text{rand}}$ is a ξ-approximate Nash equilibrium, where

$$\xi = n\frac{1-e^{-\lambda\Delta\frac{n}{m}}}{\lambda\Delta\frac{n}{m}}\left(\frac{1}{n}\sum_{i=1}^{n}f_i - \frac{1}{m}\sum_{i=1}^{m}f_i\right).$$

Specially, when $\Delta \to \infty$, the random strategy is the Nash equilibrium.

- To achieve a high revenue, miners are supposed to include transactions with high fees, i.e., to adopt the ``top n'' strategy.
- Denote $y(\Delta) = \frac{1-e^{-\lambda\Delta\frac{n}{m}}}{\lambda\Delta\frac{n}{m}}$. Note that $y(\Delta)$ is monotonically decreasing in Δ. This implies that the equilibrium transaction inclusion strategy will lean towards the random strategy.

Throughput Dilemma Analysis

Theorem 3. The block capacity utilization and the throughput of the DAG-based blockchain with the transaction inclusion strategy $\mathbf{p}$ and the network propagation delay Δ are

$$\mathrm{U}(\mathbf{p}) = \frac{m - \sum_{i=1}^{m}(1-p_i)e^{-\lambda\Delta p_i}}{n(\lambda\Delta+1)}, \quad \mathrm{TPS}(\mathbf{p}) = \lambda n \mathrm{U}(\mathbf{p}),$$

respectively.

- To achieve a higher system throughput, we should enlarge the block size so as to include more transactions.
- However, if the block size is increased, the corresponding network propagation delay Δ will also increase, leading to a lower block capacity utilization, which will further degrade the system throughput.

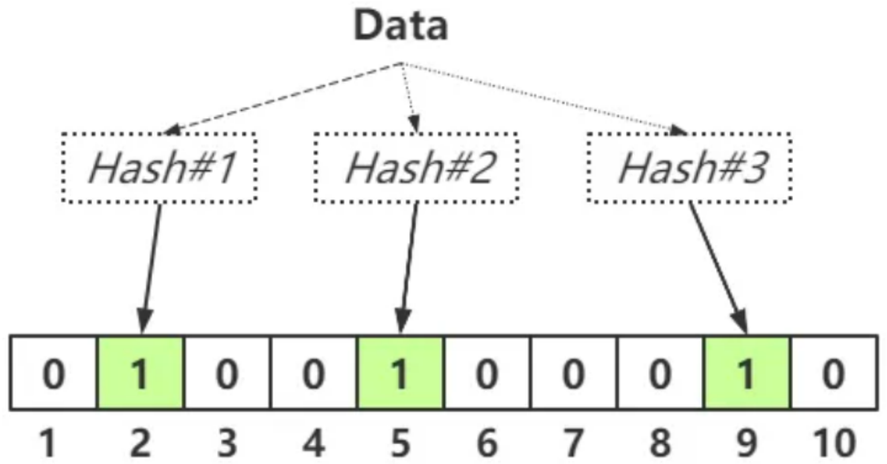
Transaction Inclusion Protocol with Signaling

To tackle the dilemmas in DAG-based blockchain, we introduce ``TIPS'', i.e., the Transaction Inclusion Protocol with Signaling. The key features of TIPS are

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

As a baseline, we will compare TIPS with the standard DAG-based blockchain protocol (i.e., without TIPS), where the miners do not obtain any information of the newly-generated block until they receive the whole block.

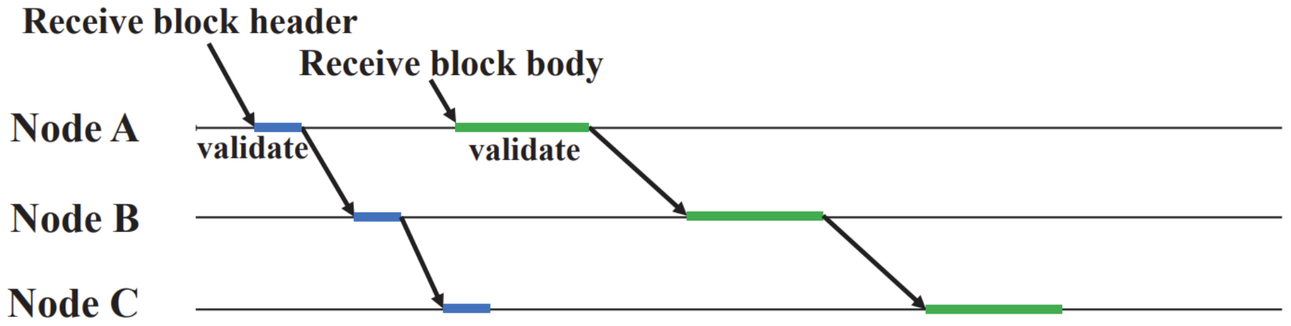
Bloom Filter in Block Header



The key metric is the false positive rate of a Bloom filter, i.e., the probability that the Bloom filter returns "True" but the element is not a member of the set. Consider a Bloom filter with b bits and h different hash functions. We assume that the block size limit is n transactions per block. Thus, we can insert at most n transactions into the Bloom filter associated with the block. The probability of false positives of the Bloom filter with n transactions is % i.e., a query returns ``exist'' while the transaction is not in the set,

$$\epsilon = \left(1 - e^{-hn/b}\right)^h.$$

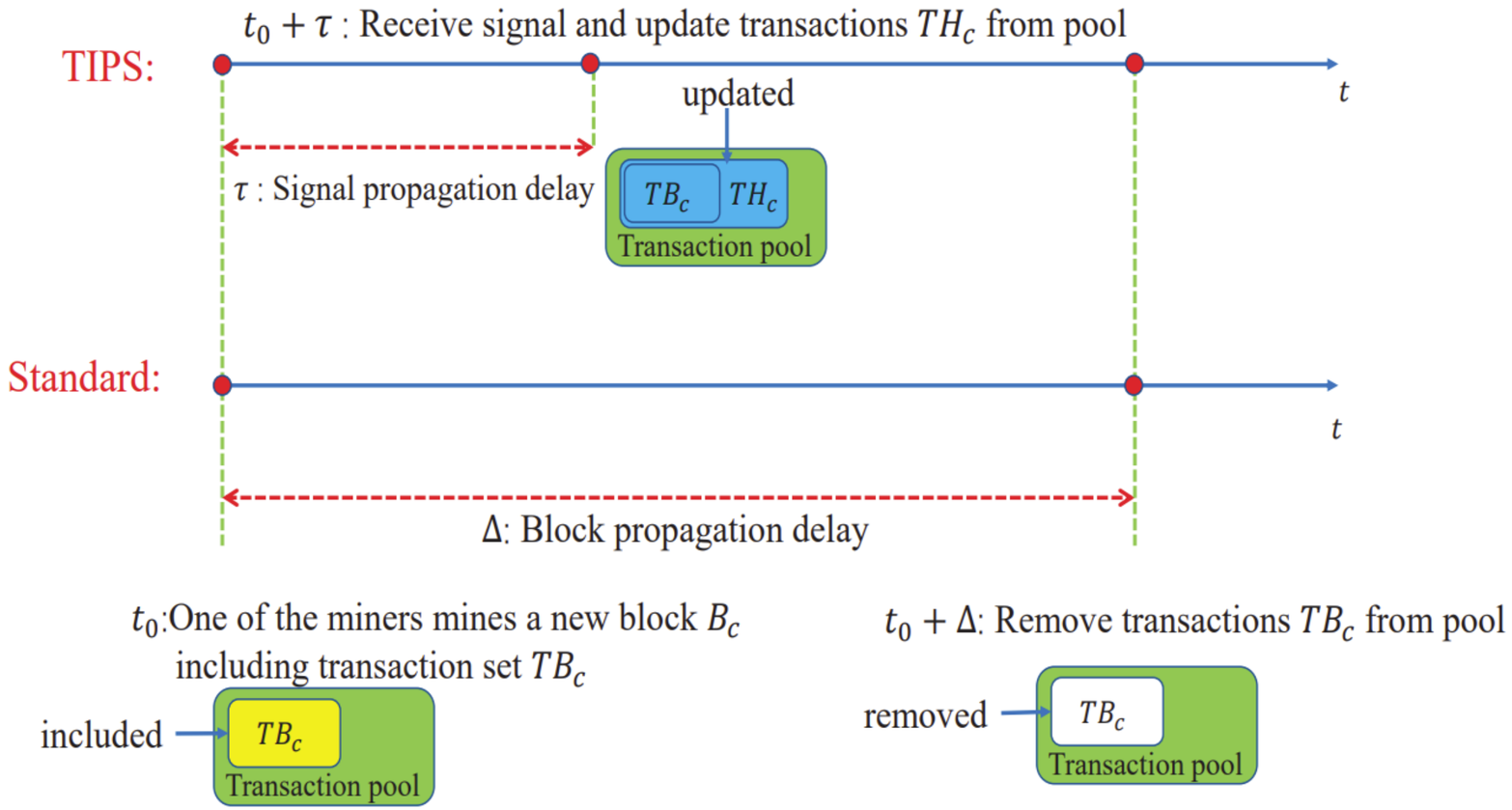
Header-First Block Propagation



For a node A, upon receiving a message, there are two possible cases:

- When node A receives a new block header BH_c of block B_c, it validates BH_c and checks whether the hash value of the block header satisfies the PoW puzzle.
- When node A receives a new block body BB_c of block B_c, it validates BB_c as follows:
  - Block Header Existence: If the miner did not receive the corresponding block header BH_c before, he should reject the block body immediately since he can not validate the PoW of the block.
  - Bloom filter Validation: If the Bloom filter in the block header does not match the transactions in the block body, the block will be marked as ``invalid'' and be rejected.

Mining Process in TIPS



If a transaction i hits the Bloom filter of a valid signal, its expected value should be multiplied by ϵ, because the Bloom filter implies that the probability that the transaction i is not included in the new block is only ϵ.

TIPS Breaks Down the Dilemmas

Lowering Effective Network Delay

Theorem 4. If the false positive probability of the Bloom filter satisfies $\epsilon < \frac{f_m}{f_1}$, the symmetric equilibrium in TIPS is $\mathbf{p}^*(\tau)$, where %Besides, the expected reward for the miner to include transaction i given that other miners include transaction i in their blocks with probability p_i in TIPS is $f_i \cdot r^*(p_i)$.

$$p_i^*(\tau) = \begin{cases} \min\{r^{-1}\left(\frac{c_{l^*}}{f_i}|\tau\right), 1\}, & 1 \leq i \leq l^*, \\ 0, & l^* < i \leq m. \end{cases} \tag{1}$$

Also, we have

$$F_l(c) = \sum_{i=1}^{l} \min\{r^{-1}(c/f_i|\tau), 1\} - n, \quad \forall 1 \leq l \leq m,$$

$$l^* = \max\{l \leq m | \forall i \leq l : F_i\left(f_i\right) \leq 0\},$$

$$c_{l^*} \text{ is the root of } F_{l^*}.$$

Approaching Top n Strategy

Theorem 5. The top n strategy, i.e., $\mathbf{p}^{\text{top}}$ is an η-approximate Nash equilibrium, where

$$\eta \leq \left| n \left(1 - \frac{1 - e^{-\lambda\tau}}{\lambda\tau} \right) f_n \right| .$$

The equation holds if and only if the transactions are homogeneous, that is, the transaction fees are the same. Specially, when $\tau \to 0$, the top n strategy is the Nash equilibrium.

Theorem 6. The top n strategy, i.e., $\mathbf{p}^{\text{top}}$ is the unique Nash equilibrium when

$$\tau \leq \frac{1}{\lambda} \varphi^{-1} \left(\frac{f_{n+1}}{f_n} \right), \tag{1}$$

where $\varphi(x) = \frac{1-e^{-x}}{x}$, and $\varphi^{-1}(x)$ is its inverse function.

Breaking Down the Revenue Dilemma

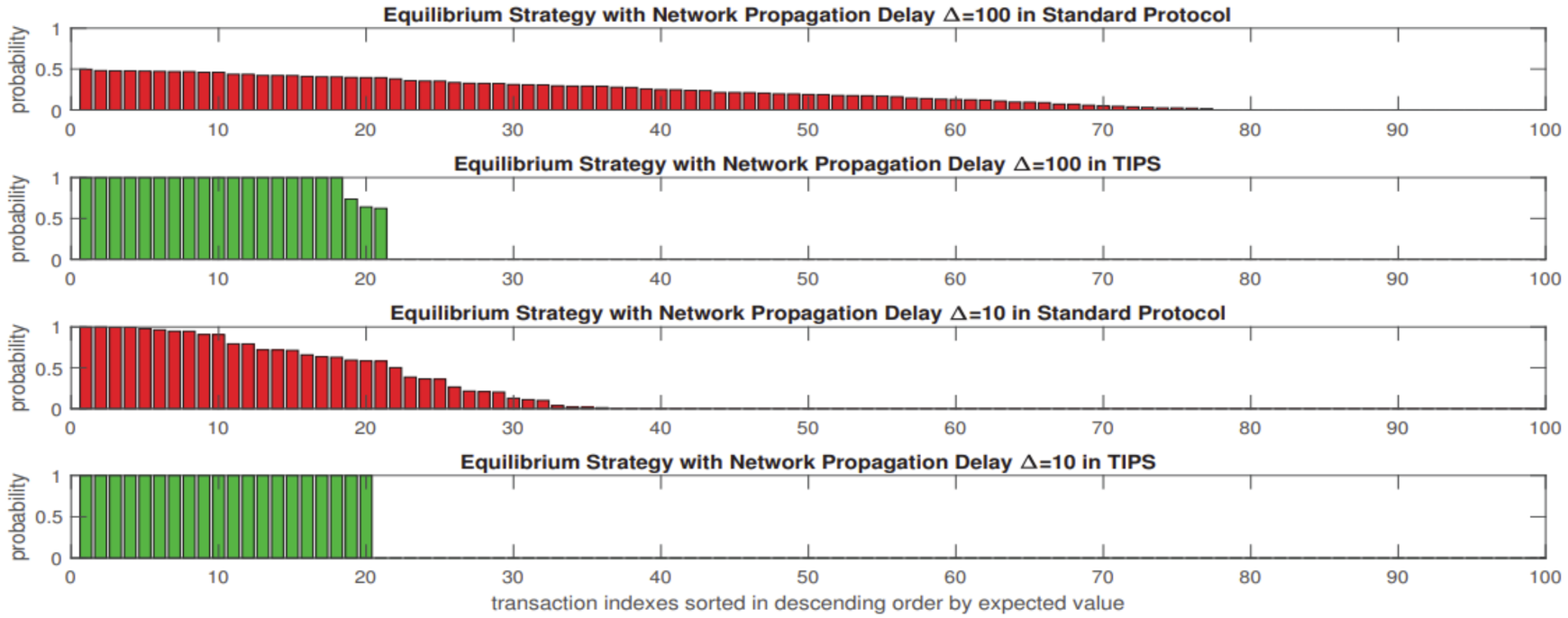


Fig. 4. Equilibrium strategy with different network propagation delay

Definition The efficiency of the equilibrium strategy of the transaction inclusion game in DAG-based blockchain under the revenue dilemma is defined as the ratio of the miners' revenue R under the equilibrium strategy of the transaction inclusion game and the highest miners' revenue achieved by any transaction inclusion strategy, which is shown as follows:

$$\text{Efficiency(R)} = \frac{\text{Revenue of Equilibrium}}{\text{Revenue of optimal strategy}}. \tag{1}$$

Theorem 7. The efficiency of the equilibrium strategy of the transaction inclusion game in DAG-based blockchain with TIPS under the revenue dilemma is

$$\text{Efficiency}(R) \geq \frac{(1-e^{-\lambda\tau})}{\left(\lfloor \frac{m}{n} \rfloor - \sum_{k=0}^{\lfloor \frac{m}{n} \rfloor} \frac{(\lambda\tau)^k}{k!} e^{-\lambda\tau}\right)}.$$

We have that $\lim_{\tau\to 0} \text{Efficiency}(R) = 1$. This is because when $\tau \to 0$, the top n strategy $\mathbf{p}^{\text{top}}$ is the unique Nash equilibrium. Besides, we have $\lim_{\Delta=\tau\to 0} R(\mathbf{p}^{\text{top}}) = \sum_{i=1}^{n} f_i$, which implies that the miner can also obtain the highest transaction fee reward.

Breaking Down the Throughput Dilemma

Lemma 2. The limit throughput of the DAG-based blockchain with the top n transaction inclusion strategy $\mathbf{p}^{\text{top}}$ is

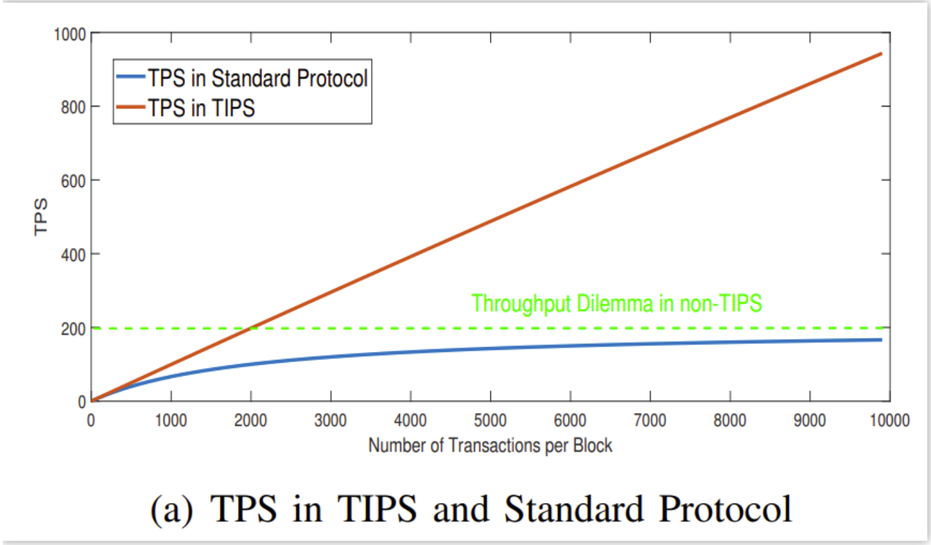
$$\lim_{n\to\infty} TPS(\mathbf{p}^{\text{top}}, n) = \lim_{n\to\infty} \frac{1}{\frac{\mathrm{d}\Delta(n)}{\mathrm{d}n}},$$

where $\frac{\mathrm{d}\Delta(n)}{\mathrm{d}n}$ is the derivative of $\Delta(n)$.

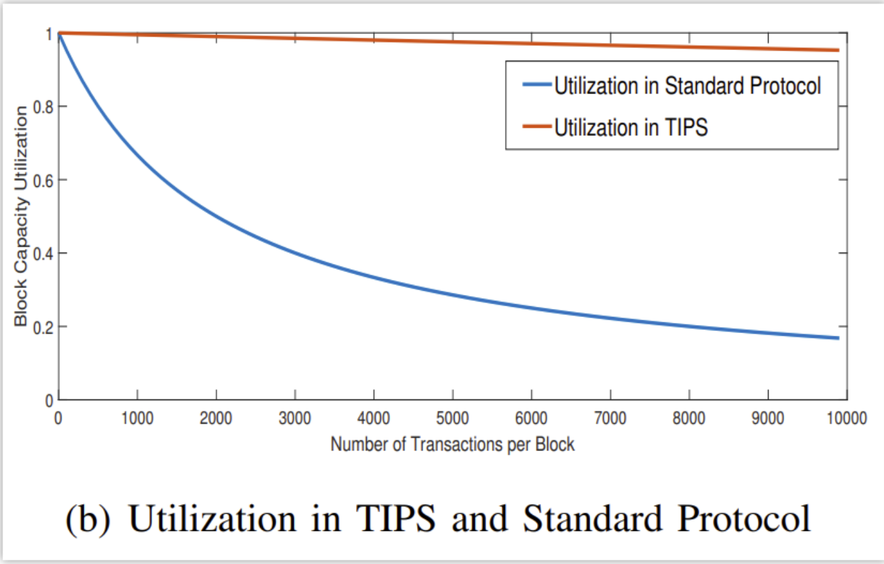
We compared the limit throughput of TIPS and the standard protocol below.

$$\begin{aligned}\frac{\lim_{n\to\infty} TPS^{\text{TIPS}}(\mathbf{p}^{\text{top}}, n)}{\lim_{n\to\infty} TPS^{\text{Standard}}(\mathbf{p}^{\text{top}}, n)} &= \frac{\lim_{n\to\infty} \frac{1}{\frac{\mathrm{d}\tau(n)}{\mathrm{d}n}}}{\lim_{n\to\infty} \frac{1}{\frac{\mathrm{d}\Delta(n)}{\mathrm{d}n}}} = \lim_{n\to\infty} \frac{\frac{\mathrm{d}\Delta(n)}{\mathrm{d}n}}{\frac{\mathrm{d}\tau(n)}{\mathrm{d}n}} \\ &= \frac{\text{transaction size}}{\varsigma \text{ bits}},\end{aligned} \tag{1}$$

where ς denotes the number of bits per transaction in the Bloom filter. Therefore, theoretically, the ratio of the limit throughput of TIPS and the standard protocol can be as large as 5×10^5.



(a) TPS in TIPS and Standard Protocol



(b) Utilization in TIPS and Standard Protocol

Theorem 8. The efficiency of the equilibrium strategy of the transaction inclusion game in DAG-based blockchain with TIPS under the throughput dilemma is

$$\text{Efficiency}(TPS) \geq \frac{(1-e^{-\lambda\tau})}{\left(\lfloor \frac{m}{n} \rfloor - \sum_{k=0}^{\lfloor \frac{m}{n} \rfloor} \frac{(\lambda\tau)^k}{k!} e^{-\lambda\tau}\right)}.$$

We have have that $\lim_{\tau\to 0} \text{Efficiency}(TPS) = 1$. Thus, TIPS can achieve near-optimal TPS, and therefore can efficiently break down the throughput dilemma.

Security Discussion

Denial of Service Attack

Signal Flood. A possible attack is that the attacker can broadcast a signal with lots of bits of Bloom filter set to 1 to lower the expected value of transactions, which can reduce the miners' expected reward (even less than the mining cost), and motivate other miners to stop mining.

After n transactions have been added to the Bloom filter, let q be the fraction of the b bits that are set to 0, i.e., the number of bits still set to 0 is qb. Thus, the expectation of q is

$$\mathbb{E}(q) = \left(1 - \frac{1}{b}\right)^{hn}.$$

According to previous research on Bloom filter, we have

$$P\left(\mathbb{E}(q) - q \geq \frac{\xi}{m}\right) \leq \exp(-2\xi^2/kn).$$

A Bloom filter with too many bits set to 1 will be rejected. Let η be the probability of rejecting a valid Bloom filter. Let X be the number of bits that are set to 1 in the Bloom filter. Then the Bloom filter will be rejected if the following condition holds:

$$X \geq b - b\left(1 - \frac{1}{b}\right)^{hn} + \sqrt{-\frac{1}{2}hn \ln \eta}. \tag{1}$$

As an example, for a Bloom filter with $b = 20000$ bits, $k = 5$ hash functions and $n = 2000$ transactions included, if the probability of rejecting a valid Bloom filter is 0.01%, a Bloom filter will be rejected if the number of bits that are set to 1 is greater than 9535, while the expectation of the number of bits that are set to 1 for a valid Bloom filter is 7869, which indicates the high sensitivity and accuracy of detection indicator.

Delay of Service Attack

In TIPS, the attacker can delay the successful record of a transaction tx_i by continuously mining a valid block that includes this transaction, but only broadcast the signal without the whole block. However, once the signal is expired, other miners will have the motivation to include the transaction tx_i in the block again.

The expiration time for a block header is T. The fraction of the computing power of the attacker is α. The attacker needs to keep mining new blocks containing the same transaction before the signal is expired. Denote the expected delay time after the attacker initiates this attack as $\mathbb{E}(D)$. If the attacker mines a new block at time $t < T$ before the previous signal is expired, he can delay the transaction with extra $\mathbb{E}(D)$ time. Otherwise, he can only delay at most the expiration time T. Then we have

$$\mathbb{E}(D) = \int_0^T (t + \mathbb{E}(D))\alpha\lambda e^{-\alpha\lambda t} dt + \int_T^\infty T\alpha\lambda e^{-\alpha\lambda t} dt.$$

Therefore, the expected delay time is

$$\mathrm{Delay}(\alpha) = \alpha\mathbb{E}(D) = \frac{1}{\lambda}\left(e^{\alpha\lambda T} - 1\right),$$

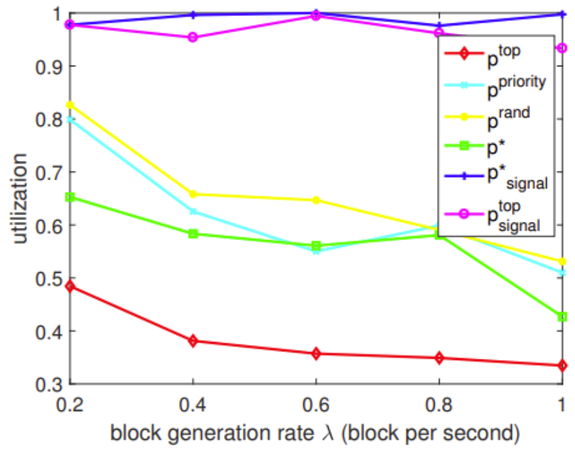


Fig. 6. Utilization of different transaction inclusion protocols

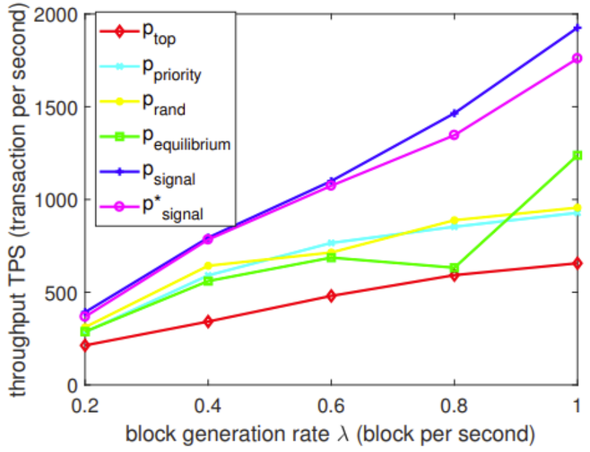


Fig. 7. TPS of different transaction inclusion protocols

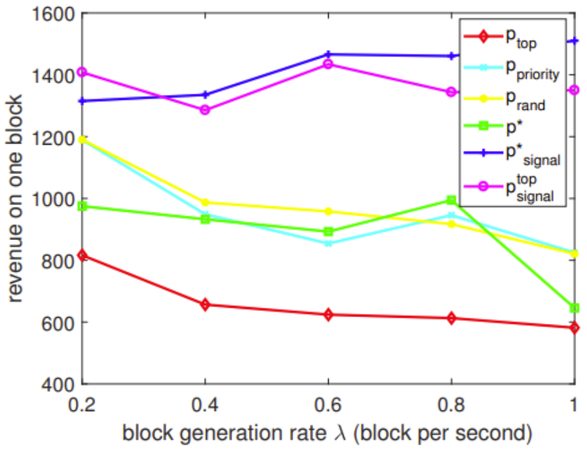


Fig. 8. Miners' revenue of different transaction inclusion protocols

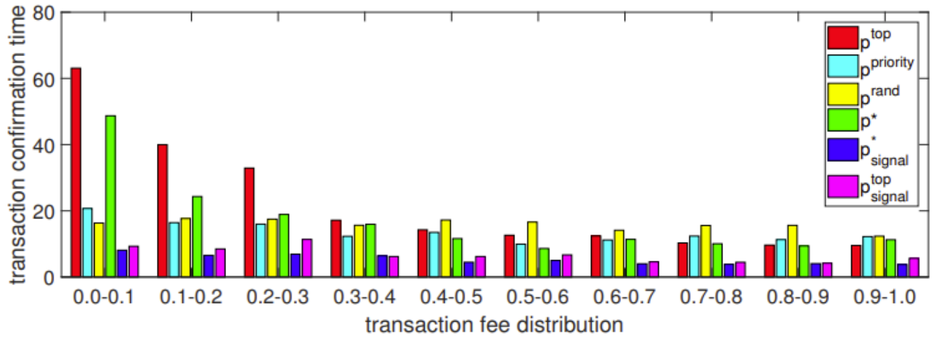


Fig. 9. Average transaction confirmation time under different transaction inclusion protocols

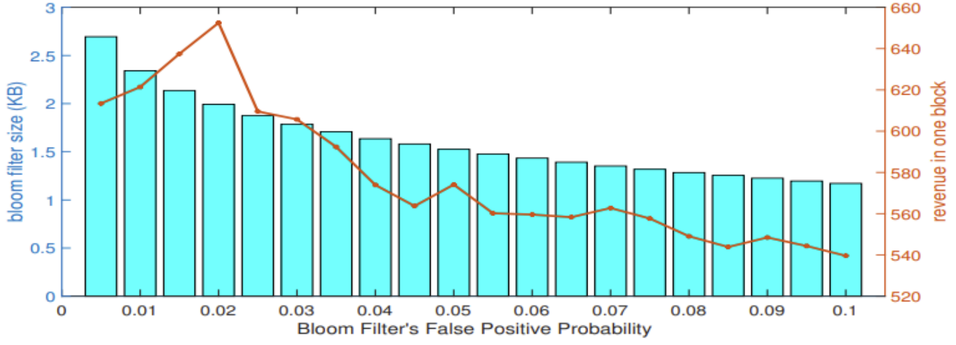


Fig. 10. Experimental results with different Bloom filters' false positive probabilities

Conclusion and Contribution

- We characterize the revenue dilemma and the throughput dilemma of DAG-based blockchain systems. We show this is due to the transaction collisions in the incordinated DAG-based blockchain system, and that a low network propagation delay is the key to break the dilemmas.
- We propose a novel Transaction Inclusion Protocol with Signaling (TIPS) in DAG-based blockchain.
- We provide a thorough theoretical analysis of the performance and security of TIPS. Besides, we also develop a DAG-based blockchain simulator and conduct intensive experiments. Both the theoretical analysis and experiment results show that TIPS can substantially resolve both the revenue and the throughput dilemmas.

Thanks~

Q&A