

# Controlling Transaction Rate in Tangle Ledger: A Principal Agent Problem Approach

ANURAG GUPTA and VIKRAM KRISHNAMURTHY\*, Cornell University, USA

Tangle is a distributed ledger technology that stores data as a directed acyclic graph (DAG). Unlike blockchain, Tangle does not require dedicated miners for its operation; this makes Tangle suitable for Internet of Things (IoT) applications. Distributed ledgers have a built-in transaction rate control mechanism to prevent congestion and spamming; this is typically achieved by increasing or decreasing the proof of work (PoW) difficulty level based on the number of users. Unfortunately, this simplistic mechanism gives an unfair advantage to users with high computing power. This paper proposes a principal-agent problem (PAP) framework from microeconomics to control the transaction rate in Tangle. With users as agents and the transaction rate controller as the principal, we design a truth-telling mechanism to assign PoW difficulty levels to agents as a function of their computing power. The solution of the PAP is achieved by compensating a higher PoW difficulty level with a larger weight/reputation for the transaction. The mechanism has two benefits, (1) the security of Tangle is increased as agents are incentivized to perform difficult PoW, and (2) the rate of new transactions is moderated in Tangle. The solution of PAP is obtained by solving a mixed-integer optimization problem. We show that the optimal solution of the PAP increases with the computing power of agents. The structural results reduce the search space of the mixed-integer program and enable efficient computation of the optimal mechanism. Finally, via numerical examples, we illustrate the transaction rate control mechanism and study its impact on the dynamics of Tangle.

CCS Concepts: • **Information systems** → **Distributed storage**; • **Networks** → **Network protocol design**.

Additional Key Words and Phrases: Distributed ledger, directed acyclic graph, Tangle, transaction rate control, proof of work (PoW), weight of transaction (WoT), principal-agent problem (PAP), mixed-integer optimization, linear program.

## 1 INTRODUCTION

Tangle was created by the IOTA foundation to enable a scalable distributed ledger technology for IoT applications with no transaction fees [21]. Tangle is an example of a directed acyclic graph (DAG) based distributed ledgers [3], [15], [22]. Tangle is a generalization of linear blockchain technology: it stores data as a DAG in contrast to the linear data structure of blockchain. The DAG structure of Tangle allows multiple transactions to be added to the ledger simultaneously. Hence, the throughput of Tangle is significantly higher than blockchain. The modified data structure also supports higher scalability and decreased mining cost [21], which are essential for Internet of Things (IoT) [6], [14] applications. This is because IoT devices have limited computing power and can not afford high transaction fees associated with mining in blockchain. Therefore, Tangle is used in IoT applications such as automating real-time trade and exchange of renewable energy amongst neighbourhoods [25].

---

Authors' address: Anurag Gupta, ag2589@cornell.edu; Vikram Krishnamurthy, vikramk@cornell.edu, Cornell University, 136, Hoy Road, Ithaca, New York, USA, 14853.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

© 2023 Association for Computing Machinery.

XXXX-XXXX/2023/4-ART \$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

There are two important elements of Tangle: proof of work (PoW) and weight of transactions (WoT) [21]. PoW requires users to solve a hash puzzle to add a transaction to the distributed ledger. Increasing the PoW difficulty level increases the computational complexity of the hash puzzle; this is used to control the rate of new transactions and increase the security of Tangle. WoT is the reputation assigned to the transaction. In Tangle, users must select two other transactions randomly and approve them to add a new transaction: if the two transactions do not conflict, they are approved. The probability that a transaction is selected for approval is proportional to its WoT. Therefore, users prefer a higher WoT for their transactions. In the current implementation of Tangle, WoT is a fixed function of PoW [21]; this makes Tangle susceptible to being dominated by users with powerful computational resources. Users with high computational resources can add a very high number of transactions with a high WoT. A natural question is *how to make Tangle fair<sup>1</sup> to all users?*

In this paper, we utilize PoW difficulty level in conjunction with WoT to control the rate of new transactions in Tangle. Specifically, we formulate the transaction rate control problem for Tangle as a *principal-agent problem (PAP) with adverse selection* [17]. The PAP has been studied widely in microeconomics to design a contract between two strategic players with misaligned utilities. Examples include labor contracts [19], insurance market [23], and differential privacy [8]. There are two types of PAP [17]: moral hazard and adversarial selection. We restrict our attention to the PAP with adverse selection as the underlying information asymmetry<sup>2</sup> is similar to that of the transaction rate control problem in Tangle. In IoT applications, heterogeneous IoT devices with different computing power are agents, and the transaction rate controller is the principal. Agents want to add new transactions in Tangle at the maximum possible rate. On the other hand, the principal wants to control the rate of new transactions to reduce network congestion and spamming. As the principal cannot observe the computing power of agents, it also has to incentivize agents to reveal their computing power truthfully. A truth-telling mechanism ensures that agents with high computing power solve a difficult PoW. Incentivizing agents to solve a difficult PoW has two benefits: (1) it moderates the rate of new transactions in Tangle (2) it is difficult for an adversary to tamper with transactions in Tangle, making Tangle more secure. We use a simple fairness measure for transaction rate control: it trades off the rate of new transactions with compensation (WoT) given to the agents for solving PoW. To control the transaction rate, the principal assigns a PoW difficulty level to each agent based on their revealed computing power. To ensure the mechanism is truth-telling, the principal compensates agents' PoW using an appropriate WoT.

To summarize, the information asymmetry between the transaction rate controller and IoT devices motivates PAP with adverse selection as a suitable mechanism for controlling the transaction rate in Tangle. It yields a tractable linear program [4] with useful underlying structures that the principal can exploit to speed up the computation.

## Related Work

Several works study the transaction rate control problem for distributed ledgers. [12] formulates a mechanism to control the PoW difficulty level for blockchain that ensures stable average block times. [18] proposes a difficulty adjustment algorithm for blockchain to disincentivize the miners

<sup>1</sup>By fair, we mean that every agent, irrespective of its computing power, can add transactions into Tangle at a low cost. Also, the mechanism should compensate agents for completing a difficult PoW. Our transaction rate control mechanism compensates agents' PoW with WoT. In Sec.4, we consider a simple fairness measure to trade off PoW and WoT. It is of interest in future work to incorporate schemes such as proportional, max-min and social welfare fairness.

<sup>2</sup>In the PAP with adverse selection, the principal cannot observe the state of agents, and hence, it has to incentivize agents to reveal their state truthfully. The principal then assigns the effort level and compensation based on the revealed information to maximize its own utility.

from coin-hopping attacks: a malicious miner increases his mining profits while at the same time increasing the average delay between blocks. The transaction rate problem has also been studied from the agent's perspective, e.g., agents optimizing their contribution of computing power to the mining process [2].

For the DAG-based distributed ledger, [24] proposed an adaptive rate control for Tangle. Their scheme increases or decreases the difficulty level of the PoW depending on the historical transaction rate of an agent. [11] uses a utility maximization approach to control the rate of transactions in Tangle using a suitable choice of network performance metric. Their model assumes that the computing power of the agent is known to the transaction rate regulator. [5] borrows an idea from wireless networks to control the rate of transactions using an access control scheme. Congestion control has also been studied in the context of wireless communication. For example, [16], [9] discuss optimal resource sharing among multiple users for a high quality of service.

To the best of our knowledge, a PAP-based approach to studying the transaction rate control problem in Tangle has not been explored in the literature. The PAP framework allows us to model the information asymmetry between the distributed ledger's users and the transaction rate controller. It yields a tractable mixed-integer optimization problem that the principal can decompose into multiple linear programs. The PAP also allows us to analyze the structure of decision variables; this is beneficial in reducing the search space dimension and decreasing the computation cost.

Finally, our proposed transaction rate controller is compatible with the IEEE standard 2144.1-2020 [1]. This standard specifies a framework for blockchain-based data management for IoT applications. The IEEE standard 2144.1-2020 identifies the following stakeholders for a typical IoT data collaborative ecosystem: data owners, data consumers, service providers, regulators/policymakers and other stakeholders. Regarding IEEE 2144.1-2020, our proposed transaction rate controller can be considered a regulator/policy maker. The regulator has higher computing power than IoT devices; therefore, it can take the role of transaction rate controller in Tangle. Higher computing power is required to solve our proposed transaction rate control mechanism; using an independent regulator as a transaction rate controller reduces the computational cost of IoT devices.

## Organization and Main Results

Sec.2 describes the Tangle protocol and the PAP approach to solve the transaction rate control problem in Tangle. The PAP is a mixed-integer program: the PoW difficulty level takes values in a finite set, whereas the WoT takes values from the subset of real numbers. We show that for a fixed choice of PoW difficulty level, the PAP for transaction rate control in Tangle is a linear program. This facilitates efficient computation of the optimal solution using standard linear program solvers.

Sec.3 exploits the structure of the PAP to characterize the decision variables. Our first structural result shows that the optimal PoW difficulty level increases with computing power. The second result shows that the optimal WoT assigned to the agents increases with computing power. The principal can exploit the results to reduce the search space for the transaction rate control problem and decrease the computation cost.

Sec.4 illustrates the application of PAP for the transaction rate control problem in Tangle using numerical examples. We also apply the structural result from Sec.3 to reduce the dimension of the search space of the decision variables. We incorporate our proposed transaction rate control mechanism in Tangle and simulate its dynamics. This yields insight into the impact of the transaction rate mechanism on the average approval time of a tip transaction. Finally, we compare the proposed transaction control mechanism with the fixed transaction control scheme in [21], which allocates WoT as a linear function of PoW.

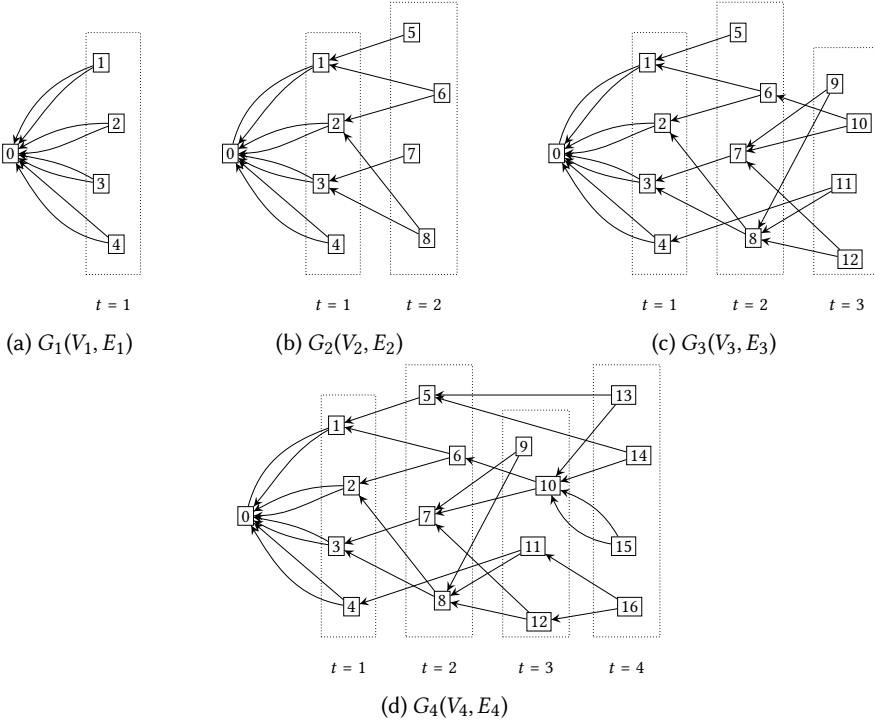


Fig. 1. Protocol for tip transaction selection and approval in Tangle. Consider a dynamic DAG  $G_t(V_t, E_t)$  representing Tangle at time  $t$ . Each node of  $G_t(V_t, E_t)$  represents a transaction. Node 0 is the genesis node at  $t = 0$ . At each time  $t$ , new transactions join the ledger by randomly selecting two tip transactions and approving them. This corresponds to formation of a directed edge. (a) Node 1, 2, 3, 4 join the ledger at  $t = 1$ . Tip node for  $G_0 = (V_0, E_0)$  is 0. (b) Node 5, 6, 7, 8 join the ledger at  $t = 2$ . Tip nodes for  $G_1 = (V_1, E_1)$  are 1, 2, 3, 4. (c) Node 9, 10, 11, 12 join the ledger at  $t = 3$ . Tip nodes for  $G_2 = (V_2, E_2)$  are 4, 5, 6, 7, 8. (d) Node 13, 14, 15, 16 join the ledger at  $t = 4$ . Tip nodes for  $G_3 = (V_3, E_3)$  are 5, 9, 10, 11, 12.

## 2 TRANSACTION RATE CONTROL PROBLEM IN TANGLE

This section describes the PAP formulation for controlling the rate of new transactions in Tangle. Sec.2.1 describes the Tangle protocol, and Sec.2.2 describes the PAP formulation for the transaction rate control problem in Tangle.

### 2.1 Tangle protocol

Tangle can be abstracted as a time-evolving DAG. Fig. 1 shows an example of the time evolution of Tangle.

Consider a time evolving DAG  $G_t(V_t, E_t)$  representing Tangle at time  $t$  where  $t \in \mathbb{Z}^+$  denotes discrete time. Each node in the graph corresponds to a transaction/record stored on Tangle. At  $t = 0$ ,  $G_0(V_0, E_0)$  denotes the *genesis* graph. We assume  $|V_0|= 1, |E_0|= 0$ . At each discrete time instant  $t$ , new transactions are added in Tangle by agents (IoT devices). To join Tangle, each new transaction at time  $t$  chooses two *tip transactions* from  $G_{t-1}(V_{t-1}, E_{t-1})$  randomly, and *approves* them. The two tip nodes are selected independently with repetition. Here, a tip transaction means a transaction with no incoming edges. Approving a tip transaction in Tangle means verifying that the transaction is valid, i.e., there is no double-spending. If the two randomly chosen transactions

are valid, the new transaction forms a directed edge to each randomly chosen tip transaction. We will assume that the chosen tip transactions are always valid, as handling double-spending attacks are beyond the scope of this study. To summarize, every new transaction forms outgoing edges from itself to two randomly chosen tip transactions to join Tangle.

When adding a new transaction, agents must show PoW by solving a hash puzzle. This is to prevent spamming<sup>3</sup>. Hash puzzles also ensure that tampering<sup>4</sup> a transaction in Tangle is difficult [10]. Based on the PoW difficulty level, the transaction is assigned a weight. During random selection of the two tip transactions, the probability of choosing a particular tip transaction is directly proportional to its weight. Hence, agents optimally choose the PoW difficulty level based on their preference for WoT. In the current implementation of Tangle [21], the relation between the WoT and its PoW difficulty level is a fixed linear function. We propose a modified mechanism to assign the PoW difficulty level and corresponding WoT based on the computing power of an agent. The mechanism is also truth-telling, i.e., agents truthfully reveal their computing power to the principal.

*Remarks:* Approving tip transactions takes finite time and leads to delay, i.e., transaction entering Tangle at time  $t$  is available as a tip transaction at time  $t + h$ ,  $h \geq 1$ . In this paper, we assume a constant delay  $h = 1$  for simplicity. The choice of  $h$  does not affect the transaction rate control problem. It only affects the dynamics of Tangle.

## 2.2 PAP approach to the transaction rate control problem in Tangle

Our PAP formulation of the transaction rate control problem in Tangle is constructed as follows:

$$\text{PAP} = \begin{cases} \text{Principal} & = \text{Transaction rate controller} \\ \text{Agents} & = \text{Users (devices) adding transactions in Tangle} \end{cases} \quad (1)$$

Consider a time-evolving Tangle where multiple agents (IoT devices) add new transactions into the distributed ledger as shown in Fig. 2. Agents are heterogeneous, i.e., agents have different computing power.

Let  $x \in X := \{1, 2, \dots, n\}$  denote the computing power of an agent. Let  $N$  denote the number of agents, and let  $p(x)$  denote the fraction of agents having computing power  $x$ . We define the probability vector  $p \in \mathbb{R}^n$  as:

$$p = [p(1), p(2), \dots, p(n)] \quad (2)$$

To add a new transaction in Tangle, agents have to satisfy the PoW requirement by solving a hash puzzle: search for a nonce [20] that results in hash code starting with a desired number of zeros. The more difficult the puzzle, the longer it takes for an agent to solve it. Hence, to control the rate of new transactions in Tangle, the principal (transaction rate controller) adjusts the PoW difficulty level for each agent. Let  $d(x) \in D := \{1, 2, \dots, m\}$  denotes the PoW difficulty level assigned to an agent with computing power  $x$ . We define the PoW difficulty vector  $d \in D^n$  as:

$$d = [d(1), d(2), \dots, d(n)] \quad (3)$$

The PoW difficulty level  $d(x)$  corresponds to the number of zeros required at the beginning of the hash code. Higher difficulty decreases the rate at which an agent can add new transactions to the distributed ledger. To compensate for the agent's PoW, the principal assigns a WoT  $w(x) \in W :=$

<sup>3</sup>Solving the hash puzzle for PoW takes a finite time. Hence, an agent's rate of new transactions is restricted through PoW.

<sup>4</sup>To tamper with a transaction, a malicious entity would need to re-solve the hash puzzle for that transaction and also for all future transactions that approve it. This is because a solution of the hash puzzle of a transaction depends on the hash of the previous transactions

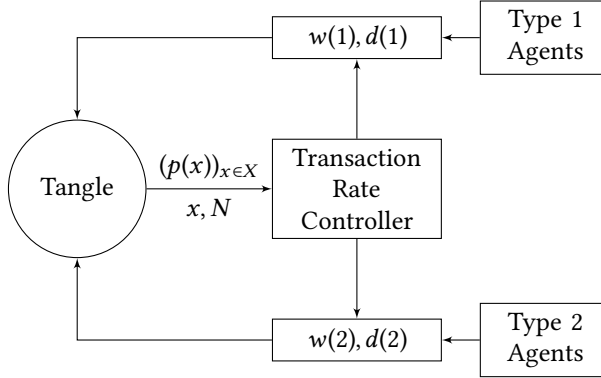


Fig. 2. Block diagram for our proposed transaction rate control mechanism in Tangle. For simplicity, the block diagram illustrates the case when the different types of agents  $X$  are equal to 2. Here, agents' type refers to their computing power. The transaction rate controller block receives the fraction of different types of agents  $(p(x))_{x \in X}$ ,  $x$ , total agents  $N$  from Tangle as an input. The controller then assigns a difficulty level of PoW  $d(x)$  to each agent depending on its type  $x \in X$ . To compensate the PoW, new transactions created by the agent are given a weight  $w(x)$ . New transactions are part of the set of tip transactions. Having a higher weight increases the chance of a tip transaction being selected for approval by other transactions.

$[1, \infty)$  to the transaction added by an agent with computing power  $x$ . We define the WoT vector  $w \in W^n$  as:

$$w = [w(1), w(2), \dots, w(n)] \quad (4)$$

Every new transaction must approve two existing tip transactions (transactions with no incoming edges) to join Tangle. In the random tip selection strategy [21], the two tip transactions for approval are chosen randomly with a probability proportional to the weight of a tip transaction. Hence, the higher the weight of a tip transaction, the faster it gets selected for approval by others on average.

### Utility function for IoT devices (agents)

We consider the following general structure of a utility function for an agent with computing power  $x$ :

$$u(w(x), d(x), x) := w(x) - g(d(x), x) \quad (5)$$

Here,  $d, w$  are defined in (3) and (4), respectively. If the WoT  $w(x)$  is large, the tip transaction gets quickly approved by new transactions. Hence, agents prefer a higher WoT  $w(x)$ . Here, the increasing function  $g(\cdot)$  models the associated cost for an agent to satisfy the PoW requirement. If the PoW difficulty level is high, the agent has to spend large computing power to satisfy the PoW requirement. Hence, agents prefer low effort  $d(x)$ . Moreover, we assume that  $g_d(\cdot)$  is decreasing in  $x$ . This models that the marginal cost due to increase in PoW difficulty level decreases with computing power  $x$ .

### Formulation of a PAP for the transaction rate control in Tangle

In our formulation, we assume that the computing power of agents is known to the principal. Still, the computing power of agents is unobserved<sup>5</sup> by the principal (transaction rate controller).

<sup>5</sup>The computing power of an agent is typically estimated by the number of transactions added by an agent in the recent history [22]. It may not be possible to estimate the computing power for IoT applications. This is because IoT devices

Therefore, the principal has to design a truth-telling mechanism that maximizes its utility. To control the rate of new transactions, the principal solves the PAP (6) to assign PoW difficulty levels  $d(x)$  to different agents, and WoT  $w(x)$  for the transactions added by them into Tangle. The incentive constraints ensure that agents truthfully choose the PoW assigned for their computing power  $x$ .

The PAP for transaction rate control is the following constrained optimization problem:

$$\min_{\substack{d, w, \\ \forall x \in X}} f(x, d, w, p, N) \quad (6a)$$

$$\text{s.t. } x = \arg \max_{\bar{x} \in X} u(w(x), d(x), x), \forall x \in X \quad (6b)$$

$$u(w(x), d(x), x) \geq u_0, \forall x \in X \quad (6c)$$

Here,  $x$  is the computing power of an agent.  $p, d, w$  are defined in (2), (3) and (4), respectively.  $N$  is the total number of agents.  $u_0$  is the base utility level of agents; if the utility is above  $u_0$ , agents are willing to participate in the distributed ledger; otherwise, agents would opt out, i.e., they would not use Tangle to store their transactions.  $f(\cdot)$  is a fairness function used by the principal for transaction rate control.  $u(\cdot)$  is defined in (5). (6b) is known as incentive constraint for the transaction rate control problem; it ensures that agents are truthful. (6c) is known as participation constraint; it guarantees a base utility level for all agents.

### Structure of transaction rate control problem in Tangle

The PAP (6) is a mixed-integer optimization problem. It has useful structure: the optimal solution of the PAP (6) is increasing in computing power  $x$ ; we would discuss these results in Sec.3. The structural result reduces the computation cost for solving the transaction rate control problem. Moreover, we derive the structural results only using the incentive constraints (6b), which are a function of the utility of agents (5). This allows the principal to choose different fairness measures  $f$  in the PAP (6) for controlling the transaction rate in Tangle. Thus the results in this paper apply to a large class of fairness measures for the transaction rate control problem in Tangle.

### Implementation of the transaction rate control problem in Tangle

The PAP (6) is a mixed-integer optimization problem. The principal first solves the PAP (6) to obtain the optimal WoT  $w^*(x)$  for each possible choice of effort  $d \in D^n$  (defined in (3)). For a fixed effort  $d$ , the PAP is a continuous optimization problem; it can be solved efficiently using standard solvers. Our model is suitable for consortium distributed ledgers [7]: a hybrid of public and private distributed ledgers. This is because it can be computationally intensive for IoT devices to solve the PAP (6). In a consortium distributed ledger, a single private agent can be the transaction rate controller (principal). Here, the private agent could be the secure facilitator of the distributed

---

are not dedicated miners. Hence, they need not add new transactions at the maximum possible rate; IoT devices could be switching between multiple tasks or could be in standby mode. Our approach is for the transaction rate controller (principal) to incentivize agents to report their computing power truthfully. Truth-telling is ensured through incentive constraints (6b) of the PAP.

ledger with higher computing power<sup>6</sup>. Moreover, the transaction rate controller can use structural results (discussed in Sec.3) to solve the PAP (6) approximately.

### Truth-telling and implications for Tangle

The incentive constraint (6b) ensures that the mechanism is truth-telling<sup>7</sup>. This is achieved by maximizing the utility of each agent when they perform PoW assigned for their computing power. If (6b) is omitted, agents can increase their utility by choosing a PoW difficulty level assigned for different computing power. In such a case, the actual transaction rate can exceed the optimal transaction rate solved by the principal. This can lead to network congestion and delay broadcasting new transactions among all agents. Therefore, (6b) ensures that an agent with computing power  $x$  will be worse off in terms of its preference for PoW and WoT if it doesn't tell truth, i.e.,  $u(d(x), w(x), x)$  is better than  $u(d(\bar{x}), w(\bar{x}), x)$ .

*Summary.* This section formulated the transaction rate control problem in Tangle as the PAP (6); it is a mixed-integer optimization problem. In Sec.3, we will exploit the structure of the PAP to formulate a mixed-integer optimization problem of smaller dimensions.

## 3 STRUCTURAL ANALYSIS OF THE TRANSACTION RATE CONTROL PROBLEM

In the previous section, we formulated the PAP (6) for the transaction rate control problem in Tangle. The PAP (6) is a mixed-integer optimization problem; the principal can obtain the optimal solution by solving  $m^n$  continuous optimization problems for each possible values of PoW difficulty vector  $d$  (defined in (3)). Moreover, the search space for each continuous optimization problem is in  $\mathbb{R}^n$ . We present two structural results on the optimal solution of the PAP (6). These structural results guarantee that the optimal WoT  $w^*(x)$  and the optimal PoW difficulty level  $d^*(x)$  are increasing in computing power  $x$ . The structural results can be used to decrease the computation cost of solving the PAP (6).

Our first result deals with the structure of the optimal PoW difficulty level  $d^*(x)$  assigned to an agent with computing power  $x$ . We show that the optimal PoW difficulty level  $d^*(x)$  is non-decreasing in  $x$ . Moreover, we derive the structural result only using the incentive constraints (6b), which are a function of the utility of agents (5). This allows the principal to choose different fairness measures  $f$  in the PAP (6) for controlling the transaction rate in Tangle.

**THEOREM 1.** *The optimal PoW difficulty level  $d^*(x)$  assigned to an agent with computing power  $x$  by the PAP (6) to control transaction rate is increasing in  $x$ . For the PAP (6), this reduces the search-space for PoW difficulty vector  $d^*$  (defined in (3)) from  $m^n$  to  $\sum_{i=1}^m \binom{n}{i} \binom{m}{i}$ . Moreover, this result holds for any fairness measure  $f$  in the objective (6a).*

**PROOF.**

Consider computing power  $x, \bar{x} \in X$  s.t.  $x < \bar{x}$ . Constraints (8b) imply

$$w(x) - g(d(x), x) \geq w(\bar{x}) - g(d(\bar{x}), x), \quad \text{and} \quad -(w(x) - g(d(x), \bar{x})) \geq -(w(\bar{x}) - g(d(\bar{x}), \bar{x}))$$

Adding above two inequalities yields  $g(d(x), x) - g(d(\bar{x}), x) \leq g(d(x), \bar{x}) - g(d(\bar{x}), \bar{x})$

<sup>6</sup>Our proposed transaction rate controller is compatible with the IEEE standard 2144.1-2020 [1]: a framework for blockchain-based data management for IoT applications. The IEEE standard 2144.1-2020 identifies the following stakeholders for a typical IoT data collaborative ecosystem: data owners, data consumers, service providers, regulators/policymakers and other stakeholders. According to IEEE standard 2144.1-2020, our proposed transaction rate controller can be viewed as a regulator/policy maker with significantly higher computing power. IoT devices with limited computing power can be categorized as data owners who add transactions in Tangle.

<sup>7</sup>The proposed transaction rate control mechanism does not prevent agents from colluding, i.e., it may be advantageous for two agents to combine their computing power and act as a single agent. Preventing malicious collusion of agents is a subject of future work.



As  $g_d(\cdot)$  is decreasing in  $x$ , last inequality implies  $d(x) \leq d(\bar{x})$

□

The formulation in Sec.2 required the principal (transaction rate controller) to solve  $m^n$  continuous optimization problems corresponding to each possible value of PoW difficulty vector  $d \in D^n$  (defined in (3)). By using the structural result in Theorem 1, we can significantly reduce the number of continuous optimization problems to be solved by the principal. Specifically, Theorem 1 ensures that the principal has to solve continuous optimization problems obtained by fixing PoW difficulty vector  $d$  (3) in the PAP (6) that satisfy  $d(i) \leq d(j), \forall i < j$ . This implies that the number of continuous optimization problems to be solved by the transaction rate controller is reduced from  $m^n$  to  $\sum_{i=1}^m \binom{n}{i} \binom{m}{i}$ .

Our second result deals with the structure of the WoT  $w^*(x)$  assigned to an agent with computing power  $x$ . We show that  $w^*(x)$  is non-decreasing in  $x$ . Moreover, we derive the structural result only using the incentive constraints (6b), which are a function of the utility of agents (5). This allows the principal to choose different fairness measures  $f$  in the PAP (6) for controlling the transaction rate in Tangle.

**THEOREM 2.** *The optimal WoT  $w^*(x)$  assigned to an agent with computing power  $x$  by the PAP (6) to control transaction rate is increasing in  $x$ . Hence, for the PAP (6), we can obtain a constrained optimal WoT vector  $w^*$  (defined in (4)) within a class of increasing functions at a reduced computation cost. Moreover, this result holds for any fairness measure  $f$  in the objective (6a).*

PROOF.

Consider computing power  $x, \bar{x} \in X$  s.t.  $x < \bar{x}$ . Constraints (8b) imply

$$w(x) - g(d(x), x) \geq w(\bar{x}) - g(d(\bar{x}), x)$$

Using Theorem 1 and  $g(\cdot)$  is increasing in effort  $d$  imply

$$w(\bar{x}) - w(x) \geq g(d(\bar{x}), \bar{x}) - g(d(x), \bar{x}) \geq 0 \Rightarrow w(x) \leq w(\bar{x})$$

□

Theorem 2 can be used to parametrize the WoT  $w(x)$  within the class of increasing functions in the PAP (6). For example, we can solve for an optimal  $w^*(x)$  within the class of increasing affine functions of  $x$ . This decreases the dimension of the search space from  $\mathbb{R}^n$  to  $\mathbb{R}^2$  and provides a constrained optimal solution (constrained to affine increasing functions) at a reduced computation cost.

To summarize, we presented two structural results on the solution of the transaction rate control problem (6) in Tangle. The first result guarantees the monotonicity of the optimal PoW difficulty level  $d^*(x)$  in computing power  $x$ . It helps reduce the number of linear programs the principal has to solve for the transaction rate control problem (6) in Tangle. The second result guarantees the monotonicity of the optimal WoT  $w^*(x)$  in computing power  $x$ . This facilitates the principal to parametrize  $w(x)$  within a class of increasing functions and obtain a constrained optimal solution at a low computational cost.

#### 4 NUMERICAL RESULTS. TRANSACTION RATE CONTROL IN TANGLE

This section illustrates, via numerical examples, our proposed transaction rate control mechanism for Tangle. We first specify the model parameters and solve the transaction rate control problem (6). Later, we utilize the solution of the PAP (6) to simulate the dynamics of an actual Tangle and study the impact of our proposed transaction rate control mechanism on the average approval time of tip transactions. The main takeaway from the simulations are: 1) agents with lower computing

power are assigned lower PoW difficulty levels at the cost of a larger average approval time of their transactions, 2) the fixed transaction control in [21] where WoT is a linear function of PoW cannot incentivize agents with higher computing power to do a difficult PoW. To incentivize a difficult PoW, the marginal increase in WoT should increase in PoW difficulty level.

### Model for the transaction rate control problem in Tangle

For a demonstration of our model, we work with a specific choice of utility function (5) for agents:

$$u(w(x), d(x), x) := \beta w(x) - \frac{\exp(d(x))}{x} \quad (7)$$

Here,  $\beta \in \mathbb{R}^+$  is a parameter that tunes agents' preference between WoT and PoW. The first term  $\beta w(x)$  models agents' preference for higher WoT, and the second term  $\frac{\exp(d(x))}{x}$  models preference for low PoW  $d(x)$  by agents. First term  $\beta w(x)$  is linear in WoT as the probability of selection of tip nodes for approval is directly proportional to WoT (see Tangle protocol in Sec.2.1). Rate of new transaction  $\frac{x}{\exp d(x)}$  is an increasing function of the computing power  $x$ ; it decreases as exponential of the PoW difficulty level  $d(x)$ . This is because PoW difficulty  $d(x)$  corresponds to a search for hash code starting with  $d(x)$  number of zeros. Assuming each hash code is equally probable, the probability of finding a hash code starting with  $d(x)$  number of zeros decreases exponentially with  $d(x)$ . Hence, the cost is an exponential function of  $d(x)$ .

For simulations, we use the following PAP for the transaction control problem in Tangle with utility function for agents defined in (7):

$$\min_{\substack{d(x) \in D, \\ w(x) \in W, \\ \forall x \in X, \\ w(1)=1}} \sum_{x \in X} p(x) [N R(x, x) + \alpha w(x)] \quad (8a)$$

$$\text{s.t. } x = \arg \max_{\bar{x} \in X} \beta w(\bar{x}) - \frac{1}{R(x, \bar{x})}, \forall x \in X \quad (8b)$$

$$\beta w(x) - \frac{1}{R(x, \bar{x})} \geq u_0, \forall x \in X \quad (8c)$$

where,

$$R(x, \bar{x}) := \frac{x}{\exp(d(\bar{x}))} \quad (8d)$$

Here, the non-negative parameter  $\alpha \in \mathbb{R}^+$  tunes the fairness measure in objective (8a) The objective function (8a) ensures a trade-off between the rate of new transactions and WoT assigned to different agents.  $R(x, \bar{x})$  denotes the rate at which an agent with computing power  $x$  can add new transactions if it claims its computing power to be  $\bar{x}$ . The first term  $NR(x, x)$  controls the rate of new transactions by adjusting the PoW difficulty level for each agent. This assumes that agents are truthful; truth-telling is ensured through incentive constraint (8b) (discussed later). The rate of new transactions is directly proportional to the number of agents  $N$  and the computing power  $x$  available to them. It is inversely proportional to the exponential of PoW difficulty level  $d(x)$ . This is because PoW difficulty  $d(x)$  corresponds to a search for hash code starting with  $d(x)$  number of zeros. Assuming each hash code is equally probable to occur, the probability of finding a hash code starting with  $d(x)$  number of zeros is proportional to  $\frac{x}{d(x)}$ . Therefore, minimizing the first term assigns higher PoW to agents and controls transaction rate. Minimizing the second term  $\alpha w(x)$  ensures that agents are assigned similar WoT. This ensures fairness amongst agents with different computing power. This is because the probability of a tip transaction being selected for approval by a new transaction is proportional to its WoT (see Tangle protocol in Sec.2.1). Hence,  $w(x)$  affects

Table 1. Simulation Parameters for Transaction Rate control Problem (8)

Parameters	Eq.	Value
$X$	(8a)	$\{1, 3, 10\}$
$D$	(8a)	$\{1, 2, \dots, 12\}$
$p = (p(x))_{x \in X}$	(8a)	$[1/3 \ 1/3 \ 1/3]$
$\alpha$	(8a)	0.1
$\beta$	(8b)	80
$u_0$	(8c)	10

the average time before a tip transaction gets approved. As the importance of WoT is only relative, we normalize the WoT with respect to the WoT of the agent with the smallest computing power. This is achieved by adding a constraint  $w(1) = 1$ . The participation constraint (8c) guarantees a base utility level for all agents; otherwise, agents would opt out of the distributed ledger, i.e., they would not use Tangle to store their transactions.

### Simulation setup for the transaction rate control in Tangle

The PAP (6) is a mixed-integer optimization problem. For a fixed effort  $d$  (defined in (3)), the PAP (8) is a linear optimization program and can be solved efficiently using standard solvers. The principal chooses the optimal PoW difficulty level  $d^* \in D^n$  that maximizes its utility. We implement the PAP (8) in MATLAB and use the inbuilt optimization toolbox to obtain the optimal WoT vector  $w$  (defined in (4)) and the optimal PoW vector  $d$  (defined in (3)). We also simulate the dynamics of Tangle [21] (see Sec.2.1 for the Tangle protocol) in MATLAB and compute the average approval time of transactions.

We begin with a simulation of the PAP (8) to compute the optimal PoW difficulty level and WoT for agents. The model parameters are listed in Table 1. We solve the PAP (8) for four different values of the number of agents  $N$ . As the PoW difficulty level exponentially affects the objective function (8a), we simulate for  $N = \{100, 1000, 10000, 100000\}$  to observe a noticeable change in PoW difficulty level. The chosen number of agents  $N$  is large enough to model a realistic scenario. We use Theorem 1 to reduce the search space for the PoW vector  $d$  (defined in (3)). Specifically, we solve the PAP (8) for those  $d$  that satisfy  $d(i) \leq d(j), \forall i < j$ . We do not use Theorem 2 to parametrize the search space for the WoT vector  $w$  (defined in (4)) and solve the PAP (8) exactly.

### Results and Discussion

Our first simulation evaluates the PoW difficulty level  $d(x)$  assigned to an agent. The optimal PoW difficulty level  $d(x)$  for each agent vs. the number of agents  $N$  is plotted in Fig. 3. For a fixed value of  $N$ ,  $d(x)$  increases with  $x$  (Theorem 1). As  $N$  increases,  $d(x)$  increases for all agents as the transaction rate is directly proportional to  $N$ . Also,  $d(x)$  is a concave function of  $N$ . Therefore, the marginal increase in PoW difficulty level decreases with  $N$ . This implies that our proposed transaction rate control mechanism does not incur a substantial increase in computation cost to agents with an increase in application size (number of agents). Therefore, the transaction rate control mechanism (8) is suitable for IoT applications.

Our next simulation evaluates the WoT  $w(x)$  assigned to an agent. Fig. 4 displays the variation of WoT  $w(x)$  for each agent vs. number of agents  $N$ . The simulation shows that  $w(x)$  increases

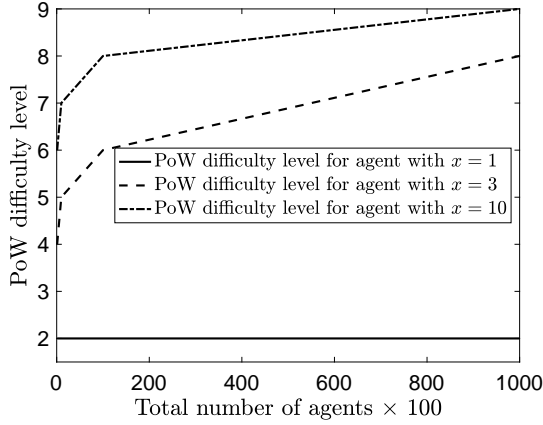


Fig. 3. PoW difficulty level  $d(x)$  vs. number of agents  $N$  for our proposed transaction rate control mechanism (8). As  $N$  increases,  $d(x)$  increases for all agents but the marginal increase in PoW difficulty level decreases with  $N$ . So, our proposed transaction rate control mechanism does not incur a substantial increase in computation cost to agents with an increase in the number of agents.

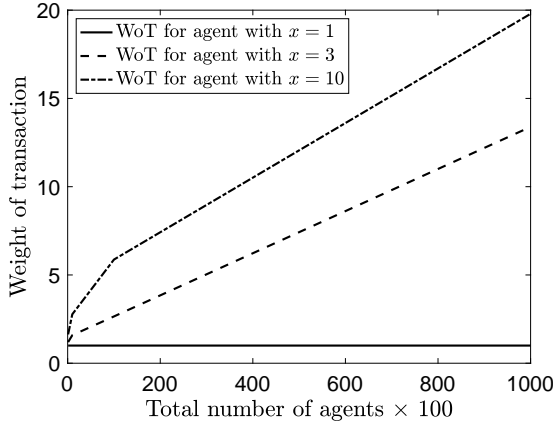


Fig. 4. WoT  $w(x)$  vs. number of agents  $N$  for our proposed transaction rate control mechanism (8). WoT  $w(x)$  increases with  $N$  to compensate for the increase in PoW difficulty level. Marginal increase in WoT decreases with  $N$ . Hence, our proposed transaction rate control mechanism (8) ensures that the relative WoT of agents with small computing power (with respect to the WoT of agents with high computing power) does not degrade rapidly with the number of agents.

with  $x$  (Theorem 2). Moreover, the WoT  $w(x)$  increases with  $N$  to compensate for the increase in PoW difficulty level. Also, the marginal increase in WoT decreases with  $N$ . Hence, our proposed transaction rate control mechanism (8) ensures that the average approval time for agents with small computing power does not degrade rapidly with the number of agents.

We now use the optimal PoW difficulty level  $d^*(x)$  and optimal WoT  $w^*(x)$ , obtained from (8), to simulate the dynamics of Tangle. Tangle protocol and its evolution have been described in Sec. 2.1. At each time  $t$ , new transactions are added by each agent at a rate that depends on their computing power and the PoW difficulty level. Each new transaction chooses two tip transactions randomly for approval; the probability that a tip transaction is selected for approval is proportional to its

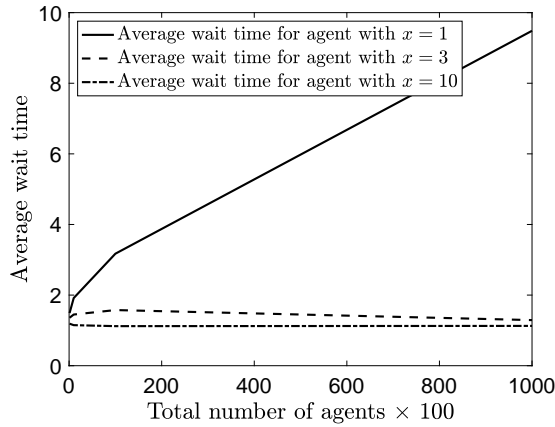


Fig. 5. Average approval time of transactions vs. the number of agents  $N$  for our proposed transaction rate control mechanism solved by the PAP (8). Agents assigned difficult PoW have to wait for a lesser time on average for approval of their tip transactions. This is because they are assigned a higher WoT. Agents assigned lower PoW difficulty levels have to wait for longer on average for approval of their transactions. This is because they are assigned a lower WoT. Compared to the fixed transaction rate control scheme in [21], our proposed transaction rate control mechanism (8) achieves two benefits: (1) it moderates the rate of new transactions and increases the security of Tangle by incentivizing agents with high computing power to perform difficult PoW, (2) it allows agents with lower computing power to perform easier PoW at the expense of larger average approval time of transactions.

weight. As different transactions have different weights, we use the accept-reject method [13] to select tip transactions non-uniformly during simulations. An important parameter associated with the dynamics of Tangle is the average approval time of transactions. The average approval time of a transaction is defined as the time between when a transaction is added to the ledger and when it gets approved by a new transaction. The average approval time of a transaction decreases with the WoT and increases with the transaction rate per number of agents<sup>8</sup>. The probability that a tip transaction is selected for approval at time  $t$  is proportional to the WoT. Therefore, the more the WoT, the higher its chance of being selected for approval. Also, if the PoW difficulty level increases, then the rate of new transactions decreases. Consequently, the number of tip transactions selected for approval also decreases. This leads to an increase in average approval time.

Fig. 5 plots the average time for approval of transactions for each agent vs. the number of agents  $N$ . As  $w(1)$ ,  $d(1)$  remains unchanged with  $N$  (refer Fig. 3 and Fig. 4), the average approval time for the agent with the lowest computing power increase with  $N$ . This is because both the relative WoT (with respect to other agents) decreases, and so does the transaction rate per number of agents. Agents that are assigned difficult PoW have to wait for a lesser amount of time on average for approval of their tip transactions than agents that are assigned easier PoW. As observed in Fig. 5, the average approval time for agents with higher computing power is almost constant because a decrease in the transaction rate per number of agents offsets an increase in relative WoT. Compared to the fixed transaction rate control scheme in [21], our proposed transaction rate control mechanism (8) achieves two benefits: (1) it moderates the rate of new transactions and increases the security of Tangle by incentivizing agents with high computing power to perform difficult

<sup>8</sup>As the number of agents increases, so does the number of tip transactions; therefore, the approval time is an increasing function of the transaction rate divided by the number of agents.

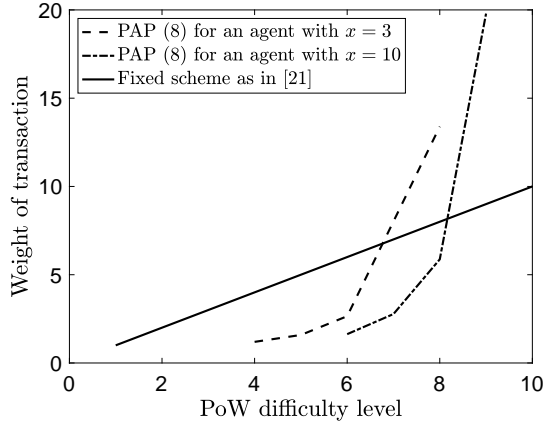


Fig. 6. Comparison of WoT vs. PoW assigned to agents by our proposed transaction rate control mechanism solved by the PAP (8), and the fixed transaction control scheme as in [21]. The fixed scheme in [21] assigns WoT as a linear function of the PoW difficulty level; this does not guarantee that agents will perform a difficult PoW. Our transaction rate control mechanism (8) assigns WoT as a convex function of PoW difficulty level; this incentivizes agents to perform difficult PoW. Transactions with higher PoW difficulty level makes it difficult for an adversary to tamper transactions in Tangle; this makes Tangle more secure.

PoW, (2) it allows agents with lower computing power to perform easier PoW at the expense of a larger average approval time of transactions.

We now compare the proposed transaction rate control mechanism (8) with the fixed transaction control scheme as in [21]: it allocates the WoT as a fixed linear function of the PoW difficulty level. Fig. 6 plots WoT vs. PoW for agents with computing power  $x = 3$  and  $x = 10$  obtained from PAP (8); it is compared with the fixed transaction control scheme as in [21]. The fixed scheme in [21] assigns WoT as a linear function of the PoW difficulty level; this does not guarantee that agents will perform a difficult PoW. Our transaction rate control mechanism (8) assigns WoT as a convex function of PoW difficulty level; this incentivizes agents to perform difficult PoW. Transactions with higher PoW difficulty level makes it difficult for an adversary to tamper with transactions in Tangle; this makes Tangle more secure. Hence, to incentivize difficult PoW, the marginal increase in WoT should increase with the PoW difficulty level.

To summarize, we simulated the PAP (8) for controlling the transaction rate in Tangle. As the PAP (8) is a mixed-integer program, we obtained the optimal solution by solving a set of linear programs. Theorem 1 was exploited to reduce the number of linear programs to be solved. We also simulated the dynamics of Tangle after incorporating the transaction rate control mechanism (8) and compared it with the fixed transaction rate control scheme in [21].

## 5 CONCLUSION AND FUTURE WORK

Tangle is a distributed ledger technology suitable for IoT applications. Motivated by designing strategic contracts with partial information in microeconomics, this paper has proposed a principal-agent problem (PAP) approach to transaction rate control in Tangle. The principal (transaction rate controller) designs a mechanism to assign proof of work (PoW) difficulty level and weight of transaction (WoT) to agents (IoT devices). As the principal cannot observe agents' state (computing power), the principal also has to incentivize agents to be truthful. Our main results regarding the proposed transaction rate controller were the following: 1) the optimal PoW difficulty level increases with the computing power of the agents; 2) the optimal WoT increases with the computing

power of the agent. We also simulated the dynamics of Tangle using the solution obtained from our proposed transaction rate control mechanism. We observed that agents with higher computing power are assigned higher PoW difficulty levels but have a smaller average transaction approval time than agents with lower computing power. As the mechanism is truth-telling, it incentivizes agents with higher computing power to perform a difficult PoW; this makes Tangle more secure. Finally, we compared the proposed mechanism with the transaction rate control scheme from the white paper on Tangle [21]; we observed that a concave relation between WoT and PoW is required to incentivize the agents to be truthful.

Our transaction control mechanism ensures that agents are truth-telling. Still, it does not prevent agents from colluding, i.e., it may be advantageous for multiple agents to combine their computing power and act as a single agent. It would, therefore, be interesting to study the rate control problem that disincentivizes agents from forming coalitions. This is essential from the security viewpoint, as collusion of agents can lead to a majority attack on distributed ledgers.

## ACKNOWLEDGMENTS

This research was supported in part by the U.S. Army Research Office grant W911NF-21-1-0093, National Science Foundation grant CCF-2112457, and Air Force Office of Scientific Research grant FA9550-22-1-0016.

## REFERENCES

- [1] 2021. IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management. *IEEE Std 2144.1-2020* (2021), 1–20. <https://doi.org/10.1109/IEEESTD.2021.9329260>
- [2] E. Altman, D. Menasché, A. Reiffers-Masson, M. Datar, S. Dhamal, C. Touati, and R. El-Azouzi. 2020. Blockchain competition between miners: a game theoretic perspective. *Frontiers in Blockchain* (2020), 26.
- [3] F. M. Benčić and I. P. Žarko. 2018. Distributed ledger technology: Blockchain compared to directed acyclic graph. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 1569–1570.
- [4] D. Bertsekas. 2015. *Convex optimization algorithms*. Athena Scientific.
- [5] A. Cullen, P. Ferraro, W. Sanders, L. Vigneri, and R. Shorten. 2021. Access Control for Distributed Ledgers in the Internet of Things: A Networking Approach. *IEEE Internet of Things Journal* (2021), 1–1. <https://doi.org/10.1109/JIOT.2021.3096129>
- [6] L. Da Xu, W. He, and S. Li. 2014. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics* 10, 4 (2014), 2233–2243.
- [7] O. Dib, K-L Brousmiche, A. Durand, E. Thea, and E. B. Hamida. 2018. Consortium blockchains: Overview, applications and challenges. *International Journal On Advances in Telecommunications* 11, 1&2 (2018), 51–64.
- [8] C. Dwork and A. Roth. 2014. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science* 9, 3-4 (2014), 211–407. <http://dblp.uni-trier.de/db/journals/ftcs/ftcs9.html#DworkR14>
- [9] A. Farrokh and V. Krishnamurthy. 2006. Opportunistic scheduling for streaming multimedia users in high-speed downlink packet access (HSDPA). *IEEE Transactions on Multimedia* 8, 4 (2006), 844–855. <https://doi.org/10.1109/TMM.2006.876227>
- [10] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert. 2017. The immutability concept of blockchains and benefits of early standardization. In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. 1–8. <https://doi.org/10.23919/ITU-WT.2017.8247004>
- [11] M. Jay, A. Mollard, Y. Sun, R. Zheng, I. Amigo, A. Reiffers-Masson, and S. Ruano Rincón. 2021. Utility maximisation in the Coordinator-less IOTA Tangle. (2021), 93–104.
- [12] D. Kraft. 2016. Difficulty control for blockchain-based consensus systems. *Peer-to-peer Networking and Applications* 9, 2 (2016), 397–413.
- [13] V. Krishnamurthy. 2016. *Partially Observed Markov Decision Processes: From Filtering to Controlled Sensing*. Cambridge University Press.
- [14] S. Kumar, P. Tiwari, and M. Zymbler. 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data* 6, 1 (2019), 1–21.
- [15] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu. 2020. Direct Acyclic Graph-Based Ledger for Internet of Things: Performance and Security Analysis. *IEEE/ACM Transactions on Networking* 28, 4 (2020), 1643–1656. <https://doi.org/10.1109/TNET.2020.2991994>

- [16] X. Liu, E. K. P. Chong, and N. B. Shroff. 2001. Opportunistic transmission scheduling with resource-sharing constraints in wireless networks. *IEEE Journal on Selected Areas in Communications* 19, 10 (2001), 2053–2064.
- [17] A. Mas-Colell, M. D. Whinston, and J. R. Green. 1995. *Microeconomic theory*. Oxford University Press.
- [18] D. Meshkov, A. Chepurnoy, and M. Jansen. 2017. Short paper: Revisiting difficulty control for blockchain systems. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 429–436.
- [19] G. J. Miller. 2005. *Solutions to Principal-Agent Problems in Firms*. Springer US, Boston, MA. [https://doi.org/10.1007/0-387-25092-1\\_15](https://doi.org/10.1007/0-387-25092-1_15)
- [20] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.
- [21] S. Popov. 2018. The tangle. *White paper* 1, 3 (2018).
- [22] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer, O. Saa, W. Sanders, L. Vigneri, W. Welz, and V. Attias. 2020. The coordicide. *Accessed Jan* (2020), 1–30.
- [23] M. Vera-Hernández. 2003. Structural Estimation of a Principal-Agent Model: Moral Hazard in Medical Insurance. *The RAND Journal of Economics* 34, 4 (2003), 670–693. <http://www.jstor.org/stable/1593783>
- [24] L. Vigneri, W. Welz, A. Gal, and V. Dimitrov. 2019. Achieving Fairness in the Tangle through an Adaptive Rate Control Algorithm. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 146–148. <https://doi.org/10.1109/BLOC.2019.8751358>
- [25] M. F. Zia, M. Benbouzid, E. Elbouchikhi, S. M. Muyeen, K. Techato, and J. M. Guerrero. 2020. Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis. *Ieee Access* 8 (2020), 19410–19432.