On the Fairness of Distributed Ledger Technologies for the Internet of Things

Luigi Vigneri*, Wolfgang Welz†
IOTA Foundation
10405 Berlin, Germany
Email: *luigi.vigneri@iota.org, †wolfgang.welz@iota.org

***Abstract*—Distributed networks have been widely studied in literature. However, the blockchain paradigm has inspired to revisit some of the results under a different point of view. In this paper, we analyze the "classic" spam protection problem applied to the IOTA Tangle, a distributed ledger technology which addresses Bitcoin's (monetary and energy) efficiency issues through the absence of mining pools. However, the lack of miners makes the network vulnerable to denial of service attacks. We propose an anti spam mechanism based on the solution of a cryptographic puzzle: When a node wants to generate a new transaction, it dynamically adapts the difficulty of the puzzle depending on its target throughput and on its reputation score. Specifically, the adaptive difficulty property guarantees that any node, even with low hashing power, can achieve similar throughput for a given reputation. In the paper, we prove this claim both analytically and through simulations, and we show that fairness between low- and high-power nodes is indeed reached.**

I. Introduction

The recent blockchain paradigm [1] started a revolution in the world of distributed systems. Since Bitcoin-like blockchains often lack efficiency (Bitcoin achieves a maximum throughput of only seven transactions per second [2]), alternative proposals have recently come up: among those, the *Tangle* [3], a data structure for storing transactions developed by IOTA [4], breaks the original distinction between miners and users in order to build a feeless protocol which can be used as the backbone for the Internet of Things (IoT).

For distributed ledger technologies, well studied networking problems need to be revisited under a different point of view. In this work, we consider spam attacks: While the introduction of small fees usually mitigates this problem, the IOTA Tangle is specifically designed to be used in the context of the IoT where fees would disable micro and data transactions. Unlike Bitcoin, where a built-in rate limit is enforced by the mining difficulty adjustment and the transaction fees [1], for the Tangle an explicit rate control mechanism becomes necessary. In the current implementation, users wanting to issue a new transaction are asked to solve the Proof of Work[1] (PoW) [5]. Due to the parallelizable nature of PoW, an attacker could use specialized hardware (e.g., FPGA or ASIC) to solve the PoW fast enough to flood the network with thousands of spam transactions. This is clearly problematic as it not only leads to network congestion, but also disables the IoT use case since IoT devices cannot keep up with such specialized hardware. Driven by the IoT world, we define *fairness* as the ability of nodes to issue valid transactions at a rate *independent* on their computational capabilities. In the next sections, we propose an anti spam mechanism which satisfies the aforementioned fairness criterion.

[1]We highlight that the PoW is only computed as an anti-spam mechanism, and it does not affect the consensus layer.

II. System model

We consider a network composed of users that transfer data or tokens to each other via *transactions*. When a user decides to issue a transaction, they perform the following actions:

- *Vouching for the validity of two existing transactions* to keep the network secure. A transaction is valid, if the funds spent are actually owned by the sender. This process of approving two transactions with each issued transaction generates a directed acyclic graph, the *Tangle*, where vertices represent transactions and edges represent the approval relations. For further information, we refer the interested reader to [3].
- *Solving the difficult to compute PoW*, that is yet easy to check by the other network participants. This work can have different degrees of difficulty where the actual required computation time is exponential with the difficulty level: it triples with every step in the IOTA protocol. Adapting the difficulty of the PoW across the various nodes of the network is the focus of the next section.
- *Adding its global identifier* to the transaction and signing everything to ensure authenticity.

In our model we make a partial synchronicity assumption, where we assume that nodes have bounded shifts between their clocks and that a transaction takes a known, bounded time h to be propagated to all network participants.

III. Adaptive rate control

The rate control relies on the following global parameters:

- *Base difficulty* d_0. It sets the minimum difficulty of the PoW.
- *Adaptation rate* $\gamma \in [0, 1]$. It provides the rate at which difficulty is adjusted.
- *Time window* $w > 0$. This parameter defines the granularity of the algorithm, and describes the width of the time interval considered by the algorithm.

At time t, node n must perform PoW with difficulty $d_n(t)$, which can be calculated by the following:

$$d_n(t) = d_0 + \lfloor \gamma \cdot r_n(t) \rfloor , \tag{1}$$

where $r_n(t)$ represents the number of transactions issued by node n in the time interval $[t-w, t]$.

When a node n receives a transaction, it must check that PoW with an appropriate difficulty was performed. Let us assume we receive a transaction with difficulty d issued by node n. To decide whether this transaction should be forwarded or not, a node counts how many transactions $r_n(t)$ issued by n it has received in the last w seconds. In accordance to the formula given by Eq. (1), the node forwards the transaction only if the following condition is satisfied:

$$d \geq d_0 + \lfloor \gamma \cdot r_n(t) \rfloor$$

For the sake of simplicity, we assume that incoming transactions are checked in the same order as they are issued by the sending node. As the expected time needed to perform the PoW is typically larger than the network latency h, this is a reasonable assumption.

Theorem 1. *When the adaptive rate control algorithm according to Eq.* (1) *is applied, a node can generate a throughput of at most*

$$\theta \leq \frac{\log_3\left(\frac{\gamma \cdot w}{b} \cdot \mu\right)}{\gamma \cdot w}, \tag{2}$$

where μ is the node's computational capability in operations per second and b is the mean number of operations needed to solve the PoW at difficulty 0*.*

Proof for $\gamma = 1$.

$$\mu w \geq b \cdot 3^{d_0} + b \cdot 3^{d_0+1} + \ldots + b \cdot 3^{d_0+n} = b \cdot \frac{3^{d_0+n} - 1}{3^{d_0} - 1}$$

$$n \leq \log_3\left(\frac{w}{b} \cdot \mu\right)$$

For the throughput $\theta = \frac{n}{w}$, we then have $\theta \leq \frac{\log_3\left(\frac{w}{b} \cdot \mu\right)}{w}$. □

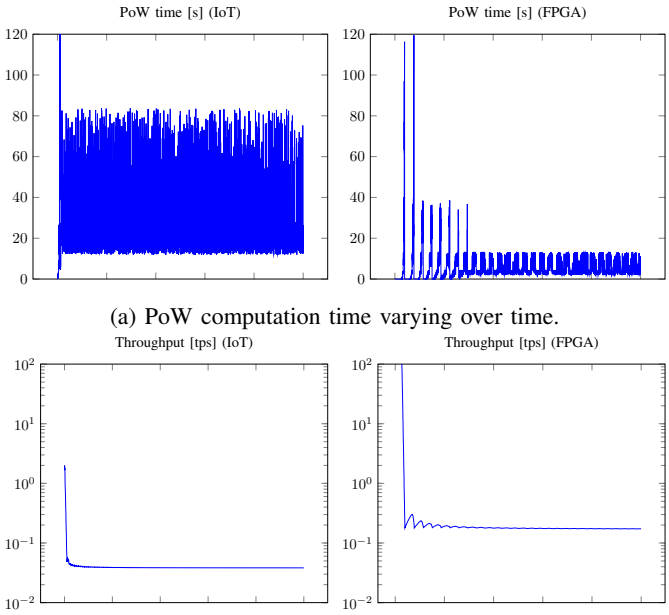
This shows that the allowed transaction rates are within the same order of magnitude, even for nodes whose computational abilities differ by orders of magnitude.

In the adaptive rate control, the node n issuing a transaction unforgeably adds its unique identifier to it. This way, any participating node can determine the number of transactions $r_n(t)$ issued by n. While this is an integral component of the rate control algorithm, it also makes the system susceptible to Sybil attacks [6], where a malicious entity masquerades many counterfeit identities and uses them to gain a disproportionately large influence on the network.

To make such an attack harder we propose to use a stake-based reputation system [7]: With each transaction, the issuer can specify which node's reputation in the network should increase by an amount equivalent to tokens transferred. This leads to a system in which users, can reward certain nodes in the network of their choosing.

IV. Simulations

To empirically validate the results of Theorem 1, we built a Python simulator. In these simulations, we evaluate the maximum throughput of a single node which can be a IoT device ($\mu = 10^{-1} \times 10^6$) or an FPGA ($\mu = 10^6 \times 10^6$).



(a) PoW computation time varying over time.

(b) Throughput (in transactions per second) over time.

Fig. 1: Adaptive rate control

Furthermore, we assume that the number of operations needed to solve the PoW at difficulty 14 is a random variable uniformly distributed with mean $3^{14} \approx 5 \times 10^6$. Finally, we set the following global parameters: Base difficulty $d_0 = 10$, adaptation rate $\gamma = 0.1$ and time window $w = 1000$ s.

In our simulations, a node aims to issue 5000 in the shortest possible time. In this scenario, the adaptive rate control algorithm makes the PoW difficulty oscillate around a certain max value, depending on the computational capabilities of the particular device. Such a different difficulty mitigates the gap between the solution time for the PoW between the different devices. This is the key principle behind the adaptive PoW algorithm: Make life easy for IoT devices, while bound the power of FPGAs and ASICs (Fig. 1a). Figure 1b shows the fundamental result: The throughput of FPGAs and IoT devices is in the same order of magnitude. This means that even specialized hardware cannot spam the network indefinitely, which validates our findings from Section III.

V. Conclusion

PoW poses an efficient anti spam mechanism. However, as specialised hardware is becoming more widespread, the performance discrepancies compared to smaller IoT devices is several orders of magnitude. In this paper, we presented a rate control algorithm that is feasible for the IoT as well as micro-transaction and showed the efficiency of the algorithm analytically and through a Python simulator.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba *et al.*, "On scaling decentralized blockchains," in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 106–125.
[3] S. Popov, "The Tangle," p. 131, 2016.
[4] IOTA Foundation, "The next generation of distributed ledger technology." [Online]. Available: https://www.iota.org/
[5] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference*. Springer, 1992, pp. 139–147.
[6] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.
[7] IOTA Foundation, "The coordicide," 2019. [Online]. Available: https://files.iota.org/papers/Coordicide_WP.pdf