Lessons learned from evaluating IOTA on Internet of Things devices

Atis E

Follow

--

13

Listen

Share

There are few openly available quantitative results aboutIOTA. Motivated by this fact, we experimented with IOTA on two different IoT devices and two modern desktop and server computers. We found that despite the theoretical scalability of the Tangle, the actual IOTA protocol has relatively high energy consumption. The Proof-of-Work and transaction signing operations are computationally complex relative to the limited capabilities of many IoT devices and and may be impractical on energy-limited / battery-powered devices.

Note: this article uses results from the research paper

[Distributed Ledger Technology and the Internet of Things: A Feasibility Study

](http://user.it.uu.se/~atiel485/iota-iot-2018.pdf), presented in the 1st Workshop on Blockchain-enabled Networked Sensor Systems (BlockSys).

Background

If you're reading this, you probably know thatIOTA is a cryptocurrency that aims to be suitable for IoT applications. In the summer of 2018, I come to realize that despite all the hype there are no publicly available numbers about energy consumption of IOTA operations, nor there are any public studies about the feasibility of IOTA on IoT devices. At the same time, the IOTA security assumptions require a large number of active IoT devices. So, "does it actually work on IoT devices?" is a critical question that should be asked more.

The ledger in IOTA is secured by a heavily distributed form of Proof-of-Work. The state of the ledger is maintained by so-called full nodes. The IoT devices are envisioned to function as light nodes; they are expected connect to the the full nodes, create & sign transactions, and compute a Proof-of-Work in a distributed fashion. The design of IOTA relies on safety in numbers

— the idea that IoT devices can out-compute any computational resources a malicious actor might realistically obtain due to the sheer number of the IoT devices.

The current state of IOTA the cryptocurrency falls short of this vision — the transactions are also validated by centralized Coordinator node(s). If IOTA wants to transition to fully decentralized operation, it needs to remove the Coordinator component. The key question here is "can the network be secured by the Proof-of-Work alone?". More specifically, "can IoT devices provide sufficient distributed Proof-of-Work to secure against centralized attacks?"

IoT devices and Proof-of-Work

IoT devices span a wide spectrum of capabilities. Some of these devices are as powerful than a typical desktop PC (or even more powerful than that). However, they are exceptions. The IOTA Vision states that "the number of connected devices that will be in use is estimated to reach 75 billion by 2025." Cisco promises more than 50 billion connected devices by 2020, Ericsson: 18 billion IoT devices by 2022. However,the vast majority of these are going to be low-power devices

. For example, the number of currently operational low-power embedded microcontrollers is orders of magnitude larger than the number of Raspberry Pi-class IoT devices.

It is extremely unlikely that the billions of connected devices are going to contribute their full computational power to IOTA's Proof-of-Work computations.

Nominal vs. available computational power

Many IoT devices run on batteries or have otherwise limited power sources. Theses devices aren't able to use their nominal computational resources all the time, so they usually perform some kind of duty cycling. A device with nominal

computational power x

only has 0.01x available

computational power if it's operating at 1% duty cycle. A thousand devices with 0.1% duty cycle only have as much available computational power as one equivalent device with 100% duty cycle. To put this in more concrete terms, a single server, on its own 1000x as powerful as the average IoT device, can effectively produce as much Proof-of-Work computations as a million

of these "average" IoT devices working at 0.1% duty cycle.

The limiting factor of these IoT devices is not their nominal computational power; it's their required battery lifetime. It's not the millions of operations per second that matter, it's the energy required for these operations.

What about the IoT devices that don't rely on batteries? Even these devices typically don't have energy available as easily and cheaply as servers and mining farms. The latter two benefit from economies of scale, while IoT devices are usually highly distributed in space, don't have nearby power sources, and don't have their CPUs optimized for Proof-of-Work computations.

Experimental setup

We looked at two IoT devices from two different power classes, and compared them with two modern computers:

- Texas Instruments CC2650 LaunchPad (48 MHz, single core, only 20 kB of RAM and 128 kB of program memory)
- Raspberry Pi Model 3 (1200 MHz, 4 cores)
- Intel Core i7–6700 desktop machine (3400 MHz, 8 cores)
- Intel Xeon E5–2623 server (3000 MHz, 16 cores) with Nvidia Quadro K620.

It's nontrivial to measure the energy consumption on such a diverse set of devices. Besides, directly measuring the energy consumed by the platforms would also include their peripheral components, which are not important for this article— we're primarily interested in the energy consumed by the CPU. So, the methodology we followed was to measure the CPU time required to perform IOTA operations, and then to extrapolate the timing to energy consumption.

Time and energy required for the Proof-of-Work

We used the CCurl implementation by the IOTA Foundation (https://github.com/iotaledger/ccurl). It is implemented in C; however, it's still too heavyweight to run on the TI LaunchPad — the core algorithm uses far too much RAM. We execute it on the three remaining platforms instead.

The results show the time required in seconds (the graph on the left); extrapolating that to energy, we got 54.9 J (joules) for Raspberry Pi, 233.2 J for the Core i7, and 93.5 J for the Nvidia GPU.

The computational power of the TI LauchPad is 10–100 times less than that of Raspberry Pi, depending on the exact workload. Even if the PoW code could run on the TI LauchPad, it would take an hour or so just to compute the PoW for a single transaction. The devices would also run out of battery in a day or a few weeks at most, depending on the capacity of the battery (100 mAh to 2700 mAh, respectively).

Raspberry Pi it itself capable of doing some PoW, but it only can do the PoW for 1000 transactions per day, assuming it's spending 100% CPU resources for the task — so, clearly, it cannot function as a major PoW hub either.

The Core i7 server is only around 20 times faster than the Pi, so, a network of 20 Pi could in theory match the computational power of a single Core i7 server. Still, the Pi's would have several times higher energy consumption.

Also to note, historically the IOTA Tangle often has failed to confirm valid transactions in the first attempt, requiring them to be "reattached" by the user, in some instances for many times. Each "reattach" operation requires a brand-new Proof-of-Work for each reattached transaction.

Outsourcing the Proof-of-Work

There is a potential saving grace: the IOTA protocol allows to outsource the Proof-of-Work computation on external devices. This feature allows to improve the system design via collaboration between IoT devices and dedicated servers. The former have the incentive to do the Proof-of-Work, the latter have the computational resources and energy for efficient computations. However, this scheme can only work if:

1. The IoT device can effectively function as an IOTA wallet, i.e. can create and sign IOTA transactions.
2. The communication overhead between the IoT device and the Proof-of-Work device is low.

Time and energy required for transaction signing and for wireless communications

We used a port of the IOTA Ledger Nano S wallet to the Contiki-NG operating system (see https://github.com/atiselsts/contiki-ng/tree/iota/examples/iota/value-transaction). The port to Contiki-NG only kept the essential algorithms to fit it in the limited RAM and environment of the TI LaunchPad.

The results (on the left) show that it takes 7.7 seconds to sign a single transaction on the TI LaunchPad on the average, which consumes 74 mJ (millijoules) on this platform. For comparison, it requires estimated 82 mJ on Raspberry Pi, 28 mJ on the Core i7 server and 31 mJ on the older-generation Xeon server.

In contrast, it only requires a few mJ to transmit a signed transaction using a one of the several low-power wireless protocol available on the TI LaunchPad (BLE and IEEE 802.15.4). It can be further optimized by transmitting only the essential parts of the transaction to a proxy device, which then fills the rest of the fields of the IOTA transaction's data structure.

Both the PoW and transaction signing have large variance of timing (see the graphs above), making it difficult to quantify the minimal energy budget required to complete an IOTA operation.

What does it all mean? In the paper we conclude that:

Given the energy usage results, it is clear that on battery-powered devices, both PoW and transaction signing are not practical without hardware-accelerated cryptography. More powerful devices such as Raspberry Pi are capable of doing both operations, but instantaneous transactions are beyond their resources.

Overall, IOTA does not feel

like it's designed for light-weight IoT applications. The communication overhead can be optimized by partially replacing the IOTA reference protocol with something more efficient, but even achieving the wallet functionality (i.e. being able to create and sign transactions) is computationally expensive and can take many seconds to complete. Consider an IoT device with a small battery (say, 100 mAh) that produces one IOTA "bundle" per minute, either with two signed transactions or a single signed transaction with two signature message fragments. Such a device is going to last less than 6 days before running out of battery —and that's under the unrealistic assumption that it doesn't do anything else besides signing IOTA transactions!

Discussion

There are two potential objections against the argument that IOTA is not suitable for the majority of IoT devices.

Objection 1. The IOTA hash function can be hardware accelerated, and these accelerators may become commonplace on IoT devices.

It's not clear if this development would significantly change the balance in the total computational power. If Keccak (SHA-3) acceleration becomes commonplace on IoT devices due to some economical incentive, the same economical incentive may also apply to servers. Therefore both next generation servers and next generation IoT devices could be able to the PoW much faster and with lower energy consumption, leaving the overall balance unchanged. At best, this objection reduces the certainty of the argument, but does not refute it.

Objection 2. The results from the current devices are not representative; CPUs of next generation IoT devices may be able to carry orders-of-magnitude more computational operations than the current ones.

This is unlikely to have a large impact on battery lifetimes, unless we find new techniques for computing in much more energy-efficient ways (other than implementing the algorithms in hardware, which was already discussed above).

Instead, a mass transition from battery-powered devices to energy-harvesting devices is currently on the horizon. Only minuscule amounts of energy can be accumulated in ways that are practical on IoT devices (which are mostly located indoors, mostly low-cost, mostly small). Devices that harvest their energy from environmental surroundings (e.g. from WiFi signals, vibrations, thermal couplings, etc.) typically have even more restricted energy budgets than devices powered by batteries.

To sum up, the need to save energy is one of IoT fundamentals; there is no obvious way of getting around it. At least in the near-term future, the majority of IoT devices are going to be stuck with low energy budgets, so their computational capabilities will remain limited. Hence, running any sort of PoW on IoT devices en masse is doubtful.