

LabBitcoin: FPGA IoT Testbed for Bitcoin Experiment with Energy Consumption

Victor T. Hayashi¹, Felipe V. de Almeida¹, Andrea E. Komo¹

¹ Escola Politécnica – Universidade de São Paulo (USP)

{victor.hayashi, felipe.valencia.almeida, andrea.komo}@usp.br

Abstract. *This paper describes a Field Programmable Gate Array (FPGA) testbed that enables Bitcoin experimentation in real-time with energy consumption. The Internet of Things (IoT) infrastructure enables practical activities considering a remote lab paradigm to allow students and enthusiasts to obtain a deep understanding of Blockchain technology, considering higher cognitive domains according to the Bloom taxonomy. The proposed solution is validated with an open-source Bitcoin miner implementation in Verilog, mobile, and web interfaces for energy consumption monitoring. This testbed may be used to foster Verilog design challenges for FPGA devices that provide a suitable solution considering performance and energy consumption metrics.*

1. Introduction

Decentralized systems based on Blockchain are gaining enormous industry and academic interest. The most popular example is cryptocurrency Bitcoin [Nakamoto 2008], which is a peer-to-peer electronic cash system whose network is one of the most powerful distributed computing networks [Oliveira et al. 2012].

A fundamental process used to validate the blocks in Bitcoin is mining. It is based on a consensus algorithm that implies the solution of a mathematical problem by each miner [Rodrigues and Rocha 2020]. For example, a Bitcoin miner spends computing power to solve these cryptography problems for the Proof of Work (PoW) consensus algorithm in exchange for some amount of Bitcoins [Oliveira et al. 2012].

Even though the applications based on Blockchain technology have shown great opportunities, its energy consumption raises concerns that may inhibit disruptive technology adoption, considering an energy consumption of more than 50 TWh per year for Bitcoin [Sedlmeir et al. 2020]. These concerns motivate research regarding a holistic analysis on the matter [Sedlmeir et al. 2020] and minimization of energy losses [Nair et al. 2020].

In this sense, engaging and enabling developers to solve this and other future problems related to Blockchain technology is essential to the wider adoption. One way of achieving this goal is by means of practical activities that motivate and challenge students and enthusiasts. Considering the revised Bloom taxonomy [Krathwohl 2002], the higher cognitive domains such as apply and evaluate may be supported by these activities. A remote lab based on the Internet of Things (IoT) [Hayashi et al. 2020] is one of the infrastructures that enable such practical activities in real-time, with integration with various interfaces such as web and mobile. Bitcoin experimentation might contribute to IoT research because there is an interest of integrating IoT with Blockchain technology [Xu et al. 2020].

Considering the energy consumption concern and the necessary Bitcoin mining, we propose a Field Programmable Gate Array (FPGA) testbed that enables Bitcoin experimentation in real-time with energy consumption. The IoT infrastructure enables practical activities considering a remote lab paradigm to allow students and enthusiasts to obtain a deep understanding of Blockchain technology, considering higher cognitive domains according to the Bloom taxonomy.

This paper is organized as follows: Section 2 describes the LabBitcoin solution with its architecture, building blocks, and a brief discussion on Blockchain usage in the considered scenario. Section 3 follows with a demonstration of the LabBitcoin with a remote lab experiment. Benchmark results are presented in Section 4, and brief comments regarding related work are presented in Section 5. Section 6 concludes the paper with final considerations and directions for future work.

2. LabBitcoin

2.1. Architecture

The architecture of the LabBitcoin is described in Figure 1. The computer, FPGA, and IoT smart meter devices compose a bench in the university lab. The computer is used by the student with remote access to design, compile and deploy Verilog designs on the FPGA board. The FPGA is used to implement the Bitcoin miner, and the IoT Smart Meter is used to monitor energy consumption. An MQTT broker is used to communicate the energy consumption reading from the IoT Smart Meter devices to the Web dashboard and mobile interface. The Web dashboard is integrated with two lab benches in this Proof of Concept (PoC) to show how an FPGA cluster may be monitored from one integrated dashboard.

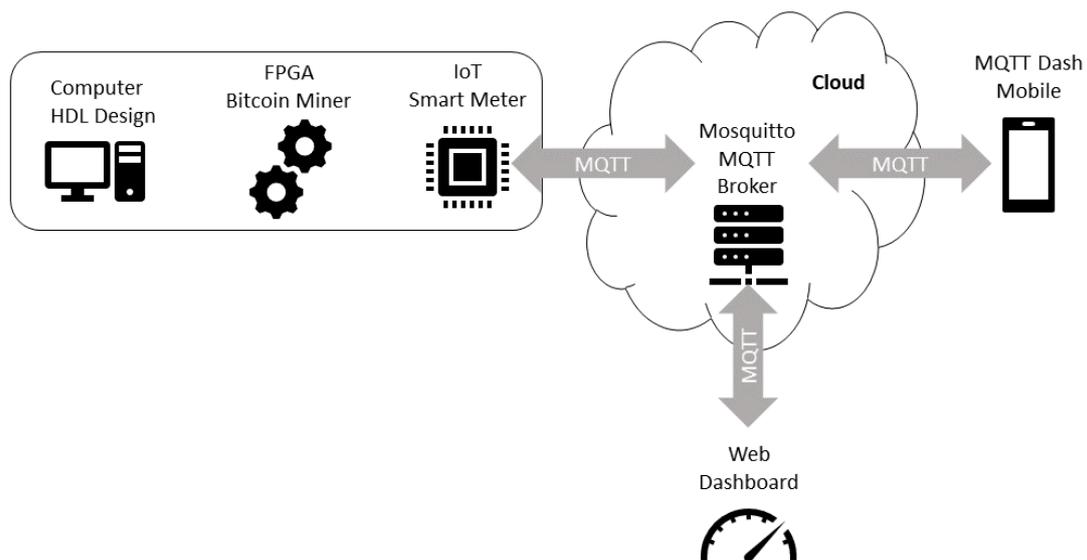


Figure 1. LabBitcoin architecture.

2.2. Why Blockchain?

Blockchain technology is related to distributed network consensus during the construction of information records [Michael Nofer and Schiereck 2017]. At blockchain, the information records are saved in a block that contains the new information for the record and the unique identifier of the last registered block. To determine which will be the next block saved, the majority of nodes in the network need to agree by a consensus. A way to provide this consensus is using extremely complex computational problems so that the node that solves this problem first can choose the next block saved. In the blockchain, the fact of solving a problem to choose the next block is called “mining”.

There is an open issue regarding high energy consumption [Nair et al. 2020], as Bitcoin has an energy consumption between 60 and 125 TWh per year [Sedlmeir et al. 2020] Therefore, a solution would be hardware that generates the consensus of the network in a more energy-optimized way. One way to start developing these devices is by using FPGA, that is why we propose this work. This can benefit the community, especially concerning the IoT because these devices started to be used with Blockchain technology [Xu et al. 2020].

2.3. Building Blocks

The resulting tool composed of Verilog and web interface files is available in a GitHub repository with related documentation to facilitate replication ¹. If there is interest for remote access, the remote lab open source materials from the authors’ previous works for the ESP8266 IoT development board are also available in GitHub repositories ².

An open-source Bitcoin miner implementation for the Altera DE2-115 FPGA board was adapted for the DE0-CV board and used as the standalone miner. Altera Quartus Prime Lite 16.1 was used for port mapping, compilation, and deployment with remote access to the university lab computer. Additionally, an HDL design for the AND port was also used for benchmark purposes. The open-source material found in the literature is available in a GitHub repository ³.

The web dashboard is portrayed in Figure 2, which shows two lab benches with the current power consumption (total and by lab bench).



Figure 2. Web dashboard for FPGA energy consumption monitoring.

¹<https://github.com/vthayashi/labbitcoin>

²<https://github.com/vthayashi/labead-labdig> and <https://github.com/vthayashi/esp8266-esp32-eos>

³<https://github.com/progranism/Open-Source-FPGA-Bitcoin-Miner>

The Android application MQTT Dash available in the Play Store was used as the mobile interface prototype. It was configured according to Figure 3, considering the label, subscription MQTT topic for both power monitoring and relay control, considering disabled publishing option for power monitoring, and enable publishing option for relay control with 1 and 0 values.

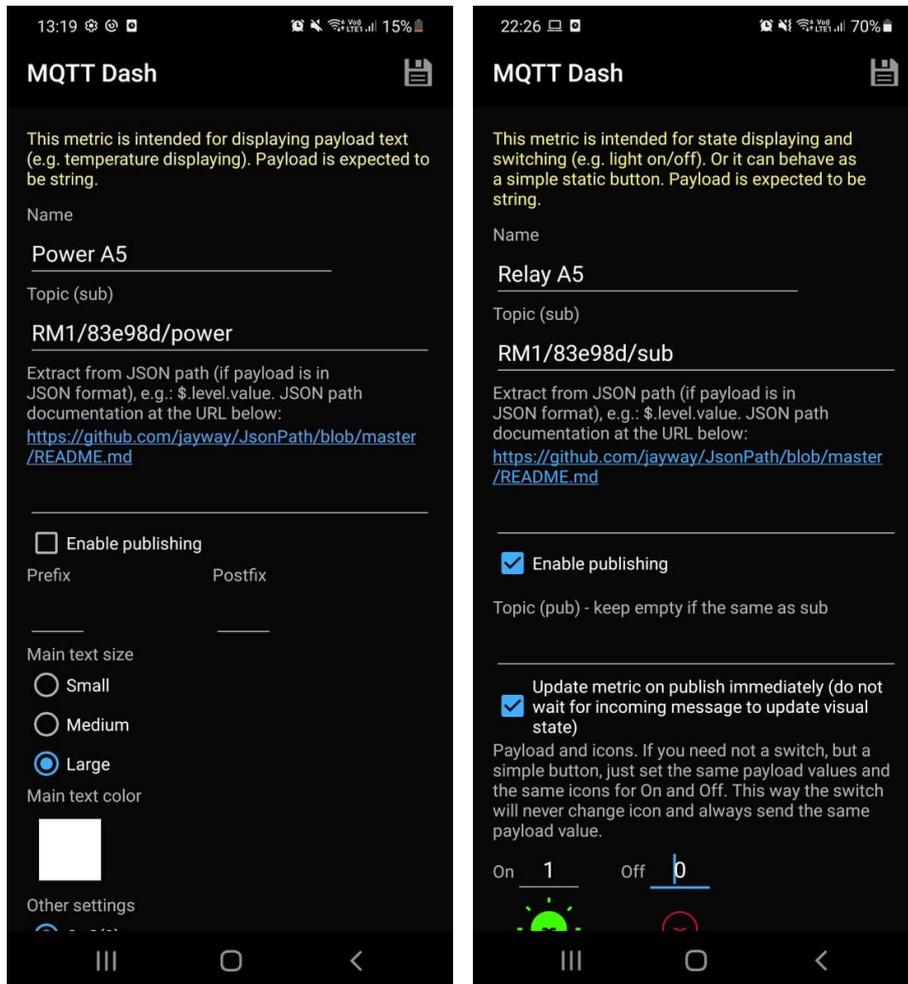


Figure 3. MQTT Dash configuration: power consumption monitoring (left) and relay control for on/off switching (right).

3. Demonstration

This section describes the planned demonstration and the required materials.

3.1. Required Materials

The required materials are a Windows Computer with Quartus Prime 16.1 Lite, an FPGA DE0-CV board, a USB Blaster cable, and the IoT Smart Meter with the integrated relay for smart plug functionality. The broker may be public or private (deployed in a private or public cloud environment), and it may employ basic authentication or it could be open accepting all connections on port 1883. Figure 4 shows the equipment deployed in the university.

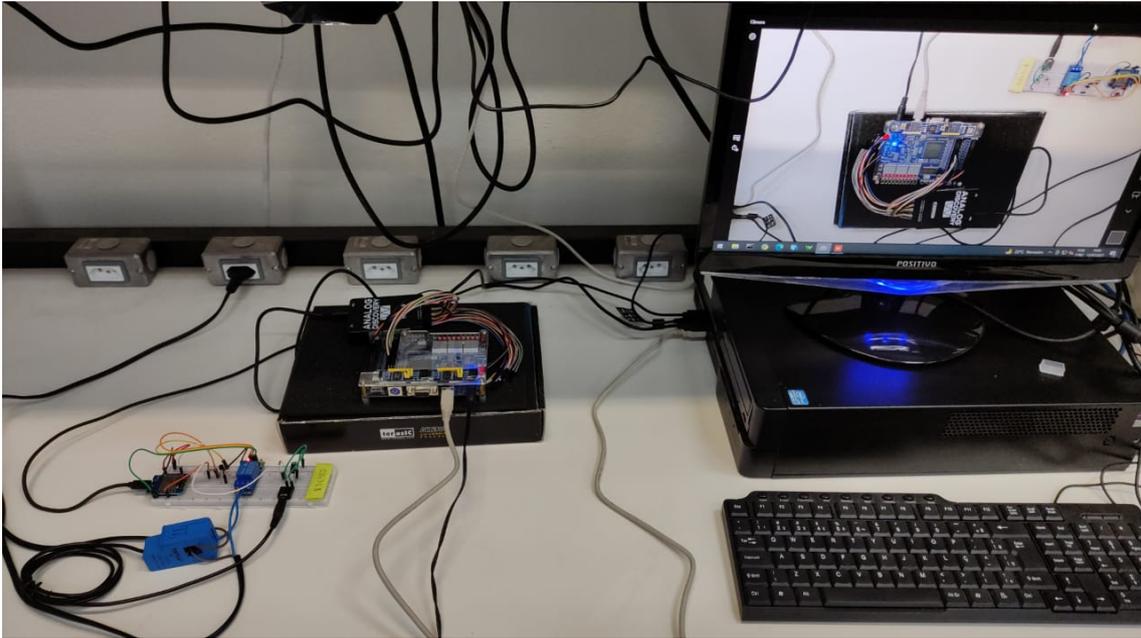


Figure 4. Equipment deployed in the university.

Table 1 presents a total cost estimate for a R\$172.03 prototype with micro controller, non-invasive current sensor, low power relay actuator, and other components.

The values presented were obtained based on the best price between the Kabum⁴ and Curto Circuito⁵ stores, in research carried out on June 03, 2021.

<i>Description</i>	<i>Unit Cost (R\$)</i>
Current Sensor 2000:1	46.80
Resistor 1k	1.00
Capacitor 10u	1.00
ESP8266 NodeMCU	35.40
Protoboard 400 Points	11.95
Male Male Jumper Kit - 65 pcs	12.40
Male Female Jumper Kit - 40 pcs	9.60
Micro USB Cable	10.90
Bipolar Power Cable	12.90
Power Cord	15.18
Module 1 relay Arduino	14.90
Total	172.03

Table 1. Prototype cost estimate.

3.2. Planned Presentation

The following steps compose the planned presentation:

⁴<https://www.kabum.com.br/>

⁵<https://www.curtocircuito.com.br/>

1. Connect the FPGA of bench by cell phone (MQTT Dash);
2. Load the program (AND or Bitcoin Miner) using Quartus and Remote Access to university lab computer (previously compiled);
3. Show power consumption using web interface;
4. If code is Bitcoin Miner, show power consumption at idle and running.

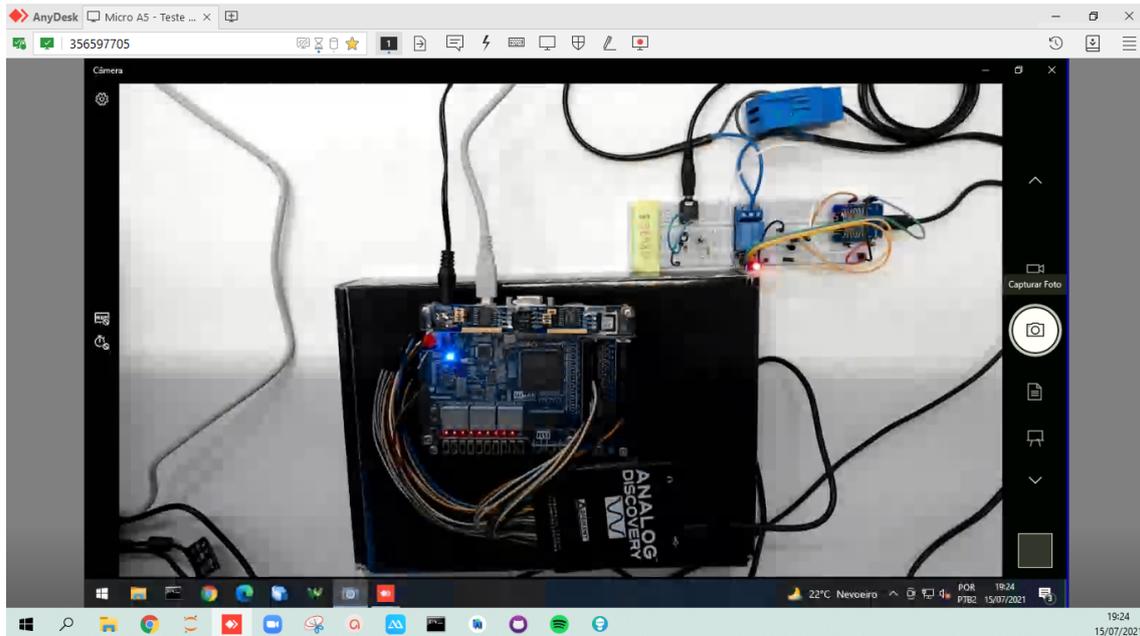


Figure 5. Remote access to the physical appliances.

4. Results

The FPGA board energy consumption was measured based on three different scenarios. The first one was using an AND gate as a baseline since it is the simplest logic circuit possible to synthesize in the FPGA. The second one was using the bitcoin miner with the nominal clock frequency of the board (50 MHz). In this scenario, we measured the consumption of the miner in three states: running, halted, and reset. In the third one, we decided to analyze the effects of overclocking the FPGA board, using the Altera Phase-Locked Loop (PLL) to generate a 100 MHz clock. The same three states were also repeated here. The results are presented in Table 4.

Scenario	State	Power consumption (W)
1	AND Gate	2.5
2	50 MHz miner (running)	3.7
	50 MHz miner (halted)	2.8
	50 MHz miner (reset)	2.8
3	100 MHz miner (running)	4.8
	100 MHz miner (halted)	3
	100 MHz miner (reset)	3

Table 2. Energy consumption tests results.

As expected, the first scenario has the lowest energy consumption. In the second and third scenarios, the miner has the same consumption between the halted state and the reset state. As for the running state, it has a higher energy consumption in both scenarios. Last but not least, the overclocking made consumption higher in all three states.

5. Related Work

We could find a proposal related to the FPGA usage as a Bitcoin miner, but with no simulation nor testbed results to validate it [Oliveira et al. 2012]. Another work assessed the use of Blockchain technology considering efficiency, availability, and integrity requirements, with results regarding performance and security. The energy consumption was not considered in the scope of this related work, and the results are based solely on simulations [Rodrigues and Rocha 2020].

6. Conclusion

This paper presented an FPGA testbed that supports Bitcoin mining experimentation with energy consumption. The IoT remote lab was used to enable monitoring of energy metrics on web and mobile interfaces integrated with MQTT publish-subscriber protocol. These practical activities may motivate enthusiasts and students to apply their knowledge in design challenges considering both performance and energy consumption. To the best of the authors' knowledge, it is one of the first works that combine a remote lab based on IoT to monitor the energy consumption of an FPGA bitcoin miner.

Future work may address a public access of the Proof of Concept presented in this paper, and a workshop using the remote lab infrastructure with university students to investigate if the experiment is useful for certain learning objectives related to the Blockchain and Bitcoin technologies.

7. Appendix

Table 3 presents the pin assignment used on the DE0-CV FPGA board.

I/O	pin
LEDS_out[7]	PIN_U1
LEDS_out[6]	PIN_U2
LEDS_out[5]	PIN_N1
LEDS_out[4]	PIN_N2
LEDS_out[3]	PIN_Y3
LEDS_out[2]	PIN_W2
LEDS_out[1]	PIN_AA1
LEDS_out[0]	PIN_AA2
halt_in	PIN_W9
osc_clk	PIN_M9
reset_in	PIN_U7

Table 3. DE0-CV board pin assignment.

References

- [Hayashi et al. 2020] Hayashi, V., Almeida, F., Arakaki, R., Teixeira, J. C., Martins, D., Midorikawa, E., Cugnasca, P. S., and Canovas, S. (2020). Labead: Laboratório remoto para o ensino de engenharia. In *Anais dos Workshops do IX Congresso Brasileiro de Informática na Educação*, pages 187–194. SBC.
- [Krathwohl 2002] Krathwohl, D. R. (2002). A revision of bloom’s taxonomy: An overview. *Theory into practice*, 41(4):212–218.
- [Michael Nofer and Schiereck 2017] Michael Nofer, Peter Gomber, O. H. and Schiereck, D. (2017). Blockchain. In *Business & Information Systems Engineering volume 59*, page 183–187.
- [Nair et al. 2020] Nair, R., Gupta, S., Soni, M., Shukla, P. K., and Dhiman, G. (2020). An approach to minimize the energy consumption during blockchain transaction. *Materials Today: Proceedings*.
- [Nakamoto 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.
- [Oliveira et al. 2012] Oliveira, S., Soares, F., Flach, G., Johann, M., and Reis, R. (2012). Building a bitcoin miner on an fpga. In *South Symposium on Microelectronics*, volume 15.
- [Rodrigues and Rocha 2020] Rodrigues, C. K. d. S. and Rocha, V. E. (2020). Uma avaliação da tecnologia blockchain considerando eficiência e segurança de aplicações do ecossistema iot. In *SBSEG 2020*.
- [Sedlmeir et al. 2020] Sedlmeir, J., Buhl, H. U., Fridgen, G., and Keller, R. (2020). The energy consumption of blockchain technology: beyond myth. *Business & Information Systems Engineering*, 62(6):599–608.
- [Xu et al. 2020] Xu, L., Chen, L., Gao, Z., Kim, H., Suh, T., and Shi, W. (2020). Fpga based blockchain system for industrial iot. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 876–883.