Ph.D. Project:
Efficient PoWs for IoT Networks

Le génie pour l'industrie

General Information

Research fields:	Blockchain, proof of work, Internet of Things, and digital circuits
Advisor:	Prof. Pascal Giard <pascal.giard@etsmtl.ca>
Location:	École de technologie supérieure, Montréal, Quebec, Canada
Starting date:	Immediately or to be discussed

Project Context

The concept of the Internet of Things (IoT) has exploded in popularity in recent years. Massive networks of small devices are expected to be the main enablers for the vision of smart cities, smart production methods, smart patient care, as well as improved traceability of resources (e.g., medicine and food).

The realization of IoT networks poses a number of challenges as billions of small devices are expected to regularly communicate with each other. Existing networks of connected objects have already raised security concerns, which were prominently covered by popular news outlets such as The Guardian [1] and Forbes [2]. It has thus become clear that identity theft, information leakage, and data manipulation can translate into concrete real-world dangers, meaning that strict security guarantees are required. This is particularly challenging on small IoT devices due to their stringent limitations in terms of computation, storage, and energy. Thus, **new energy-efficient yet robust mechanisms and corresponding hardware implementations must be developed**.

The use of blockchain technology is a promising avenue to provide these security functionalities. At the heart of the most prominent and well-established blockchain contenders lies a Proof-of-Work (PoW) mechanism, whose role is to prove that a significant amount of a limited resource was used to construct a new block before it gets accepted into the blockchain. This approach makes it extremely costly to attack the network. However, the need for a PoW is a major challenge for small IoT devices, whose resources are typically severely constrained.

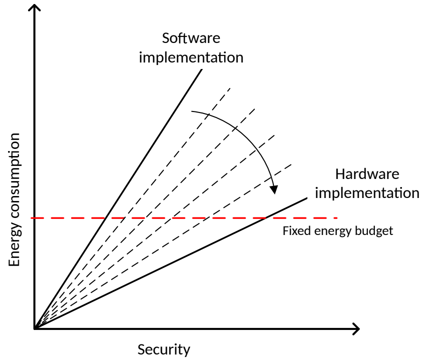

Figure 1: Energy consumption as a function of security, a comparison between software and hardware implementations of a PoW.

This project focuses on the design and implementation of the first dedicated hardware implementation of a PoW algorithm suitable for small IoT devices, which will significantly reduce the energy consumption compared to the existing software-based solutions. As a result, the autonomy of devices targeted at IoT networks will be increased without sacrificing security. Alternatively, for a fixed energy budget, the hardware implementations proposed in this project will enable the use of more complex and more secure PoW algorithms as illustrated in Fig. 1.

Project Description

Almost all existing work on IoT applications in the literature only considers the algorithmic aspects of blockchain technologies as well as the limitations of their current software implementations (e.g., [3]–[6]). Furthermore, the inclusion of a PoW algorithm in IoT devices is considered as one of the major challenges for the integration of blockchain technology in IoT applications [7]. The premise of this project is that **an efficient hardware implementations of current blockchain-based systems would be highly disruptive** in terms of application.

The main objective of this project is to design and implement the first hardware architectures for PoW algorithms suitable for IoT devices. The student will start with the identification of good PoW candidates, evaluating their complexity and bottlenecks. They will then design and implement hardware architectures of the selected PoWs, and verify their functionality against software models by way of simulation. Lastly, the student will integrate the hardware PoWs on a FPGA board, and measure its performance.

Supervision and Funding

Supervision will be provided by Prof. Pascal Giard, a newly appointed professor in the electrical engineering departement of École de technologie supérieure (ÉTS). Professor Giard's research focuses on the efficient implementation of digital systems, from algorithm design to software and/or hardware implementation. His research led to 3 patents, 1 reference book, 11 journal articles, and 21 conference articles. According to Google Scholar, his work has been cited over 1040 times over the last 5 years.

Funding is secured for 4 years (the expected duration of the Ph.D.).

Location

École de technologie supérieure is located in Montréal, Québec, Canada. Often described as an appealing blend of North American and European culture, Montréal is a safe, multicultural city, nice to live in, with an affordable cost of living. It's the most bilingual and trilingual city in North America. More than 50% of Montrealers speak fluent English and French, and more than 20% of them speak three or more languages. Since its inception in 2016, Montréal has constantly ranked as Quacquerilli Symonds' Best Student City in North America.

Montréal is also recognized for its quality of life. Close to both peaceful rural beauty and exciting ski slopes, this dynamic city offers lively districts and many green spaces. Located in the heart of the city, the ÉTS campus is easily reached by bicycle or public transit. Almost 1,100 students live in the school's university residences. These studios and apartments include furnishings, heating, electricity and unlimited Internet access.

Since its creation, ÉTS has pursued a mission that is deeply rooted in all its activities: To meet the needs of the industrial sector, which is in need of engineers who have not only a good theoretical background, but also practical knowledge. To fulfil this mission, ÉTS has a unique partnership with the business and industrial spheres that includes both small and large companies. It stands out from other universities in Quebec because of the applied training it offers students, as well as its research activities conducted by and for companies.

Position Requirements

- Good oral and written communication skills
- Master's degree in electrical or computer engineering, or equivalent
- Research experience in a field related to the topic is an asset
- Proficiency in prototyping algorithms
- Proficiency in implementing algorithms in hardware (VHDL preferred)
- Interest in the field of blockchain
- Experience with FPGA implementation is an asset
- Some knowledge about Proof-of-Work algorithms is an asset

How to Apply

Send an email to pascal.giard@etsmtl.ca with "Ph.D. Project: Efficient PoWs for IoT Networks" as the subject line, including a full CV, university transcripts, recommendation letters and/or contact information from suitable references, and a short statement (max. 1 page) describing how your experience is relevant to successfully carrying out this project. Women, visible minorities, and members of indigenous communities are welcome to apply.

References

[1] The Guardian, *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*, 2017. [Online]. Available: `https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update`.

[2] Forbes, *Confirmed: 2 billion records exposed in massive smart home device breach*, 2019. [Online]. Available: `https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach`.

[3] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Commun. (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436. DOI: `10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102`.

[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *IEEE Int. Conf. on Pervasive Computing and Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623. DOI: `10.1109/PERCOMW.2017.7917634`.

[5] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Int. Conf. on Advanced Commun. Techn. (ICACT)*, Feb. 2017, pp. 464–467. DOI: `10.23919/ICACT.2017.7890132`.

[6] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018, ISSN: 0167-739X. DOI: `10.1016/j.future.2017.11.022`. [Online]. Available: `http://www.sciencedirect.com/science/article/pii/S0167739X17315765`.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018, ISSN: 0167-739X. DOI: `10.1016/j.future.2018.05.046`.