FPGA based architecture for securing IoT with blockchain

Conference Paper · October 2019

DOI: 10.1109/SPED.2019.8906595

2 authors:

Rastoceanu Florin
Agentia de Cercetare pentru Tehnica si Tehnologii Militare
18 PUBLICATIONS **65** CITATIONS
SEE PROFILE

Ionut Radoi
Military Equipment and Technologies Research Agency (METRA)
12 PUBLICATIONS **28** CITATIONS
SEE PROFILE

FPGA based architecture for securing IoT with blockchain

Rastoceanu Florin
Military Equipment and Technology Research Agency

Bucharest, Romania
frastoceanu@acttm.ro

Radoi Ionut
Military Equipment and Technology Research Agency

Bucharest, Romania
frastoceanu@acttm.ro

***Abstract* —The Internet of Things (IoT) became widely utilized during last years, due to the large number of object that are connected to it - not only computers, but also humans, sensors and actuators. In the near future, a large number of objects will communicate to each other in a way never experienced before by the humankind. Connecting all these objects together will come with a wide area of challenges. One of the most important issues concerns trust. In majority of cases, centralized architectures are used to solve the problem, but the enormous number of object that can be connected in IoT will make almost impossible to manage and implement these solutions. Blockchain technology offers powerful solutions for decentralized architectures, which can be the future of IoT systems. A strong solution needs to be flexible to changes and must offer powerful resources to be successful. A hardware platform that uses FPGAs is suitable for those systems. In this paper we propose a solution for securing IoT systems using blockchain technology, implemented on a FPGA based architecture.**

Keywords— blockchain, IoT, FPGA, security

I. INTRODUCTION

IoT (Internet of Things), through interconnection between people, sensors, actuators and IT components offers various services used on a large scale. The number of connected IoT devices is steadily increasing. If in 2015 approximately 15 billion devices were connected, in 2019 they reached about 26 billion and by 2025, approximately 75 billion would connect [1]. This generates an increasing interest in the market. According to statistics [2] the size of the IoT market worldwide has increased twice since 2016 and the forecast estimates it will reach about 457 billion dollars by 2020.

There are many areas of cyber security involved in IoT [3]. One of the most important is referred to cryptographic techniques, which are used to secure IoT data and transactions. In conventional networks the cryptographic techniques have been already standardized. Most of them can be applied to IoT, but there are a lot of challenges for the rest. Because many IoT applications require environmental constraints, it is necessary to adapt or rethink existing cryptographic techniques. IoT security can be ensured by meeting the following objectives: confidentiality (data protection against unauthorized disclosure), integrity (ensuring that data cannot be modified if a prior authorized has not been obtained) and availability (assuring that data can be accessed as needed). Confidentiality can be guaranteed by encryption algorithms and integrity by digital signatures and MACs (Message Authentication Codes). Availability is not provided directly by cryptographic techniques. In cryptography, the most commonly used algorithms are: AES (Advanced Encryption Standard) for symmetric encryption, RSA for asymmetric encryption and DSA (digital signature algorithm) or ECDSA (Elliptic curve DSA) for digital signatures. These algorithms, however, require a great amount of computing power, so efforts are now heading towards lightweight cryptography, which provides useful solutions for confidentiality and integrity in IoT.

All these cryptographic techniques can be implemented in a client / server architecture. This centralized architecture comes with a few drawbacks for IoT:

- all components must be connected and authenticated to the server and that creates a single point of failure;
- the high maintenance costs of the servers is increasing as the number of IoT devices is steadily increasing;
- transaction time increases as the size of the network increases as well.

Taking into account these issues, a decentralized architecture could solve some of the problems. The most current technology is blockchain. This technology is currently being used successfully for financial transactions like Bitcoin, but it is rapidly evolving for the usage in IoT applications. The technology is based on a distributed database, called the ledger, which stores all transactions made by network participants. All transactions are contained in blocks that are checked by consensus by most network participants and cannot be modified later. This ensures two of the IoT security objectives: integrity and availability. All blocks contain a HASH to verify the integrity of the block transactions. The ledger can be stored by all network participants, which allows access to it even if only a part of them are available.

A challenge for IoT is to deal with the large amount of data generated by the big number of components. These data must be processed in real time, and this requires a lot of computing power. Blockchain technology also requires significant computing resources. Another challenge of IoT is the multitude of different components that it contains. On the other hand blockchain technology is implemented in a multitude of alternatives that continuously change. Taking these issues into consideration in order to implement blockchain for securing IoT, it is necessary to use a technology that is sufficiently customizable and powerful enough. FPGAs can successfully accomplish these tasks. Due to their parallel processing capability, they can process in real time and with relatively low power consumption data from a considerable number of sensors and they can also successfully compute the needs imposed by the blockchain technology.

The remainder of this paper is organized as follows: Section II is reviewing IoT issues and challenges, in Section III there are the main features of BC and how can it improve the security of IoT, in Section IV there are the benefits of using FPGAs in IoT and blockchain and a FPGA architecture

978-1-7281-0984-8/19/$31.00 ©2019 IEEE

for IoT with blockchain is presented, in Section V there are the implementations and experimental results and the last section contains the conclusions remarks.

II. IoT Issues and Challenges

IoT is a difficult concept to define. Due to its high complexity, the multitude of beneficiaries and specific applications, and the fact that the technologies that support it are constantly changing, there is no universal definition for IoT by all parties involved. Several standardization organizations have tried to define IoT and each of them has touched a specific aspect of the concept. In IEEEP2413 project [5] IoT is described as a "system of entities that exchange information and interact with the physical world by sensing, processing information, and actuating". ITU introduced in [6] the term ubiquitous network for IoT, which means: "anytime, anywhere, by anyone and anything". NIST approaches IoT in terms of two foundational concepts [3]: IoT components are connected to many network types and some of the components contain actuators and sensors for interacting with the physical environment.

A. IoT applicability

IoT is now involved in many other aspects of people's lives. There are many areas of applicability in which it has emerged. There are more and more startups every year that have as main activity the IoT applications. The most popular IoT app on Google is smart home. These applications can greatly improve the life of the owners of such houses through the ability to control the lighting system, home access door, heating systems, etc. In [7] is presented how blockchain smart contracts can improve the services for a smart home. Another application that has been interesting in recent years is connected vehicles. It is estimated that by 2036 a number of 2.8 billons vehicles will be on the roads. The need for connectivity will also increase. There are many types of connectivity: V2I -Vehicle to Infrastructure, V2V-Vehicle to Vehicle, V2C-Vehicle to Cloud, V2P- Vehicle to Pedestrian and V2X - Vehicle to Everything. In [8] is explained why blockchain can be a potential solution to automotive security and privacy challenges. The blockchain technology can be used with success in smart cities applications. Nation Leagues of Cities an Advocacy organization in the United States, that represents the country's 19,000 cities, towns and villages, explores the developing blockchain opportunities for cities in areas like voting, real estate, transportation, energy, water management [9].

Other IoT applications are as follows: wearable devices, connected health, smart grid, smart farm, smart retail, smart supply chain, industrial internet, etc.

B. IoT architecture

Communications networks have evolved over time. If, at first, network users were connected to a server that managed communication, when the need for access to services and information increased the Cloud appeared. In the end, a fully connected network was needed in which everyone communicated with each other without the need for a central authority.

The IoT architectures follow the same principles. The base architecture is built of three levels (see Fig.1): perception layer – the interface with physical world (sensors and actuators), network layer – responsible for communication between components and application layer

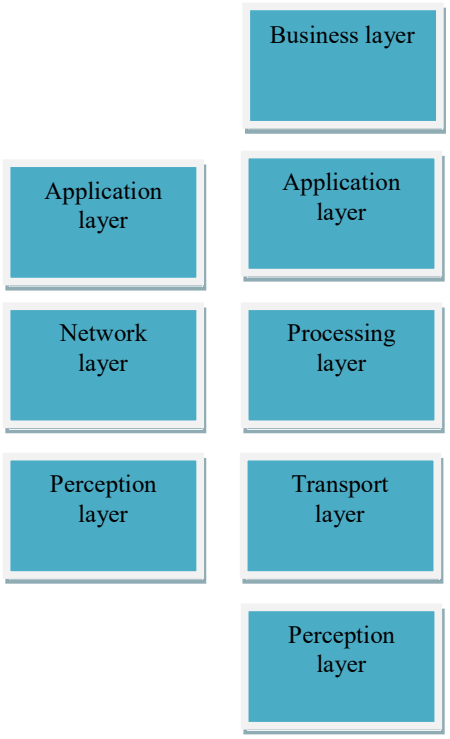

Fig.1 - Three and five layers IoT architectures [10]

– deliver specific services applications to users. Another architecture that details fine aspects of IoT contains five layers [10]. It includes, besides perception and application layers, another three: transport layer that transfers data from sensors and actuators to the next layer and vice versa, processing layer that stores, analyses and processes the big amount of data from second layer, and business layer that manages the entire system.

IoT architectures can be differentiated taking into account the data processing method: centralized, partially centralized and distributed. Cloud architectures are ideal for centralized systems because of their flexibility and scalability. In [11] is presented the Microsoft Azure IoT reference architecture. Cisco [12] introduced a new layer between IoT devices and Cloud, a pre-processing layer called fog. Thus, fog-based architectures introduce gateway devices that process data directly from sensors and then transmit them to the cloud, that can process and store a high amount of data. This solves the problem of the large diversity of IoT components. IoT is comprised by a large number of different objects that need to interact in a fully connected network.

A centralized architecture does not fulfill all the needs for such systems. In this case a distributed architectures is needed. Blockchain is a technology for fully interconnected devices and assures security by design.

C. IoT challenges

Most of the challenges in IoT are to ensure security and privacy. Security issues that IoT deal with, are related to:

- design practices, because there are no models and architectures to refer;

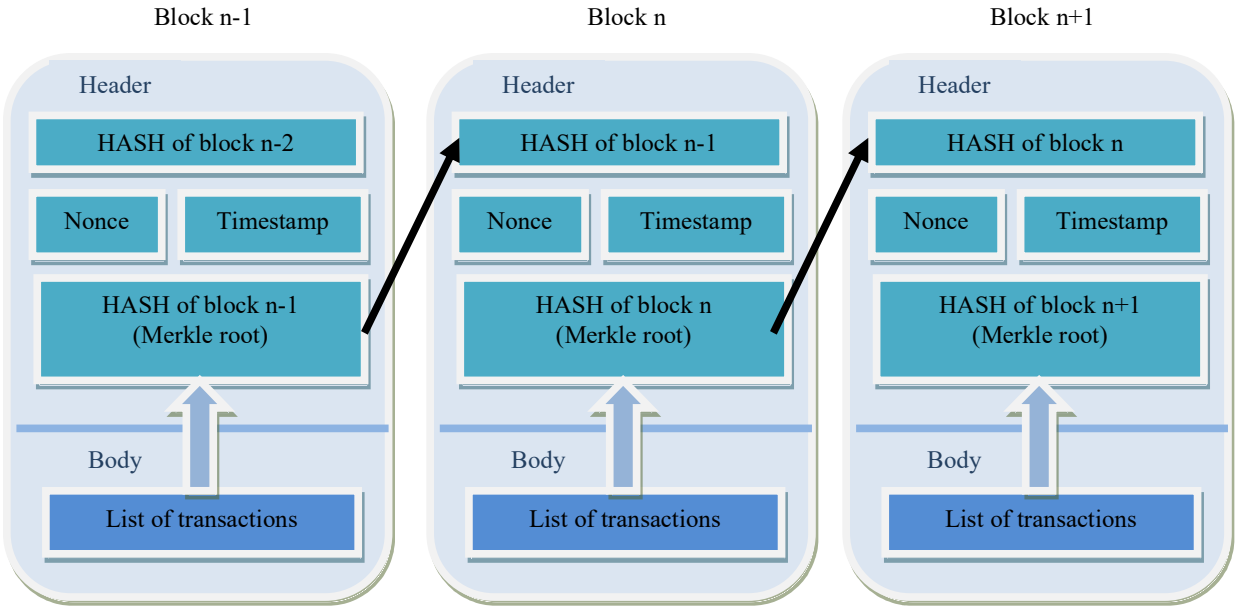

Fig. 1. Blockchain architecture

- lack of standardization, due to the diversity of component types;
- confidentiality;
- authentication &control, regulation;
- low-capability computer power, that cannot implement strong cryptographic methods;
- and many others.

Privacy issues are related to:

- the correctness of data collection and usage;
- lack of resources to develop IoT devices taking into account the privacy rules;
- lack of protection of data collected by IoT devices, etc.

A part of these issues can be addressed using blockchain technology.

III. Blockchain For IoT Security

Can blockchain be a solution for assuring IoT security? In the last few years there are more and more specialists that confirm this. Blockchain was successfully used for Bitcoin. Has been demonstrated to be a robust technology that can be successfully used in other types of applications as well. To answer that question, some aspects of the blockchain architecture need to be presented along with the benefits it can bring to improve security and privacy for IoT systems.

A. Blockchain technology

A blockchain is made up of a chain of blocks called a ledger. As shown in Fig.2. Blocks are linked by hashes. Every block contains the previous block hash. In this way the blocks are linked in a list. The blocks are divided in two parts: header and body. The header contains, besides the previous block hash, a timestamp showing when the block was published and its hash. This hash represents the Merkle tree of all transactions contained in the block, as shown in Fig.3. The Merkle tree is a very ingenious solution due to the fact that it greatly reduces the calculation needed to verify the correctness of block transactions. The body contains all block transactions.

The role of blockchain is to store transactions in a secure manner. Let's see how transactions are added to blockchain and why they cannot be tampered. The flow of events occurring to record a blockchain transaction is the following:

- Each transaction is signed by the owner using a private key kept in an electronic wallet and broadcasted to every node in the network. The owner is represented by an address, a 2^{160} number, generated using the owner public key.
- The miners nodes validate the transactions by verifying its signature. They collect a predefined number of transactions and make up a block, which is distributed to the network to be validated by consensus.
- After the block is validated, it is added to the blockchain and the updated ledger is distributed to all nodes in the network.
- Once stored in a ledger, transactions cannot be changed. To change a transaction the ledger must be changed. For that to happened, it is necessary to gain control of a 51% of the validators in the network. It depends on the consensus mechanism implemented in the blockchain. Consensus is a fault tolerant mechanism used to achieve the necessary agreement to validate a block. It is in some manner similar to Byzantine Generals Problem (BGP) [13]. Generally speaking, the issue is how the generals make a decision, taking into consideration that there might be a small number of traitors and communication problems. There are two types of consensus protocols [14]: *Proof-of-* ... and *Byzantine Agreement (BA)*.

In *Proof-of* consensus type the main idea is to select a node to validate the block. There are several types of such protocols. The most known is Proof of Work (PoW), used in Bitcoin and Ethereum. In this case all nodes try to solve a high computational problem: finding a hash that starts with a certain number of zeros. The hash will be calculated on the block plus a nonce. The nonce will be found by successive iterations. The probability of finding a hash that starts with many zeros is very low, therefore many attempts must be made. PoW is very good to avoid the spamming attacks but is very expensive in terms of energy consumption. For this reason other consensus protocols have been developed such as: Proof of Stake (PoS), Proof of Capacity (PoC), Proof of Authority (PoA), etc.

In *Byzantine Agreement,* validation of blocks is done by majority vote. An important assumption is that most participants must be honest.

B. *Benefits of securing IoT using blockchain technology*

Blockchain technology has several predefined features, that integrated in IoT can bring security benefits. These features can be summarized as follows:

- Decentralization - offers increased confidence since a large number of participants validate transactions and eliminate the single point of failure, making hard to conduct Denial of Service (DoS) attacks;
- Immutability: all blockchain transactions are stored in an immutable ledger. This means that cannot be altered or easily deleted. To change one of these, an attacker must control most nodes in the network.
- Resiliency: each node has a copy of the ledger, so transactions are in the possession of all the nodes. This way they cannot be compromised easily and can also be audited at any time. These features also ensure the transparency and audibility properties.
- Cryptographic support: blockchain technology implements strong cryptographic function that can assure confidentiality, integrity and authentication. Each user holds a pair of public keys that is generated at enrollment. Using the strong cryptographic mechanism provided by elliptic curves it is easy to assure confidentiality of data by encryption and integrity and authenticity by signing the transactions.

IV. FPGAs , IoT AND BLOCKCHAIN

FPGAs for IoT applications have recently begun to be used. Reducing size, reducing power consumption, great reconfiguration and parallelism make them a serious competitor to microcontrollers and ASICs.

Blockchain technology that can be used in IoT requires great computing power and is constantly changing. At this moment blockchain applications mostly uses ASICs, but their lack of adaptability and flexibility make them useless to the changes that occur in IoT systems. FPGAs can replace them with success especially as they are very close to their performance.

A. *Benefits of using FPGA in IoT*

Components required for communication with network devices and with sensors and actuators can be easily implemented in existing FPGAs of low power consumption. The other FPGAs are available for custom accelerators blocks that can improve the performance of IoT applications by moving certain functionality to the hardware. The benefits of using FPGAs in IoT can be summarized as follows:

- Speed: IoT applications need to acquire data from multiple sensors at the same time. The parallelism property of FPGAs allows data to be processed at the same time, thus improving speed.
- Flexibility: IoT sensors and actuators are very different and can be changed at any time. The property of FPGAs to be reconfigurable allows programmers to adapt the system in real time to these rapid changes;
- Reliability: this property o FPGAs can be very useful in complex IoT systems where there are many error sources;
- Low cost: in the last years a lot of low cost FPGAs chips with high computational power appeared;
- Reusability: the hardware platform can be reused to another platform, if needed;
- Long term maintenance: certain IoT components are located in hard-to-reach locations, and it is important that maintenance operations are carried out as rarely as possible

B. *Benefits of using FPGA in blockchain*

Blockchain technology needs fast and reconfigurable devices to be deployed. FPGAs can be used to implement many of the components included in blockchain architectures. The protocols, like PoW, and cryptographic functions like encryption, hashes and digital signatures that require high computational power can be easily and efficiently implemented in FPGAs. Even the network interface can be implemented with good results in FPGA, see [15] for Network Interface Card (NIC) FPGA implementation.

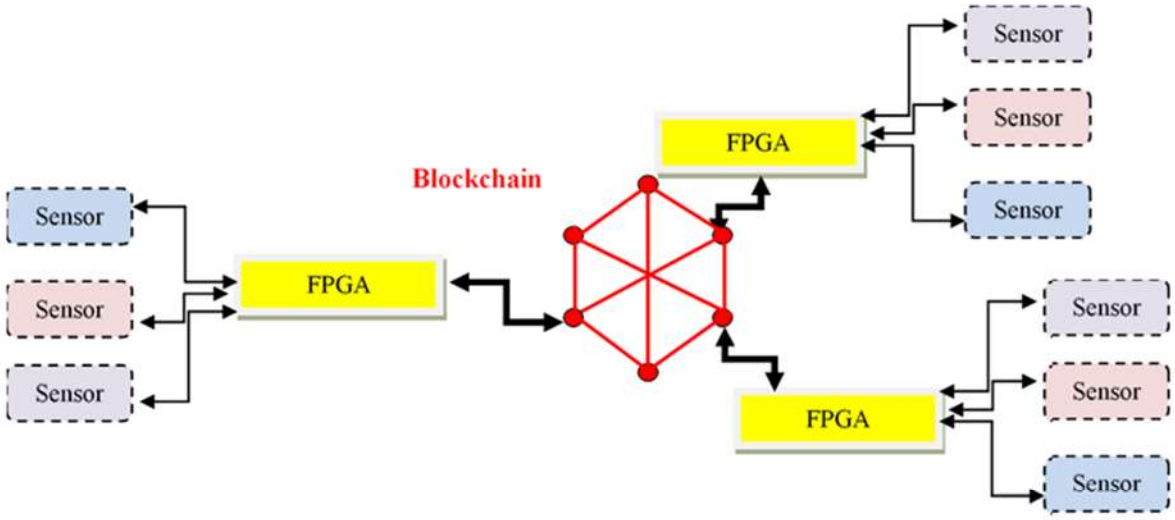

Fig. 2. IoT architecture using blockchain and FPGA

C. FPGA architecture for IoT with blockchain

The usage of FPGA technology in blockchain IoT systems applications is very useful because of the implementation flexibility and parallel processing capabilities. Using its internal reconfigurable resources, FPGAs can implement almost any functionality needed to develop complex IoT devices.

In Fig.3 we propose an architecture of IoT using blockchain and FPGA. In this architecture FPGAs take the role of an edge computing device or gateway, that compute the data from sensors right where is produced, "at the edge" of the IoT network. This comes with some important advantages like:

- Improved security – the data can be secured at this point by reducing the potential of cyber-attack against IoT components;
- Lower operational costs – is not needed to send all data to a Cloud/ Blockchain to be stored. At this point the unnecessary information can be filter out and backup only the relevant data;
- High degree of scalability- FPGAs are flexible and can be adapted to interact to all kind of IoT components;

Besides this role, the FPGA in this architecture can also perform the necessary functions to interconnect with the blockchain. Blockchain technology can be implemented in FPGA circuits in two ways – the solutions are presented in figures 4 and 5.

Fig. 4 presents a typical block diagram common to the most FPGA circuits that don't include the so called "hard processors" (dedicated software processing cores). For this type of FPGA circuits, all the main blocks (processing core, memory controller, communications controllers, blockchain modules) are implemented from the FPGAs' system gates. Modern FPGAs contain dedicated cores that can implement specific functions like Digital Signal Processing, Analog to Digital Conversion, data storage, data buffering, Ethernet and PCI communication. The processing core along with the memory controller are used in applications where software processing (Ethernet layer stack) is needed. In this case, external DDR memory is needed, but power consumption will increase. To reduce power consumption, developers must implement all the system's blocks using only the logic gates.

Today, the electronic IC manufacturers provide smart communication modules that require no operating system and have a completely integrated TCP/IP stack that only requires specific commands to establish connectivity. That is useful because of the high degree of difficulty for the implementation of the TCP/IP stack using only FPGA's reconfigurable resources. This type of communication devices can be connected to the FPGA through serial communication controllers (SPI, I2C, UART, CAN. etc.). The serial communication controllers are easy to implement due to the flexibility of FPGA devices and can be used to connect many other devices common to IoT technology (e.g. sensors, communication modules, data storage devices, etc.). Also, the FPGA provides the possibility to connect analog devices using dedicated Analog to Digital Convertor.

Some FPGAs also include configurable media access controllers (TEMAC - Tri-Mode Ethernet Media Access Controller) that are ideally suited for usage in networking devices.

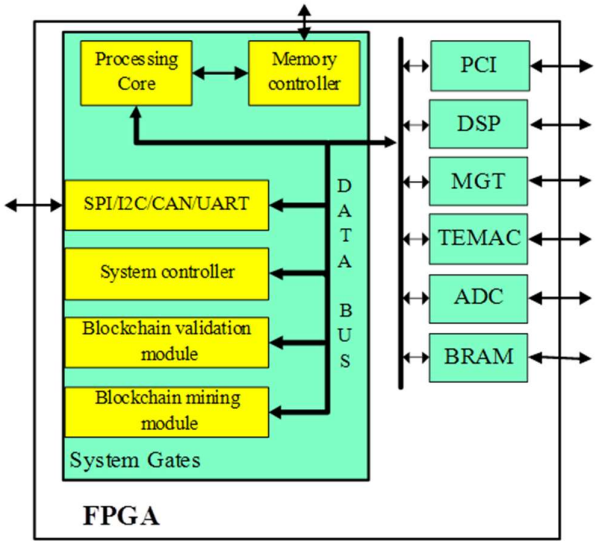

Fig. 3. FPGA block diagram

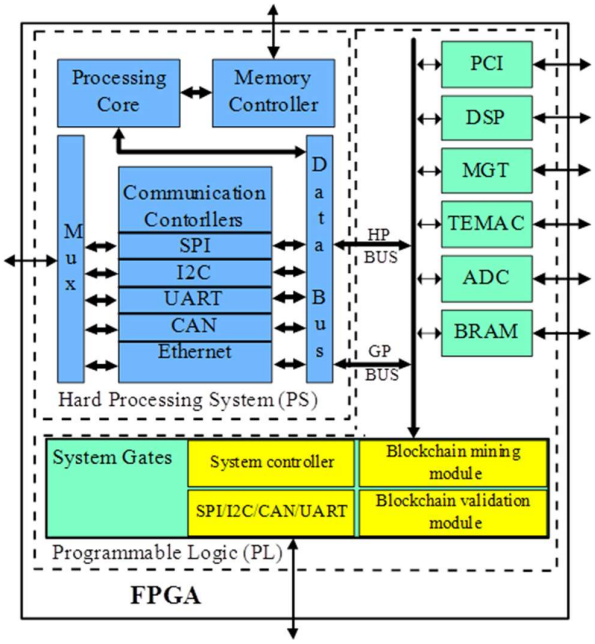

Fig. 4. SoC block diagram

Depending on the choice of the developer, the main component of the system processing can be either processing core (mixed software-hardware design) or system controller (pure hardware design). The second choice is preferred if power consumption is a significant factor.

Depending on the chosen circuit, tens or hundreds of SHA256 cryptographic cores can be implemented. All these cores can perform HASH functions at once, increasing considerably system speed.

Fig. 5 presents a FPGA architecture that includes dedicated processing units (hard processor). The Hardware Processing System block presented in this figure is included only in the newest FPGA circuit families (e.g. Zynq-700, Zynq UltraScale+, Cyclone V) that integrates the software programmability of an ARM-based processor. Because these types of circuits contain dedicated processing units along with several controllers, monitoring and memory blocks, cryptographic modules and reconfigurable logic, these circuits become System-on-a-Chip. Because this is a powerful software processing core, the usage of high speed external memory like DDR3 is mandatory, making it a strong energy consumer. Thus, these types of FPGA circuits are recommended to be used in applications where complex functionalities are performed (e.g. IoT repeater node or IoT gateway). In addition to the conventional data buses (GP BUS), these kinds of FPGAs have dedicated high performance buses capable of transferring tens of gigabits per second [16].

V. Implementation and experimental results

The purposed design depicted in the last chapter was tested using dedicated simulation and development tools provided by Xilinx (Xilinx ISE Design Suite 14.7, Xilinx Vivado 2018.3 and Xilinx XPE). ISE DS was used to implement the design presented in Fig. 5, Vivado to implement the designs with the latest FPGA circuits (Xilinx 7 Series) and the design presented in Fig. 6 and XPE (Xilinx Power Estimator) was used to estimate the power consumption for each type of FPGA circuit. All the hardware modules were implemented using Hardware Description Language (Verilog and VHDL).

In the first part of the experiment the three main blocks found in any IoT node were implemented and for each block logic utilization was noted in order to estimate the remaining logic resources available to implement blockchain mining module. Those three blocks are the following:

- TEMAC (10/100/100Mbps tri-mode ethernet MAC) – 1,256 LUTs;
- SPI CONTROLLER (Master/Slave Serial Peripheral Interface) – 164 LUTs;
- I2C CONTROLLER (Master/Slave Inter-Integrated Circuit) – 216.

For the second part of the experimental chapter, a SHA256 mining module was implemented and then optimized in order to obtain the best timing results. The SHA256 module produced an output after 64 clocks for one 512 bits input block and used only 1152 LUTs. In Fig. 6 is presented the simulation results for this SHA256 module.

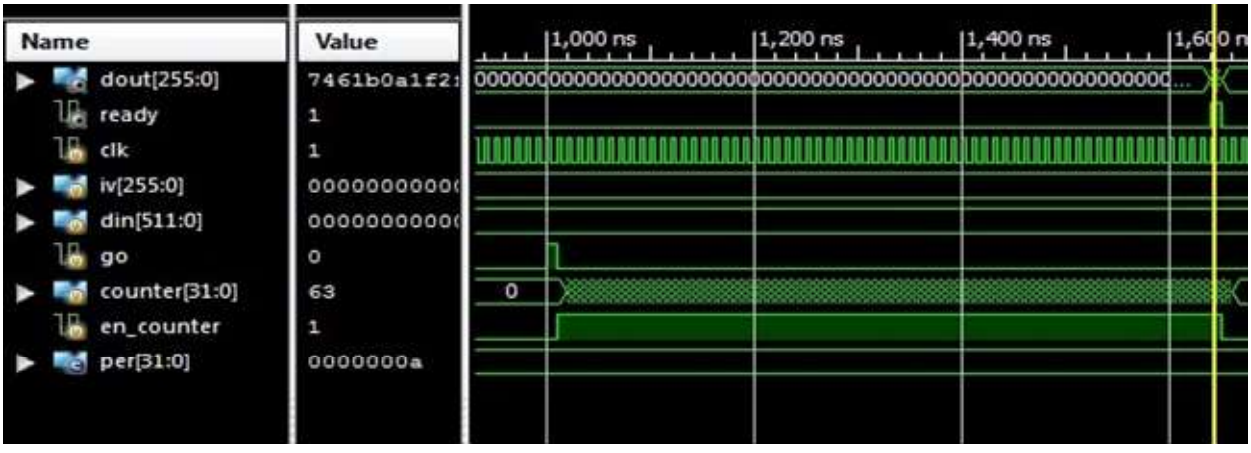

Fig. 5. SHA256 simulation results

TABLE I. EXPERIMENTAL RESULTS

FPGA Family	FPGA Circuit	Embedded Soft Processor	Equivalent HW Platform	Circuit Type	Available LUTs	No. SHA256 cores	Max. Frequency MHz	Output Gbit/sec	Iccq mA
Spartan 6	XC6SLX9	-	-	FPGA	5720	3	69.46	1.66	4.9
Spartan 6	XC6SLX150T	-	-	FPGA	92152	78	69.46	43.44	63
Artix 7	XC7A12T	-	-	FPGA	8000	5	138.7	5.5	51
Artix 7	XC7A200T	-	-	FPGA	134600	115	138.7	127.6	268
Zynq-7000	XC7Z007S	Single-core ARM Cortex-A9	Artix 7	FPGA SoC	14400	12	138.7	13.3	172
Zynq-7000	XC7Z020	Single-core ARM Cortex-A9	Artix 7	FPGA SoC	53200	46	138.7	51.3	437
Kintex 7	XC7K70T	-	-	FPGA	41000	34	151.5	41.2	208
Kintex 7	XC7K480T	-	-	FPGA	298600	257	151.5	311.4	840
Zynq-7000	XC7Z030	Dual-core ARM Cortex-A9	Kintex 7	FPGA SoC	76600	66	151.5	79.9	437
Zynq-7000	XC7Z100	Dual-core ARM Cortex-A9	Kintex 7	FPGA SoC	277400	240	151.5	290.8	1095
Virtex 7	XC7V585T	-	-	FPGA	364200	314	196.1	492.6	1597
Virtex 7	XC7VX1140T	-	-	FPGA	712000	473	196.1	966.3	3698

The SHA256 module, along with the communication controllers was synthesized only on FPGA platforms presented in Fig. 4, as this type of FPGA does not include dedicated communication controllers. For the second platform there is no need to implement auxiliary controllers because, as seen in Fig. 5, this type of FPGA has dedicated communication controllers, thus logic cells are spared but with the price of increasing power consumption.

In Table I the experimental results are presented after hardware synthesizing using Xilinx development tools of the basic and top level circuits for most common FPGA circuit family. Those results are useful for developers, providing important information when new IoT projects are initiated, allowing rapid identification of the proper FPGA devices. Also, the experimental results presented in Table I proves that low-area and low-power FPGA devices (e.g. Low-power Spartan 6 and Artix 7) can be used to build IoT nodes with cryptographic support. Top FPGA devices (e.g. Zynq, Kintex 7 and Virtex 7) are adequate for complex IoT nodes or gateways where power is not important. All the components chosen for this work are low power versions, except Virtex 7 Family, which has no such type of circuit. For each circuit estimated quiescent current is also presented (ICCINT+ICCAUX).

The quiescent supply current (Iccq) values from Table 1 were estimated with the circuit in standby mode, with no data on the circuits I/O pins. The supply current can increase when data is transmitted through the output ports. Also, the current drawn by the auxiliary components has not been taken into consideration. The overall supply current can be decreased by using low power auxiliary components with standby or shutdown capabilities and by efficiently alternating active and standby modes.

VI. CONCLUSION AND FUTURE WORK

In this paper we propose a security solution for the IoT infrastructure, using blockchain technology implemented on FPGA devices.

We have identified the security issues faced by IoT and then presented the advantages of using blockchain technology to solve them. Later we showed the benefits of using FPGAs in IoT applications, but also in the implementation of blockchain technology. Finally, we proposed a general architecture for using FPGAs and blockchain technology to secure IoT infrastructure.

The experimental part was designed to demonstrate that it is possible to implement this architecture in FPGAs. The tests were done for a number of six FPGA families for the weakest and the most powerful FPGA circuits. For each of these, after estimating the degree of occupancy for the implementation of the base modules needed for an IoT node block with blockchain, we optimally implemented the maximum number of SHA256 modules required to implement the PoW consensus algorithm, since this is the most demanding module according to the computing power.

The results presented are useful in choosing the family and type of FPGAs, as they provide information about the number of SHA256 cores that can be implemented, the output in Gbit/sec and the power consumption.

The results can be improved by testing different synthesize strategies and by placement optimization using Xilinx PlanAhead Tool. The study of latest FPGA circuit family (e.g. UltraScale and UltraScalePlus) may be taken into consideration for future work.

REFERENCES

[1] Statista estimates. Size of the IoT market worldwide from 2016 to 2020 (in billion U.S. dollars). Available online: https://www.statista.com/statistics/764051/iot-market-size-worldwide/

[2] Statista estimates. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] NISTIR 8200 - Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT), November 2018, available from: https://doi.org/10.6028/NIST.IR.8200

[4] Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Gary B. Wills, "Blockchain with Internet of Things: benefits, challenges, and future directions", International Journal of Intelligent Systems and Applications· June 2018, pp. 40-48

[5] IEEE 2413-2019 - IEEE Approved Draft Standard for an Architectural framework for the Internet of Things (IoT). https://standards.ieee.org/content/ieee-standards/en/standard/2413-2019.html

[6] ITU Internet report - The Internet of Thinks, november 2005

[7] Yiuyun Zhou, Meng Han, Liyuan Liu, Yan Wang, Yi Liang, Ling Tian, "Improving IoT services using in smart –home using blockchain smart contract", 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

[8] Ali Dorri ; Marco Steger ; Salil S. Kanhere ; Raja Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy" , IEEE Communications Magazine (Volume: 55 , Issue: 12 , Dec. 2017

[9] Camille Moore, Brooks Rainwater, Elias Stahl, "Blockchain in cities – restoring trust and transparency in digital transactions", National League of Cities 2018 report, https://www.nlc.org

[10] Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Hindawi Journal of Electrical and Computer Engineering, Volume 2017

[11] Microsoft Azure IoT Reference Architecture, version 2.1, 26.09.2018

[12] Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, white paper, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

[13] Darya Melnyk, Yuyi Wang, Roger Wattenhofer, "Byzantine Preferential Voting", 07.03.2018

[14] Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A.: Blockchain and IoT integration: a systematic survey. Sensors 18(8), 2575 (2018)

[15] Yuma Sakakibara, Kohei Nakamura, Hiroki Matsutani, "An FPGA NIC Based Hardware Caching for Blockchain", IEICE Transactions on Information and Systems, Amy 2018.

[16] Radoi Ionut, Rastoceanu Florin, Hritcu Daniel, "Data Transfer Methods in FPGA Based Embedded Design for High Speed Data Processing Systems", RISS 2018 Workshop.