Annals of Emerging Technologies in Computing (AETiC)
Vol. 3, No. 5, 2019

Review Article

Blockchain Technology in IoT Systems: Review of the Challenges

Yeray Mezquita[1,*], Roberto Casado[1,2], Alfonso Gonzalez-Briones[1,2], Javier Prieto[1,2], Juan Manuel Corchado[1,2,3,4]

[1]BISITE Research group, University of Salamanca, Salamanca, Spain
yeraymm@usal.es; rober@usal.es; alfonsogb@usal.es; javierp@usal.es; corchado@usal.es
[2]Air Institute, IoT Digital Innovation Hub, Carbajosa de la Sagrada, Salamanca, Spain.
[3]Faculty of Engineering, Osaka Institute of Technology, Osaka, Japan.
[4]Pusat Komputeran dan Informatik, Universiti Malaysia Kelantan, Malaysia.
*Correspondence: yeraymm@usal.es

Received: 15th November 2019; Accepted: 3rd December 2019; Published: 15th December 2019

Abstract: Internet of Things (IoT) platforms have a great number of vulnerabilities which cyber-attackers can exploit. A possible solution largely contemplated in the state of the art is to make use of blockchain technology in any IoT system to enhance the security of the platform while improving other of its aspects. Although there are valuable benefits of the use of IoT platforms based on blockchain technology, it is worth studying the different alternatives between blockchain technologies, because all of them have their own limitations that are not suitable for every use case scenario. In this work, we listed a number of flaws that blockchain technology has in this respect. We have identified that, most of the flaws can be overcome by adapting the variants of this technology to the specific needs of the IoT platform. Every IoT system based on blockchain technology, should perform a systematic analysis of their needs, identifying what are the blockchain features sought for that scenario, to choose the solution that best meets the needs among the different blockchain technology alternatives.

Keywords: ***Blockchain; IoT; Security; Review***

1. Introduction

The interconnected world in which we live generates information from which we can extract knowledge from the use of everyday objects. By placing sensors and actuators on those objects, they send and receive data over the Internet and allow them to interact with their environment without the need of human intervention. The concept used to define this network of devices that interconnect the real world with the virtual one is the Internet of Things (IoT) [1].

By giving everyday objects the ability to measure almost any real-world phenomenon, thanks to the installation of sensors, we can extract knowledge from the data generated. With that knowledge, we can predict some events and carry out preventive actions. In addition, if we install actuators in these objects, we get a greater ability to manoeuvre by getting an automatic reaction and letting the

Yeray Mezquita, Roberto Casado, Alfonso Gonzalez-Briones, Javier Prieto and Juan Manuel Corchado, "Blockchain Technology in IoT Systems: Review of the Challenges", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 17-24, Vol. 3, No. 5, 15th December 2019, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2019.05.003, Available: http://aetic.theiaer.org/archive/v3/v3n5/p3.html.

objects themselves communicate with each other and operate in their environment. All of this is based on measurements and/or predictions previously carried out automatically [2].

The improved responsiveness offered by IoT makes this concept very popular in resource optimization issues, much in demand in today's industry, due to its cost savings (Smart Grids, Smart Home, Smart Farming, Smart City) [3],[4],[5],[6]. In addition, this type of platforms can be used in the automation of services that improve the user experience, giving more information to the user to improve their decisions (Smart Supply Chain, Connected Health, Wearables) [7],[8],[9].

Although these possibilities make the use of IoT platforms very attractive, they also face many challenges: privacy is a growing concern, as companies increasingly have access to information about our daily lives, and the security of devices, which, due to the continuous exchange of information between them via the Internet, become vulnerable to attacks that endanger the integrity of data [10].

There are some authors in the literature who have proposed the use of Blockchain Technology (BT) to protect the privacy of the data generated and its integrity [11],[12]. A blockchain is an incorruptible distributed digital ledger of transactions that can be programmed to store virtually everything of value [13]. The technology behind this ledger is based on a peer-to-peer (P2P) network of nodes that keeps the information stored in a redundant way. These nodes use a consensus algorithm that ensures that the information produced on the platform is stored by the actor who claims it and, once stored, remains unchanged over time.

BTs have a public key signature mechanism; thanks to which it is possible to easily verify the source of the data generated. The mentioned characteristics guarantee the integrity of the data by themselves, but to address the problem of privacy, the public key mechanism can be used to also encrypt the data stored in the block chain [12].

In an IoT system, BT can be used as an alternative to traditional databases, which are controlled by centralized authorities such as banks, accountants and governments. Due to the open, decentralized and cryptographic nature of a blockchain, we can list its main benefits [14]:

- Ensure data integrity, due to the use of consensus algorithms that keeps the data stored in the blockchain in a consistent state between the nodes of the network. This protocol provides the ledger with its immutable nature, making that everything written in there cannot be tampered or edited afterwards.
- Data signed by a public key mechanism. This feature allows the origin of any data stored in the blockchain to be easily verified.
- Dispose of some intermediaries that increase the price of the system's use while making it vulnerable to human errors in the operations of a system. This feature is due to the possibility of storing in the blockchain code that cannot be altered.

The code stored can be executed in a distributed way along the network, reaching a consensus between the nodes on the result obtained from its execution. The programs created with this code are called smart contracts and facilitate, verify and enforce an agreement on a set of predefined conditions [15]. These are self-execution and self-verification contractual agreements that automate the life cycle of a contract to improve compliance, mitigate risk and increase efficiency on any platform where entities with different interests have to interact with each other [16].

As an example, Smart Contracts can be used in an IoT system to configure and manage its IoT devices [17]. Using them together with a security system based on an asymmetric key agreement, it is possible to ensure the integrity and privacy of the data. This gives the devices that read data from the blockchain and operate on the basis of that data the ability to know if the data comes from a trusted source, or if some malicious actor has attempted to attack them. This will prevent, for example, the light in a smart city from being turned on or off by trusted devices and not by others [18].

Thinking of a blockchain as a distributed file system where data is stored, means that all data are possessed by everyone in the network. But, thanks to the nature of this technology, no one can tamper it, those data is always accessible and, if encrypted, just the owner and the ones selected by it can understand the read data. Another positive thing of BT being decentralized, is it can remove the

risk of single point of failure, which make the blockchain always being operative although some of the nodes of its network are down [19].

Although, as we will see in section II, there exists some limitations to provide a blockchain solution to improve an IoT platform, there is an increasing number of works on different use cases that contemplate its application [20].

The majority of proposed architectures in the literature does not make a thoroughly description of how they managed to overcome the flaws of BT when implementing it in this kind of platform, [21] is an example of it.

One of the most common use case in BT based platforms is the traceability of assets. The traceability of assets is a challenge of the current industry because there is no way to prove the origin of any item. With the use of a blockchain, and its immutable nature, it is possible to trace back the origin and the changes that affected an asset during the supply chain [22].

Taylor [23] describes the use of a permissioned blockchain based on Hyperledger technology to store when and where a medicine has been produced. This kind of permissioned blockchains allows for near network latency responsiveness. Also, because all the actors that take part in the blockchain are the stakeholders of the supply chain that share a common interest in keep the blockchain network up, it has mitigated the risk of attackers appearing within the network.

A similar approach has been carried out in [24]. In that work it has been proposed a multi-agent architecture for a BT based platform to improve the supply chain of agri-food assets. There, the blockchain is used to trace the origin and the position of the agri-food assets. In addition, IoT devices store in the blockchain the conditions to which the agri-food assets are exposed during the different stages of the supply chain.

The base of these approach for using a permissioned blockchain is because of the scalability it offers. It is a good approach, based in the security aspect, because the number of companies that take part during the transport and storage of agri-food assets is enough to maintain a strong network of nodes against some attacks, like used in [25].

In [26] it has made an exhaustive review of some real world implementations of blockchain-based platforms for the exchange of energy directly between producers and consumers. Most of those platforms make use of permissioned blockchains instead of public ones, making them the solution most extended among implemented platforms.

In the next section (II) there is a study of how to approach the design of an IoT system architecture based on blockchain. The last section of this paper emphasizes the conclusions of the study carried out in this work, to help designers overcome the shortcomings produced when joining together both terms blockchain and IoT.

2. Challenges of BT

The purpose of this section is to point out the limiting factors of BT to enhance IoT systems. In addition, we will explain some basic concepts of the blockchain protocols that will help to better understand their technology.

First, data sent to a blocking chain are called transactions (Tx). These data are signed by the owner and validated by the network nodes that want to write them in the blockchain. Once validated, a Tx is grouped with others and a block is made from them.

The block is the fundamental part of the blockchain, which is formed by the concatenation of a new block with the last one stored. The process of adding a new block to the blockchain is called mining, and was firstly used in the Proof of Work (PoW) consensus algorithm of Bitcoin, whose nodes solve a cryptographic problem spending a great amount of energy in order to be rewarded with bitcoins [27].

A Tx that have been stored in a block of the blockchain needs to be confirmed. The confirmation process is just the addition of new blocks of data to the blockchain after the one that stores that Tx. The number of blocks needed to be written depends on the BT used, for example in the Bitcoin blockchain [28] the minimum is 6 blocks to fully confirm the data stored.

Due to the possibility of appearing forks in the blockchain, a Tx should not be considered until the block in which it is stored, is not fully confirmed [29]. This is because a fork of a blockchain will only appear from the blocks that are in the edge of the chain, being very improvable to appear from a block that has enough blocks above it.

These basic concepts will help us explain the most important challenges BT is currently facing when used in conjunction with IoT systems [14]:

- **Storage capacity and scalability**. In BT the size of the data stored in the blockchain is growing continuously. As time passes and more transactions are carried out, the nodes require more resources to storage them. One of the possible solutions used by some blockhains like Bitcoin [30], is to make use of different types of nodes with different functionalities in the network, e.g. full.nodes that have the full chain of blocks and are in charge of the verification, routing and mining processes; and light nodes, that stores just a part of the history of transactions carried out in the platform, whose only aim is to provide the data to the users that request it.

  Regarding to the scalability problem of the network, it depends in the consensus protocol of the BT used. It is possible to use a public blockchain as a service to ensure that the technology has a proven security [1]. Regarding this scenario, limiting factors comes from the time needed by the public network to process the petitions of the IoT platform; another factor is the cost of storing the transactions carried out.

  An alternative is to make use of a permissioned blockchain, deploying its network within the IoT system. The nodes of this kind of platforms are needed to be known, so they have a Global Unique Identifier (GUID) with a determined role in the platform. For these systems, the considered fastest protocols are those based on Byzantine Fault Tolerance (BFT) consensus algorithms [31], giving an almost network-speed latency for transaction confirmation [32].

  One of the problems with BFT consensus algorithms, is that it can be exploited their time assumptions and been vulnerable to DDoS attacks [33]. For this reason, a preferable solution is to use another type of consensus protocol, like for example Proof of Stake (PoS) or one of the variants described in [34]. This kind of consensus algorithms are much faster than the PoW solutions, although there is the nothing at stake theory, which claims that these algorithms may suffer for the creation of a great number of forks because of the validation process when adding new blocks [35].

  There is another alternative to the common concept of blockchain, designed for its use in IoT platforms: The Tangle [36]. The Tangle is a Directed Acyclic Graph (DAG) which store the transactions in blocks linked to two previous ones, unlike blocks of any blockchain that are linearly linked. In order to store a new transaction in the DAG, the one who wants to add it has to find if two previous transactions in the edge of the Tangle, are in conflict with the tangle history. This mechanism of consensus would allow the DAG to be executed by the edge devices of a IoT platform without a great waste of energy. Making a new transaction help validate two previous ones, that's why this kind of systems will be scalable by nature, letting The Tangle grow faster as more transactions are made between devices.
- **Security**. Some experts recommend the use of blockchain to provide a security layer in any IoT platform [37]. The blockchain can confirm that the data stored in it come from the IoT devices it claimed to be from. The problem comes when those sources send corrupted data, due to vandalism, a short circuit, disconnection, weather, etc. The corrupted data sources are not always malicious, but if corrupted data is stored in the blockchain, it will be stored in that state forever.

  Because of this scenario, we need to thoroughly test the IoT devices before they are installed in the system and connected to a blockchain. Also, they have to be sealed to prevent the software from being modified and the sensors connected to it from being

exposed and deteriorated. Finally, to make feasible a platform like this, we need to periodically audit this kind of IoT devices [38][40].

The way the IoT devices are protected right now is by using security protocols like Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) to provide secure communications between them. These protocols are expensive in terms of energy and computational cost. A blockchain based platform makes the information-sharing communication between devices unhackable. By giving each device a GUID, they act as peers and they just have to sign and encrypt the information by its private key, letting the blockchain know that the information it receives comes from the source who actually signed it and no one else. Thanks to this and its tamperproof property by design, the system can have both the ultimate hack-proof and foolproof capabilities.

- **Anonymity and data privacy**. In order to protect some sensitive and private data from users of an IoT platform, the public key mechanism of BT can be used to encrypt it. This mechanism can be used from outside the devices while calling the services provided by a blockchain network, or it can be deployed in the device by implementing the security protocol within it. The response time of the first possibility depend on the network latency, while the second one depends on the device characteristics. To make this process faster, it is possible to integrate a security cryptographic hardware into the device [39]. Thanks to this hardware, the encryption and sign process is faster and less computationally expensive, allowing typical IoT devices to make use of this cryptographic mechanism without relying on network latency.
- **Smart contracts**. One of the problems of this kind of programs is that the code is distributed only to be verified, not to share the tasks and gain computational power. This is a limitation which led to the implementation and execution of simple and cheap, in terms of computational cost, smart contracts.

  Another problem is that smart contracts need a trusted source of information, for example a temperature sensor which will tell if a cold chain is broken or not. For this reason, the devices that provide that information need to be thoroughly tested before being integrating in any platform operated by smart contracts [33]. This is important not only for prevent the storage of corrupted data in the blockchain, but to ensure that we are using non-tampered data in the execution of the smart contracts too.
- **Legal issues.** Spanish legislation says in the 1290 article of its civil code: "validly concluded contracts may be terminated in cases established by law". The same goes for the rest articles written for contract termination, which means every contract should offer a way to terminate it. Thanks to the immutable nature of Smart Contracts deployed in a blockchain network, it is impossible to terminate them.

  The only solution to update or terminate an active smart contract, is to deploy a new one with updated clauses. The old smart contract should be able to redirect the petitions it receives to the new one, making this approach valid, at least for the current Spanish legislation [40].

  Another important aspect regarding legal issues, is the way it is protected the rights of investors that put their money in cryptocurrencies. Some countries like Malta have started to create regulation measures for the activities carried out inside distributed ledger based platforms to protect and offer guaranties to people that make use of those technologies [11].

As shown in this section, BT has some flaws that are not suitable for every IoT platform. The mentioned flaws can be overcome by making a systematic analysis of the IoT system to be designed, and choosing how to adapt the BT used to its needs. In the light of these guidelines, it is possible to bring it together both technologies in a real use case, like shown in [26].

3. Concluding Discussion

There is an increasing number of information shared through internet thanks to the IoT devices that monitor their surroundings. The information transmitted may be sensitive, and such platforms need a way to protect the data from being read by non-allowed parties or to prevent the data-tampering by attackers.

BT can enrich IoT platforms by providing a trusted sharing service, where information is reliable and can be traceable. Data sources are easily identified and once the data is stored, it remains immutable over time, increasing the security of a platform that relies on those data. Also, the devices of the network can stop relying in a central entity thanks to the smart contract system provided by the blockchain.

The integration of these two technologies together supports platforms comprised of autonomous agents that negotiate between themselves the progress of the hole system. All of that without the need of central governance and/or human intervention, discarding intermediaries and achieve durability, operational effectiveness, efficiency and financial economy.

To study what it is done in the literature, it has been selected a sample of the current state of the art in blockchain based platforms. There it can be said that the most extended solution to make scalable a system is to use permissioned blockchains instead of the public ones.

The main aim of this work is to enumerate the principal challenges BT based systems are currently facing and describe the alternatives to solve them. The problems discussed in this work are scalability and storage capacity of the blockchain; the corruption of the data stored in a blockchain by a device that hasn't been tested enough, being it corrupted permanently; the difficulty to have data privacy when everyone has access to it; the smart contracts that run in the blockchain cannot be complex; there is no regulation in most of the countries for data stored; and it is no easy to use a consensus protocol that will bring enough security to a public platform and yet let the blockchain to grow at the time-speed needed by the interactions made between the devices of the system, only Tangle seems close to achieve it.

Acknowledgements

The research of Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and Banco Santander. Also, this paper has been partially supported by the Salamanca Ciudad de Cultura y Saberes Foundation under the Talent Attraction Program (CHROMOSOME project).

References

[1] Chamoso, Pablo, et al. "Tendencies of technologies and platforms in smart cities: a state-of-the-art review." Wireless Communications and Mobile Computing 2018 (2018).

[2] Francisco, M., et al. "Multi-agent distributed model predictive control with fuzzy negotiation." Expert Systems with Applications 129 (2019): 68-83.

[3] Gazafroudi, Amin Shokri, Karim Afshar, and Nooshin Bigdeli. "Assessing the operating reserves and costs with considering customer choice and wind power uncertainty in pool-based power market." International Journal of Electrical Power & Energy Systems 67 (2015): 202-215.

[4] González-Briones, Alfonso, et al. "Agreement technologies for energy optimization at home." Sensors 18.5 (2018): 1633.

[5] González-Briones, Alfonso, et al. "A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study." Wireless Communications and Mobile Computing 2018 (2018).

[6] Briones, Alfonso González, et al. "Use of gamification techniques to encourage garbage recycling. a smart city approach." International Conference on Knowledge Management in Organizations. Springer, Cham, 2018.

[7] Christopher, Martin. Logistics & supply chain management. Pearson UK, 2016.

[8] Dykes, Daniel E., Alexander D. Curry, and Alex X. Frommeyer. "Connected health care system." U.S. Patent No. 9,811,636. 7 Nov. 2017.

[9] Rawassizadeh, Reza, Blaine A. Price, and Marian Petre. "Wearables: Has the age of smartwatches finally arrived?" Communications of the ACM 58.1 (2015): 45-47.

[10] Lin, Huichen, and Neil Bergmann. "IoT privacy and security challenges for smart home environments." Information 7.3 (2016): 44.

[11] Valdeolmillos, Diego, et al. "Blockchain Technology: A Review of the Current Challenges of Cryptocurrency." International Congress on Blockchain and Applications. Springer, Cham, 2019.

[12] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[13] D. Tapscott and A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, 2016.

[14] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., 2018.

[15] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in International Conference on Business Process Management, 2016, pp. 329–347.

[16] Icertis, "Smart contracts are transforming the way we do business," 2017. [Online]. Available: https://www.icertis.com/resource/smart-contracts-are-transforming-the-way-we-do-business-featuring-gartner-research/.

[17] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on, 2017, pp. 464–467.

[18] Sun, Jianjun, Jiaqi Yan, and Kem ZK Zhang. "Blockchain-based sharing services: What blockchain technology can contribute to smart cities." Financial Innovation 2.1 (2016): 26.

[19] Atlam, Hany F., et al. "Blockchain with internet of things: Benefits, challenges, and future directions." International Journal of Intelligent Systems and Applications 10.6 (2018): 40-48.

[20] Mezquita, Y. (2019, June). Internet of Things Platforms Based on Blockchain Technology: A Literature Review. In International Symposium on Distributed Computing and Artificial Intelligence (pp. 205-208). Springer, Cham.

[21] Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40.10 (2016): 218.

[22] Tian, Feng. "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things." 2017 International Conference on Service Systems and Service Management. IEEE, 2017.

[23] Taylor, P. "Applying blockchain technology to medicine traceability." Securing Industry (2016).

[24] Mezquita, Yeray, et al. "Blockchain-Based Architecture: A MAS Proposal for Efficient Agri-Food Supply Chains." International Symposium on Ambient Intelligence. Springer, Cham, 2019.

[25] Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." 2016 13th international conference on service systems and service management (ICSSSM). IEEE, 2016.

[26] Pichler, M., Meisel, M., Goranovic, A., Leonhartsberger, K., Lettner, G., Chasparis, G., ... & Bieser, H. (2018, July). Decentralized Energy Networks Based on Blockchain: Background, Overview and Concept Discussion. In International Conference on Business Information Systems (pp. 244-257). Springer, Cham.

[27] Kiayias, Aggelos, et al. "Blockchain mining games." Proceedings of the 2016 ACM Conference on Economics and Computation. ACM, 2016.

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

[29] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security 19.5 (2017): 653-659.

[30] Palai, A., Vora, M., & Shah, A. (2018, February). Empowering light nodes in blockchains with block summarization. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[31] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in International Workshop on Open Problems in Network Security, 2015, pp. 112–125.

[32] J. Sousa, E. Alchieri, and A. Bessani, "State machine replication for the masses with BFT-SMaRt," 2013.

[33] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of BFT protocols," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 31–42.

[34] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in International Conference on Financial Cryptography and Data Security, 2016, pp. 142–157.

[35] Martinez, J. Understanding Proof of Stake: The Nothing at Stake Theory, 2018. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027, [Accessed; 27/11/2019]

[36] S. Popov, "The tangle," cit., p. 131, 2016.

[37] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

[38] Liang, Xueping, et al. "Towards data assurance and resilience in iot using blockchain." MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017.

[39] A. Singh, N. Chawla, J. H. Ko, M. Kar, and S. Mukhopadhyay, "Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-edge Nodes," IEEE Internet Things J., 2018.

[40] Mezquita, Yeray, et al. "Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain." International Conference on Knowledge Management in Organizations. Springer, Cham, 2019.