Blockchain implementation for IoT devices, Blockchain of Things

Nikola Pavlović*, Marko Šarac**
* University of Singidunum, Belgrade, Serbia
** University of Singidunum, Belgrade, Serbia
nikola.pavlovic.141@singimail.rs, msarac@singidunum.ac.rs

***Abstract*—Internet of Things and Blockchain are considered two major technologies. Internet of Things is facing many challenges such as poor interoperability, security vulnerabilities, privacy, and lack of industry standards. Most Internet of Things Devices needs a constant connection to the internet which brings many challenges in their protection and security the data. This is where Blockchain technology comes into use. The Blockchain provides decentralization and authentication that makes is impossible for third parties to gain access to the network. It provides much needed privacy and flexibility which is currently missing from IoT infrastructure. Our work provides a solution with overview what can be done to implement Blockchain in existing IoT infrastructure and furthermore improve security and privacy of the system.**

I. INTRODUCTION

Even though Internet of Things (IoT) is able to solve a wide range of problems, still the security challenges exist. The concerns are related to security and privacy.

Security challenges come in the form of design practices, lack of standards and regulations. Privacy concerns are most visible in data collection and use and bad privacy implementation of designs.

Many IoT devices manufacture are collecting user activity under the agreement to improve service. This is, however, big privacy concerns due to inability to opt out of doing so. Other IoT devices come with no sufficient information on maintainability and upgradeability, which means there is a high probability that it could have zero-day exploit and there will be no way to resolve it.

One way to resolve privacy and security challenges is a synthesis of blockchain technology with it. Blockchain technology removes servers which are the center of IoT infrastructure. This means that data flows through blockchain nodes and each transaction have appropriate authentication. The core of Blockchain technology are blocks that are generated by participant transactions. Each block transaction details are validated if they are maintained in the correct way. This does not allow for tampering of the data inside of the block. Due to data flow inside IoT architecture, Blockchain is a great solution. Blockchain allow it devices to maintain current data flow and improve security and privacy by sequentially checking for each transaction, network request.

Standard data flow for IoT devices is following. Sensors are sending data using internet to the central server. Central server works with Big Data and provide the IoT device, with a specific set of commands what to do.

If we add Blockchain to this data flow, central server would be removed and replaced by distributed blockchains. Introducing Blockchain technology to IoT infrastructure has the following advantages:

- Elimination of single control authority.
- Built on trust between IoT devices.
- Records of historical actions performed by IoT devices.
- All data shared by this device are private.
- Reliability of this device is increased due to being in the closed decentralized network.
- Allowing others, much stronger, cryptography, algorithms to be implemented in this network.

However, Blockchain is not a perfect solution that would fix all of the IoT architecture problems. One of the greatest issues is limitation of storage, scalability, and processing time. Limitation of storage is directly linked to how Blockchain works, it requires a single database with a list of all sequential transactions. Adding more IoT devices to one decentralized network will create scalability issue which means that more storage is directly linked to having more IoT devices. Processing time is linked to allowing other much stronger cryptographic algorithms to protect data. More devices mean more actions and more data processing.

In 2016 Mirai botnet [12] took over 8.4 million IoT devices. The devices were used to perform Distributed Denial of Service (DDoS) attacks. Some actions to find malicious code on devices are performed even today. The problem here is that there is no recorded history of actions performed by devices which makes it even harder to find a malicious device in network.

Silex/Brickerbot [13] was discovered in 2017 but appeared again in 2019. The software scans for public internet access and try to find IoT devices in it. If the IoT device is discoverable, it tries to access it using most common weak login combinations. If it gains access it deletes all network data on the smart device which makes it unusable unless somebody physically get access to the device to restart it to factory defaults. The malware has no other purpose but destructive one, making the device unusable.

In 2019 multiple attacks on Amazon Ring home-security cameras have been reported. Attackers could turn on and off cameras and use built-in microphone to communicate with residents. Attackers used, exploited devices to encourage destructive behavior in children and asking for ransom to leave them alone. The Ring cameras attracted customers who wanted to talk to their children at home. However, the devices which should be used as security devices become a source of privacy invasions.

Another noticeable incident of attacking happened in the spring of 2019. The devices exploited in this case were

Amazon Echo and Google Home. By pointing high power laser to the microphone of the Google Home or Amazon Echo and changing the intensity of the laser, the microphone would convert laser's light into an electrical signal, just as would do with sound [14]. This way attackers could use this device to open garages, make online purchases and execute any command they want. As a way to protect this device some of the manufacturers design their devices to respond only to the voice of the authenticated user or to use two factors authentication when executing a secure command like opening/closing garage, making purchases or setting up security, alarm, system.

Some of the smart devices can only be used from the authenticated user, the voice of the authenticated user can execute commands. Surfing Attack allows attackers to send ultrasonic commands to the smart device. Since the voice of the authenticated user has been just soundwave on a specific frequency, the attacker could record the voice and reproduce it to exploit the device. A remote laptop can use text-to-speech module to send ultrasonic attack via Bluetooth or Wi-Fi.

With the usage of Blockchain all these records are stored, and it is much easier to check for abuse, modification or deletion of the collected data done by unauthorized persons.

There are three types of blockchains:

- Public
- Private
- Consortium

Public blockchain is made to be fully decentralized. No individual or entity cannot control which transactions are recorded or not. This blockchain type is open and anyone can join it.

The private blockchain is also known as permission blockchain. This type of blockchain is most widely used in enterprises. Reason for this is the ease of sharing the data, but still making it private. These chains are centralized by their nature since one entity allows others to join or leave the network.

Consortium blockchain are controlled by the group, compared to private. This approach has all the same benefits are private. This is why some consider it a subcategory of private blockchains.

An essential challenge for IoT is its distributed infrastructure. Each IoT device is a single node that can be exploited and used to get more devices in network to launch for example Denial of Service attack. Another concern regarding security is its centralized configuration. IoT devices in current state most likely are communicating with the cloud service provider. A cloud service provider if compromised is a central point of failure of the entire system.

Important preconditions for Blockchains are:

- It is distributing database system based on rules that allow the transfer of data between entries.
- It is trustless, the entries do not know each other, nor have digital signatures, but they can exchange data without knowing their identities.
- It is permission less, nobody in the network can decide who will operate on it, there are no permissions or controllers.
- It is censorship resistant, a transaction once sent from one node to another cannot be censored or stopped.

There is one special case of Blockchain where it is permitted, but this means that only selected nodes can validate the transactions.

Blockchain technology is based on four concepts:

- A peer-to-peer network, all participants use private/public key to interact with the network. The private key is used to sign transaction and the public key is used as an address on the network.
- Open and distributed ledger, database of all transactions, which is open to everyone.
- Ledger copies synchronization, a way to synchronize ledger across all participants.
- Mining, a way to prevent adding nodes on a chain, because the chain must be valid and ordered.

On Figure 1. It is displaying content of one blockchain block. Each block contains two elements, header, and block content. Headers have a timestamp, the hash values of previous block and hash values of current block. Links using hash values prevents replay attack. The block content contains all inputs and outputs of each transaction.

In case of Public Blockchain the only way to tamper with Blockchain is to gain ownership of 51% of the computing power of the whole network.

In case of Private Blockchain there is no way to tamper with network since all transactions are controlled by one person or entity.

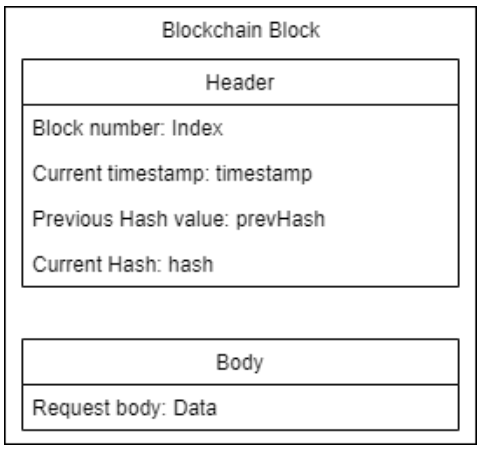

Figure 1. Blockchain block data

II. STATE OF ART

N. Kumar and P. Mallick [1] researched what challenges are facing current IoT infrastructure. In the paper authors dealt with privacy and security challenges. They have identified biggest issues with current infrastructure and provided overview of them all. With provided overview authors also provided why Blockchain is needed in the IoT. Some of the sectors where blockchain and IoT can be merged and provided good benefits are Agriculture, Business, Distribution, Energy, Food, Finance, Healthcare, Transport and logistics and Smart city. Authors also provided a list of benefits such as

tamper proof data, elimination of single control authority, robust, records data of old transactions in smart devices and others.

M. Miraz [2] in the work provided an overview of blockchain and how it works with fundamentals as well as IoT fundamentals. After providing fundamentals of IoT and Blockchain author proposed merge of these two technologies and present the benefits of the merge, improved security, the immutability of the data, verifiability, and access to smart contracts from the Blockchain. The benefit IoT provide to Blockchain is by actively participating in the consensus process.

V. Hassija et al. [3] provided an overview of historical changes of IoT infrastructure, from a cloud based to present IoT infrastructure with many servers with a single point of failure and future Blockchain based. In the survey authors presented security threats at different layer of the network. Some of the attacks are discussed and provided solutions for them on different network layers. The survey authors provided is expected to serve as a resource for future research and resolve the challenges with security and privacy that exist in current IoT infrastructure.

H.F Atlam et al [6] in the work addressed the issues with the client/server model that is using current IoT infrastructure. Out of many issues that exist the most important ones are scalability and security. In the paper authors provided an overview of integrating Blockchain with IoT. The merging of these two technologies would bring many benefits and challenges that should be addressed. The challenges that are faced with merge are scalable, legal compliance, processing power and time, storage.

III. PROPOSED SOLUTION

Using Blockchain technology in current IoT infrastructure provides a network with possibility to add or remove any device to the network and enforce custom access control policies. In proposed solution we are using private blockchain. Reason for this is to move control of the network to a single point of security and if some of the IoT devices get compromised it would cause no harm to the network. Also, another important fact is that to get access to private blockchain network a device would need an invitation. All the devices in this network would be hidden from the public network and for someone or something to access the smart device it would need to send request to control point of the blockchain network.

For one IoT device to work without any problems and get the data from Cloud services it would need to do the following actions. For IoT device to send a request to Cloud service and get data first it would need to send request to blockchain interface that authenticate, records and enforce access policies. Request to blockchain interface is one blockchain transaction. The transaction is successful if it is done from devices that are approved in the private network and if provides proper hash and data that is needed to validate a transaction in blockchain. Once the transaction is successful the blockchain interface will send request, that is copy of the blockchain body data, to cloud service. The cloud service would respond to the blockchain interface with command. Blockchain interface parse the request from Cloud service and create new transaction to the IoT device that requested the data from Cloud.

All the requests inside private network are transactions and there is no way for them to be fabricated or changed. Each transaction is saved in Distributed Ledger, a database that can be on the blockchain interface. A blockchain interface could be hosted on any computer and the distributed ledger could be saved on the device, local network server or in case of usage in smart homes where there is no local server a remote database that can be encrypted with strong encryption algorithm and requested to this server can be done using RSA algorithm.

We have tested different approaches when integrating IoT with Blockchain technologies. To make sure all data shared by the blockchain nodes is secure we have used a private blockchain approach in the protocol.

To make sure proposed solution will work, we have created demo version of it and tested on simple humidity and air temperature sensor and cloud service that provided actions depending on values sent by sensors. The data provided by sensors is sent to blockchain interface which created new transaction, check validity of the block, and write to distributed ledger. Then this data is sent to cloud and response from the cloud is received by the blockchain interface. The interface creates new transaction for response and provide a smart device with command.

With this approach we have created a private blockchain network with single point where data from the cloud is received, validated, and properly parsed then sent via blockchain transaction to smart device.

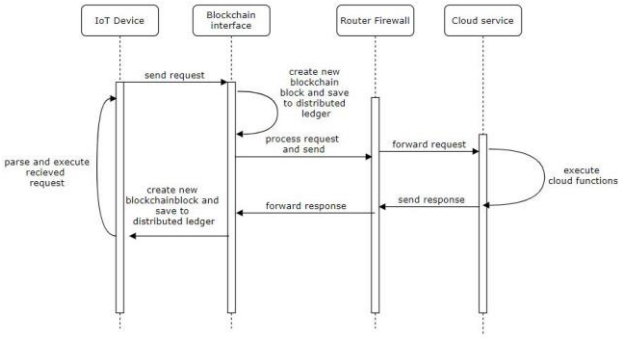

Figure 2. Sequence diagram of the proposed solution

This proposed solution can be furthermore improved by adding the following:

- Filtering allowed cloud services that can access Blockchain network, by allowing certain IP addresses or range of addresses that can access.
- Adding an additional layer of security by implementing an interface that will encrypt/decrypt the data that is leaving the blockchain network.
- Adding form of caching response from the cloud to prevent request leaving the blockchain network. If same request is sent to cloud, we can use distributed ledger to provide smart device with a previous response from the cloud.

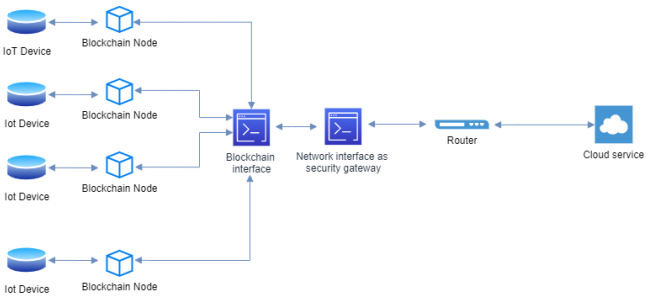

Figure 3. Network infrastructure of the proposed solution

On Figure 3. It is displayed the structure of proposed solution. Each IoT device is connected to Blockchain infrastructure and each network request is a transaction. As previously mentioned, security interface is between Blockchain interface and the router and it monitors each request made to the internet.

In the future work we will integrate all previously mentioned features and provide a solution that can be easily setup in any IoT network.

IV. CHALLENGES

The fundamental problem with current IoT architecture is their security, with centralized model, with central authority, which makes it susceptible to a single point of failure. Blockchain eliminate single points of failure and move decision making to shared network of devices in case of public blockchain infrastructure or single entity in case of private blockchain infrastructure.

There are three main challenges when designing architecture for IoT to work with Blockchain technology:

- When working with large number of devices in a single network, the main problem here is scalability. By adding more devices network transaction processing speed lowers.
- The privacy of transaction history in the shared ledger for a network of IoT devices cannot be easily granted on public blockchains.
- The reliability of IoT sensors could potentially be undermined by interfering with the correct measurement of the criteria that need to be met to execute a transaction.

Measures to ensure the integrity of IoT devices so they cannot be altered by external interventions are must for securing a safe environment for data flow and transactions.

We propose an approach with following advantages:

- The system can be isolated and free to add any device to the network while still enforcing access control policies.
- In case of failure of some device, entire network will still be visible and operating properly.
- Approach has no issue with scalability, which means any device can be added or removed from the network without causing any issues.
- The system hides all IoT devices behind Blockchain.

By creating a fusion of blockchain and IoT technologies, it is inevitable to change how current technology is used. Integrating them together is not a straightforward matter. To maintain consensus blockchain is using two main consensus mechanism, Proof-of-Work and Proof-of-Stake. Proof-of-Work is first consensus algorithm and up to this day most used one. This algorithm prevents double-spend. Double spends is when the same data is used twice or in case of cryptocurrency same funds spent twice. In Proof-of-Work, the miners solve cryptographically hard puzzles by using their computational resources. In Proof-of-Stake instead of miners, there are validators. The validators as the name says validates the blocks and add them to the chain.

Since Proof-of-Work requires too much electricity and power it is not a good combination with IoT. The best combination in this case is Proof-of-Stake.

In this paper, each node (IoT device) has access to Distributed Ledger – a shared but temper-proof digital ledger. Distributed Ledger is a database of all transactions which are chronologically recorded time-stamped transactions or data. Distributed Ledger is append-only and existing blocks cannot be updated or removed.

The advantages of this approach are that we are eliminating single point of failure. If one node in the network becomes unavailable or compromised, the network will continue its work without any disruptions.

Since IoT devices cannot do blockchain validation and sending requests we propose a hub architecture.

All IoT devices will have access to IoT Hub. Each request from the IoT device (or sensor) will be directed to the Hub. In cases where IoT devices are connected to the LAN and try to send the request to cloud computer, this request will be firstly forwarded to Hub. This can be done with firewall rules that can be updated on home router.

Each request done to IoT Hub is being treated as a transaction. It must have sender, receiver, and additional data (which is response from a cloud computer). As previously explained each transaction is being validated so this prevents any kind of data tampering by third party. With blockchain implementation in IoT adding any additional device is rather flexible and requires no additional work on protocol. The device requests will go through hub and will get responses from a hub (forwarded from cloud server).

In our previous research we proposed An Approach to Adding Simple Interface as Security Gateway Architecture for IoT Device. As a blockchain and IoT implementation is flexible we can furthermore improve security of entire IoT infrastructure by adding simple an interface as security gateway. Since blockchain body has additional data that we are passing from cloud we can add additional simple interface that will encrypt / decrypt this data and prevent attackers to record remote requests. The interface would work between blockchain and cloud.

With the merge of Blockchain, IoT and Simple interface as security gateway we achieved the following:

- Any remote request, from the moment request leave LAN and go to the Internet it is encrypted. The security gateway will encrypt data in any Cryptographic algorithm (which is supported by cloud).

- Response from the cloud will be encrypted with the same algorithm that is used when sending the request.
- When a remote request is received by Router, it will be forwarded using firewall rules to IoT Hub.
- The IoT Hub will decrypt the request and proceed it to Blockchain implementation.
- Once Request is decrypted blockchain have following parameters (Receiver – to whom is request sent, Sender – from who is request sent, Additional Data (in body) – Command or any info from the cloud).

Once Request is decrypted blockchain have following:

- Blockchain implementation will validate the request and create a new block.
- The newly created block will be appended to distributed ledger.

V. CONCLUSIONS

With the proposed merge of the solution, we achieved security of LAN and remote requests. Not only we improved security but got a database (distributed ledger) with a list of all requests written in it. So, if some attack happens, we can debug it from the database and add an additional layer of protection to existing architecture, update the infrastructure loopholes. In the continuation of this research, we will provide what attacks are possible on current IoT infrastructure and how strong our proposed solution is against them.

This approach would greatly improve the security of the smart devices. Right now, smart devices are vulnerable to different attacks, and most of the smart devices have low or no enforced security policies at all.

The approach we propose to improve security of the smart devices by restricting it from making direct requests to the internet. All requests are authenticated by Blockchain interface and approved if they are correct. Another layer of security from internet is added by implementing a simple interface as security gateway. This interface protects the devices from third parties that are not allowed by network rules to access local network.

Smart homes, healthcare, private businesses, etc. are all industries where our proposed solution could be used. Flexibility of the solution provides a high level of security to all the devices in the environment where private data of the residents in case of smart home or highly valuable data of the private businesses and data on the patients need to be hidden and only saved on the local hard drive. Another layer of security provided by the simple interface as a network gateway could be used in this case as encryption logic to protect the data in the blockchain body when saving it in storage.

REFERENCES

[1] Kumar, N. and Mallick, P., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, pp.1815-1823.

[2] Miraz, M., 2020. Blockchain Of Things (Bcot): The Fusion Of Blockchain And Iot Technologies. [online] Arxiv.org. Available at: <https://arxiv.org/pdf/1910.06898> [Accessed 1 November 2020].

[3] HASSIJA, V., CHAMOLA, V., SAXENA, V., JAIN, D., GOYAL, P. and SIKDAR, B., 2020. A Survey On Iot Security: Application Areas, Security Threats, And Solution Architectures. [online] Ece.nus.edu.sg. Available at: <https://www.ece.nus.edu.sg/stfpage/bsikdar/papers/access_19.pdf > [Accessed 4 November 2020].

[4] Dai, H., Zheng, Z. and Zhang, Y., 2019. Blockchain For Internet Of Things: A Survey. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/333600905_Blockchain_for_Internet_of_Things_A_Survey> [Accessed 5 November 2020].

[5] Andersen, M., Kolb, J., Chen, K., Fierro, G., Culler, D. and Popa, R., 2017. WAVE: A Decentralized Authorization System For Iot Via Blockchain Smart Contracts. [online] Www2.eecs.berkeley.edu. Available at: <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-234.pdf> [Accessed 4 November 2020].

[6] Atlam, H.F., Alenezi, A., Alassafi, M.O., & Wills, G. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. International Journal of Intelligent Systems and Applications, 10, 40-48.

[7] Makhdoom, Imran & Abolhasan, Mehran & Ni, Wei. (2018). Blockchain for IoT: The Challenges and a Way Forward. 594-605. 10.5220/0006905605940605.

[8] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. Sensors (Basel, Switzerland), 18.

[9] Dwivedi, A., G. Srivastava, Shalini Dhar and R. Singh. “A Decentralized Privacy-Preserving Healthcare Blockchain for IoT.” Sensors (Basel, Switzerland) 19 (2019): n. pag.

[10] Tariq, Noshina & Asim, Muhammad & Al-Obeidat, Feras & Farooqi, Muhammad & Baker, Thar & Hammoudeh, Mohammad & Ghafir, Ibrahim. (2019). The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. Sensors. 19. 1788. 10.3390/s19081788.

[11] Kim, S.-K.; Kim, U.-M.; Huh, J.-H. A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security. Energies 2019, 12, 402.

[12] G. Kambourakis, C. Kolias and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 2017, pp. 267-272, doi: 10.1109/MILCOM.2017.8170867.

[13] Shouran, Z., Ashari, A., & Kuntoro, T. (2019). Internet of things (iot) of smart home: Privacy and security. International Journal of Computer Applications, 182(39), 3-8. doi:10.5120/ijca2019918450

[14] Nirupam Roy, Sheng Shen, Haitham Hassanieh, & Romit Roy Choudhury (2018). Inaudible Voice Commands: The Long-Range Attack and Defense. In 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18) (pp. 547–560). USENIX Association.