Blockchain for IoT using Lightweight Cryptography

Submitted by:

Deniz Aytemiz
Jamous Bitrick
Satish Vankatesan

11/15/2021

Submitted in partial fulfillment of the requirements for CS/ECE 5560 Class project

Bradley Department Electrical and Computer Engineering Department
Virginia Tech

Abstract

Write a concise abstract of the paper, including goals/objectives. Abstract should be about 100-200 words in length and Times New Roman, 12point. Pay close attention to grammar and spelling.

1. Introduction

Problem Statement:

The Internet of Things, IOT, is a very exciting field of study in Computer Science due it's seemingly boundless potential. One challenge with implementing IOT, is managing all the sensitive data collected in a secure and efficient manner. One proposed solution to data management in IOT applications is the use of Blockchain. However, two primary challenges are impeding the utilization of Blockchain with IOT. IOT devices are typically low-power devices, and supporting a blockchain is a very computationally expensive procedure. To successfully implement blockchain in IOT applications, either a change in blockchain implementation to be more computationally efficient must occur or a lightweight cryptography algorithm must be implemented for security.

Background:

Internet of Things:

The Internet of Things is the idea that everyday objects are interconnected on the same network. (Xia et al., 2012) The data these devices send between each other can be used to gather more information on users to better serve their needs. One common IoT example is the idea of interconnected vehicles. If all vehicles on the road can communicate with one another and sensors on a road, traffic patterns could be better predicted for users, and navigation systems could reroute users to prevent any lockups. This example has not been implemented in the real world yet, and while we have only just scratched the surface with IoT technology, there are still many devices which utilize IoT principles, like smart watches, health devices and smart home appliances. (Stoyanova et al., 2020) These devices are all connected to the internet and store data on user profiles which is used to improve user experience across their devices.

Protecting the data associated with IoT devices is of utmost importance, as the data is often very sensitive and private to the users. If successful, attackers would have access to a prodigious amount of personal data, including health diagnostics, daily patterns etc.

Blockchain:

Blockchain, very simply, is a decentralized distributed ledger. Blockchain has become very popular as it is a platform which can share transaction information throughout all members of the chain without needing a central authority while maintaining data security. The decentralized nature of blockchain is considered it's most attractive feature as decentralized currencies have less restrictions on transactional behavior and also are more protected against inflation or deflation. (Yaga et al., 2018)

Blockchain has the potential of solving the problems of scalability and security with regards to data management for IoT networks and devices. By design, blockchain is a peer to peer network of shared data, which lends itself nicely to managing IoT data. Furthermore, data within a chain is immutable and available to all users in chain, meaning there's no need for trust between uninitiated users. Lastly, smart contracts can be used to automatically perform functions based on IoT data.

The main blocker to the integration of Blockchain and IoT is the fact that Blockchain is very computationally expensive and IoT devices are typically low power devices.

Consensus Protocols:

Blockchains use consensus protocols to get each node in the chain to validate transactions. There are two types of consensus protocols that are mostly used: Proof of Work and Proof of Stake.

Proof of Work:

Proof of Work is the first consensus protocol used in a Blockchain. In Proof of Work, each miner must solve a complex hash problem for their block to be added successfully to the chain. This prevents users from entering duplicate transactions or double spending. Proof of work also ensures that attackers would need to spend a high amount of computational power to compromise a chain.

Proof of Stake:

Proof of Stake is an alternative consensus protocol, which will be used in Ethereum 2.0, which examines how much stake a miner has before allowing them to add a block to the chain.

Compared to proof of work, proof of take is far more computationally efficient and sustainable for a network.

Objective of the Project:

The objective of this project is to survey academic papers discussing solutions with the utilization of blockchain in IoT applications. After analyzing the papers, we want to analyze the proposed solutions and their implications for the field, as well as discuss potential future paths for research to follow in this field.

Approach:

We plan on reading multiple papers in this domain, and surmising their research and proposed solutions. After interpreting the results and judging the implications of their research, we will compare and contrast the findings of each paper and discuss the merits and limitations for each. Lastly, we want to discuss potential directions we believe research in this field should address to further this domain.

Limitations of Paper:

The nature of the papers and the research we are surveying, makes the results very difficult to reproduce, so our analysis is dependent on the results reported in each paper.

2. Literature Review

This Section should include related work, along with a discussion on its contribution to the current project; which existing practices are not suitable for this project and why; which one will be used, and why. Finish with a short summary of this review.

2a. Black-Box IoT: Authentication and Distributed Storage of IoT Data from Constrained Sensors

The use of Blockchain technology in IoT settings has been proposed for fast detection of errors and inconsistencies among network data without including a third party authority. BBox-IoT proposes a solution for implementing Blockchain technology into low SwaP devices. The approach enables low-SWaP devices to authenticate without reliance on clock synchronization and ensure that the collected data is immutable and tamperproof while preserving data provenance and non-repudiation.

BBox-IoT architecture does not depend on heavy cryptographic primitives which low-Swap devices cannot process. It uses a novel hash-based digital signature with a one time hash chain and eliminates the need for synchronicity between signer and verifier. Therefore does not require clock synchronization.

In BBox-IoT there are five main types of participants, most of them are inherited by Hyperledger Fabric. These can be listed as follows; the MSP, orderers, local administrators, aggregators and sensors. In Hyperledger Fabric, peers equal to aggregators and clients are equivalent to sensors. What differs in BBox-Iot is, clients only broadcast the transaction to the peer and the peers are responsible for the signing of the transaction. In Hyperledger Fabric, clients collect signed transactions and send it to ordering services which a lightweight device cannot perform.

As the consensus protocol permissioned blockchain setting is used, where a trusted party authorizes system participation at the aggregator level. The trusted party doesn't necessarily need to be present and only required for high-level administrative operations.

In the overall structure; a MSP is a trusted third party and is responsible for authorizing participation in the system. The orders complete consensus on forming new blocks. Local administrators are responsible for its group membership, which are a set of aggregators and sensors. A set of aggregators act as peers in Hyperledger Fabric. Aggregators have the ability to perform regular cryptographic operations and they collect data from sensors. Sensors are constaried devices; they are equivalent to the clients in original architecture.

BBox-IoT, can eliminate a possible man in the middle attack in all cases where there is more than one aggregator in the proximity of the sensors. Its consensus protocol is also resistant against denial of service attacks. The structure works with 8 bit sensors and 16 MHz microcontrollers with 2 KB RAM. It broadcasts data every 10 seconds which in the end is submitted to the cloud infrastructure. In comparison to ECDSA, which is the industry standard, BBox can do more than 5000% signing and verification operations with the same amount of power.[4]

2b. Blockchain as a Service for IoT:

Blockchain technology guarantees tamperproof storage of approved transactions. It also provides distribution and decentralization. Hence IoT technology can benefit from its implementation to IoT based networks for managing device configuration and/or store and broadcast of sensor data. However this is challenging due to low computational power and insufficient bandwidth and limited battery. Therefore the challenge is to find a host that can utilize blockchain technology. This paper suggests and evaluates the performance of network latency when cloud and fog are used as the hosting platform for blockchain.

The fog and cloud technology are both equally well suited platforms for blockchain. They have conflicting characteristics regarding computational resources and latency. Fog is limited by computational resources however it has low latency. Cloud can scale out and overcome the computational resources however it comes with a price of significant latency issues.

For evaluation purposes Intel Edison Arduino boards(as edge device) are used consisting of; 500 MHz dual core with System on a chip dual threaded Intel Atom,100 MHz 32-bit Intel Quark microcontroller and Uno R3 compatible Edison breakout board. The Edison board is connected to wifi hotspot with three standard workstations that host python servers each interacting with a multichain node. In the experiments, an Edison board executes ten simultaneous write requests of 720 bytes to the python server. We vary the arrival rate of the write requests by adding different delays which can be 0, 50,100, 150,200, 250 and 300 milliseconds and observe the results. Before focusing on IBM's Bluemix blockchain, we make sure that local private multichain is not a bottleneck. Hence the traffic on the Edison chip will determine the performance.

The results demonstrate that changing the arrival time does not necessarily give a better answer so there is no observable correlation. This may be due to the latency occuring while interacting with the cloud services. Observing the output charts of latency one can conclude that fog gives better performance with lower latency.[5]

2c. A Lightweight Blockchain-Based IoT Identity Management Approach

One use for IoT devices is Identity management. Identify management is a framework that provides authentication to authorized users. Identity management on IoT devices could benefit from the added accountability of Block chain. Unfortunately, blockchain requires significant computational power and struggles to run, or flat out cannot run on low power IoT devices. “A Lightweight Blockchain-Based IoT Identity Management Approach”, by Mohammed Amine Bouras, Qinghua Lu, Sahraoui Dhelim and Huansheng Ning, proposes solving this problem using a Consortium blockchain.

A Consortium blockchain is a permissioned blockchain, a type of blockchain that requires nodes to be authenticated to the network. Nodes in a consortium blockchain work together to authenticate or deny new nodes access, set domain policies for the consortium, and distribute work.

Identity management encompasses all nodes, users, smart appliances, and applications in an IoT ecosystem. All of these endpoints and nodes should be able to authenticate with the identity management system. The consortium will include a membership service that can add, remove, and authenticate members as needed. The Consortium consists of four layers.

The highest layer of the Consortium is the Management and governance layer. This layer is responsible for the Identity Management protocol and the Consortium Membership Management. The Identity Management protocol performs three main functions. It can register and revoke certificates for new users in addition to providing authentication for each user. Consortium membership management can issue and revoke Certificate Authorities, controlling who can and can not authenticate with the network.

The second layer is the Data layer. This layer consists of a revoked certificates repository and an issued certificates repository. Both of these repositories are stored “off chain” (not

computed in the chain.) These repositories are used in conjunction to validate users using certificates.

The final layer is the Blockchain layer. The blockchain layer uses smart contracts, a protocol to allow the identity management protocol to add items to the block chain ledger. The blockchain computation is distributed around the consortium utilizing roles defined by the Consortium membership management.

Takeaway on Consortium blockchain. A consortium blockchain tries to leverage a network of IoT devices to distribute the computation of blockchains. Its proposed methods include a central controller, and identity management protocol to handle authentication and blockchain computation distributed across the consortium member nodes. The consortium assumes there is a locally connected network of IoT devices, and that not all devices will be processing all the time. This model would not work if only one IoT device is available, or if every device is already computationally taxed.

2d. IoT Blockchain for Smart Sensor

IoT Blockchain for Smart Sensors, byVladimir Voicu, Dorin Petreus and Radu Etzbegins, is making the argument that one of the most important features of IoT devices is access control, and that the best way to secure IoT based access control is blockchain. This paper suggests that, with an estimated 18 billion connected IoT devices by 2022 (the article is from 2020) that the need for secure access management is more important than ever and will continue to grow. Blockchain consists of four components.

Nodes are the first component of blockchain. Nodes operate by storing all current transactions on a blockchain network. A transaction can be any form of authentication and can be human, node, or sensor value authentication. Once complete the transaction is added to the end of a ledger, more commonly known as Mining.

A Distributed Database is the second component of blockchain. A distributed database contains blocks of data from every transaction in the blockchain network. A transaction has 3 parts: A list of transactions, a timestamp, and information about previous transactions in the chain.

The Ledger is the third component of blockchain. The ledger is a database of all previous transactions. The ledger is publicly available, and a separate copy is kept on every node in the blockchain network.

And finally Cryptographic functions. The hash from the previous block is added to the current block and then hashed, usually with SAH256. The has from this block is then added to the next block. Blocks are then publicly published. This allows each block to be accountable for the block before it, effectively "chaining" the blocks together. This is where the chain in blockchain comes from.

This article focuses on incorporating blockchain into an IoT weather station. In this example, a small weather station is created. Because the data points on the weather station are space, compared to other devices, and the system has some computational overhead. This device is able to hash blocks and create a blockchain of variables while keeping computational resources low.

Takeaway on IoT Blockchain for smart sensors. This article investigates how blockchain works and how it can be applied in IoT smart sensors. It makes that argument that, while computationally expensive, devices that require little power and have few data points can compute blockchain without much difficulty while providing added security. This approach works for sensor networks, but will not scale well for larger networks and for nodes with more complex tasks.

3. Methods / Approach

3.1 Methods

To effectively analyze and compare each solution for lightweight cryptography in blockchain for IoT applications, we realize that there are 3 major challenges when developing a solution. The first major challenge is computational efficiency. This is the major blocker to the implementation of blockchain in IoT settings, and is the primary evaluator for a solution. The second major challenge is security, IoT data has a lot of private and sensitive data that needs to be protected. Lastly, it is imperative that each solution is scalable, as IoT data will only continue to increase as more devices join the interconnected networks.

A major challenge for us when carrying out this procedure is that each paper does not discuss its effectiveness in handling all three challenges. To overcome this, we will discuss in detail the approach of each paper and use that to surmise its effect on each area of our criteria.

The main methodological limitation of our survey paper is that there is no uniform scale upon which we can quantitatively assess each solution's performance against our criteria. Our analysis is strictly qualitative.

Each group member will handle the analysis and discussion for one criteria in our analysis.

Analysis Results:

3. Results and Contributions

This Section should summarize the results and highlight project's contribution; include a discussion on what problems can be addressed; list concrete examples.

4. Conclusions / Summary / Recommendations

This section is should provide a short summary of the projects activities and results. A conclusion section contains high-level material that refers to the main part of the paper (methods) and was not included in the introduction, including solution proposed, main results, and significance of the project compared with other existing solutions.

If relevant, indicate if there are any suggestions for further development of the work done.
Recommend some further research or a change in practices.

5. REFERENCES

[1] F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1101–1102, 2012.

[2] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (IOT) forensics: Challenges, approaches, and open issues,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[3] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” 2018.

[4] Chatzigiannis, P., Kolias, C., Baldimtsi, F. and Stavrou, A., 2021. *Black-Box IoT: Authentication and Distributed Storage of IoT Data from Constrained Sensors*. [ebook] Available at: <https://computing.ece.vt.edu/~angelos/research/iotdi2021-final114.pdf> [Accessed 10 November 2021].

[5] Samaniego, Mayra, and Ralph Deters. "Blockchain as a Service for IoT." Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on. IEEE, 2016.

Use one consistent system for citing works in the body of your report. Several such systems are in common use in textbooks and in conference and journal papers. Ensure that any works you cite are listed in the references section, and vice versa.

IEEE standards for citation should be used (check the IEEE citation standard uploaded in the resources)

Make sure any sites used as sources are mentioned as well.