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

The Internet of Things (IoT) is an emerging technology space that uses the interconnected network of personal devices to offer valuable and timely functionality to their users. However, IoT networks are very comprehensive and contain sensitive personal data, and any implementation must be able to maintain efficiency with a large number of users as well as security. Blockchain, with it's immutable data and decentralized structure, seems like a natural solution to the problem of data management.

In this paper, we analyze the different applications and approaches towards leveraging blockchain technology in IoT applications with a goal of identifying specific features or design implementations that ensure efficiency, scalability, and security.

After surveying five papers, we have recognized that the use of permissioned blockchain networks, cloud technologies, and using both of these technologies to minimize the computational load on local IoT devices can ensure that the system is efficient, scalable and secure.

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. [6] 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. [7] 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. [1] 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. [2] 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. [3]

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.[8] 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. [9]

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 proposed solutions and their implications for the field, we would like to extract useful technologies and design architectures that enable an application of blockchain in IoT to be efficient, scalable and secure.

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. We have also been very limited in the amount of papers we have been able to analyze as research in this area is ongoing and recent, and as a result a lot of papers are protected behind memberships.

Overview:

In this paper, we review five papers on the implementation of blockchain and IoT technologies. Our purpose is to examine each approach and determine the ways in which the complete architecture can be improved. For this we gave brief summaries of each paper in ‘Literature Review’, our methodology and approach on the problem and analyzed each paper in terms of Security, Efficiency and Scalability in the ‘Results and Contributions’ part. At the ‘Conclusion and Future Work’ we briefly discuss the deductions we made based on the literature review and mention what our next steps will be to advance our research.

2. Literature 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.[13]

2d. IoT Blockchain for Smart Sensor

IoT Blockchain for Smart Sensors, by Vladimir 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.[12]

2e. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT

The paper “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT” introduces a novel approach to assigning roles and permissions to nodes in an IoT based access control system.

The key issue this paper tries to address is replacing a centralized access control system design with a decentralized access control system design. To accomplish this goal the researchers apply their new decentralized access control system model to a geographically distributed sensor network. This is possible due to the adoption of blockchain.

Blockchain allows nodes to communicate with each other in a secure fashion that enforces non-repudiation. These advantages allow decentralized networks to grow while still being able to maintain secure communication.

The new approach in this paper brings four advantages. This approach is highly mobile and can be used in isolated networks or within existing networks. Because individual IoT devices are not required for this network and all nodes in the network keep a complete copy of all transactions at all times, it is accessible at any given time regardless of if a node is in the network or not. This approach is lightweight and will run on most IoT devices without modification. And finally, this approach is highly scalable by simply adding in new managers and management hubs to handle new nodes.

This architecture does not include IoT devices in the blockchain, instead opting to have all IoT communicate with a Management Hub. The management hub operates by requesting access control information from the IoT devices and performs blockchain operations on the submitted access control information.

All devices in the blockchain network have a smart contract with the management hubs and other nodes in the network. This contract is edited by a manager and sent to all the nodes and management hubs as policies.

“Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT” proposes a solution that incorporates multiple layers in the access control system. Decentralized

IoT devices will communicate with local management hubs to perform blockchain actions. Management hubs are decentralized and communicate with a decentralized blockchain network and are controlled by managers which create network policies. This approach allows decentralized IoT devices to participate in a blockchain network that can be managed from one or two locations.[14]

3. Methods / Approach

3.1 Methods and Approach

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. At the end, we aim to compare the different applications in each criteria and extract design techniques and the methodologies that contribute to fulfilling each criteria. With a recognition and analysis of certain design decisions or approaches that lead to better efficiency, scalability and security, we believe that this paper will help inform all members in the field as to how they can approach implementation of Blockchain in IoT networks.

4. Results and Contributions

Results:

Security:

Black Box IOT Solution:

The black-box IoT solution consists of certain implementation design decisions in order to ensure the security of the system and the data it contains.

One of these design decisions is the utilization of a novel hash-based digital signature to ensure data integrity and confidentiality. This signature in conjunction with the immutable Blockchain Ledger ensures that the system heavily mitigates the potential of a successful man-in-the-middle attack.

Furthermore, the black-box IoT solution utilizes a permissioned Blockchain network, which ensures that every participant on the network is approved and that only certain individuals can add or remove sensors or other data entities in the chain. This protects the network from dealing with excess and fraudulent sensor reports while also ensuring no sensors or devices are maliciously removed from the network.

While the Black-Box IoT system can't prevent physical tampering with sensors or other devices, the system is equipped to recognize any data discrepancies. The only way for data discrepancies to not be detected is if an attacker manages to physically tamper every sensor in the chain, which requires a prodigious effort from nefarious entities.

Lastly, as the Black-Box IoT system's permissioned network is built to be very scalable, the system is resistant to denial of service attacks.

Due to specific design decisions made with security considerations in mind, the Black-Box IoT system handles a variety of potential attacks. Due to the use of a permissioned network and it's consensus protocol, a custom hash signature scheme, and design robustness, the Black-Box IoT system is resistant to a variety of man in the middle attacks, denial of service attacks and can also detect any data discrepancies or bad actors in the system.

A Lightweight Blockchain-Based IoT Identity Management Approach

This solution leverages the use of a consortium blockchain which is a type of permissioned network. This means that there is a group of participants that act as an authority on the network and set protocols, add and remove entities. This helps keep the network secure as it ensures that the data on the network can only be modified by certain validated entities, and furthermore ensures that participants in the network are pre-approved and validated. This increases complexity for attackers as they need to exploit the approval process to get access to the network.

For Identity Management and verification, the solution uses the hash of the concatenation of the encrypted custom id and the metadata for the entity, ensuring both id confidentiality and data integrity.

The approach towards security here is based upon the assumption that a permissioned network in conjunction with an identity management layer would prevent any bad actors from interacting in the network. However, there is no acknowledgement of attacks on the physical layer, such as sensor tampering, or the possibility of an attacker breaking the identity verification algorithm and gaining access to the network's data.

Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT

This paper mentions that the management hub is susceptible to spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges attacks. While the blockchain itself ensures data confidentiality and integrity, the management hubs which manage the IoT devices are susceptible to these attacks as a fraud management hub could enter the network and interact with the devices. The paper does mention that utilizing a signature scheme for management hubs could prevent many of these attacks, however it could have an adverse effect on efficiency.

Overview:

______ Both IoT for Smart Sensors, and Blockchain as a Service for IoT were focused on physical applications, and as a result had very minimal discussion on security.

On the other hand both BlackBox IoT and the identity management approach had substantial discussion on how they ensured security of the network. With both applications, it is clear that using a permissioned blockchain helps alleviate many security concerns, than using the more standard permissionless chain. Also, both papers use a form of a hash signature for verification that is both secure and efficient.

BlackBox IoT's approach to security seems to be the most comprehensive as the paper specifically names the two prevalent attacks it is resistant to, man in the middle and denial of service attacks.

Scalability:

One of the critical factors for Blockchain for IOT devices is scalability. A blockchain network consists of many distinct nodes, and must be able to grow and shrink as new nodes enter and leave the network. This is a comparison of scalability traits and tradeoffs between our analyzed papers.

BlackBox IoT introduces the idea that all transactions do not have to be tied to a clock, but are rather tied to hash-based digital signatures. A hash-based algorithm can be used across an entire network, and is not limited to the number of participating nodes. This is a novel method that can easily scale up and down to the size of the network.

A consortium network, as introduced in Lightweight blockchain-based IoT Identity management approach and used in BlackBox IoT, creates a network of nodes each with their own roles in the network. Management nodes are responsible for letting new nodes into the network and assigning tasks. In this model the speed at which the network can scale is dependent on the management nodes, the network can scale as fast as the management nodes will allow. Consortium networks can, and will scale easily, but require additional computational resources as it scales, which can become a burden on large scale networks.

BlackBox IOT operates on the principle that all transactions are not tied to a clock, but are rather tied to hash-based digital signatures. BlackBox IOT is a consensus-based protocol that utilizes trusted third parties to provide trust to the nodes in the network. Because the hash-based digital signature requires little computational overhead this model can scale as large and as fast as the consensus based trusted third parties will allow.

Blockchain as a service for IoT focusses on latency differences between a cloud and fog network. A fog network is a network composed of strictly local nodes, forming a low lying cloud (or fog). This paper concludes that blockchain as a service does not benefit from a fog network over a cloud network, but that a fog network is scalable the same as the cloud network.

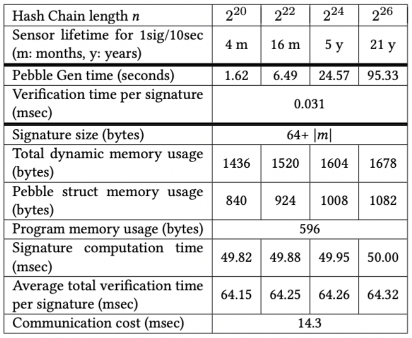
A Lightweight Blockchain-Based IoT Identity management approach introduces the concept of a Consortium blockchain, which is used as the basis of BlackBox IoT paper. Just like BlackBox IoT, any consortium based block chain will be able to grow up to the extent that the manager node can handle. Once a management node is maxed out more management nodes can not be added. Consortium blockchains are scalable, but require additional overhead to grow beyond a certain point.

IoT Blockchain for Smart Sensors looks at devices based on gathering telemetry, be it weather, access, tempter, ect. This article suggests that smart sensors will be computing minimal amounts of information and will have the computational overhead to perform blockchain actions locally. This method works on individual nodes, but does not scale, as different devices may not be able to compute their own blockchain operations.

Efficiency:

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

One of the most important aspects of IoT settings is energy efficiency. Considering the energy efficiency of the BBox-IoT system, the microcontroller can perform more than 50x hash based signing operations compared to the equivalent ECDSA operations for the same amount of power.



Hash Chain length *n*	2^{20}	2^{22}	2^{24}	2^{26}
Sensor lifetime for 1sig/10sec (m: months, y: years)	4 m	16 m	5 y	21 y
Pebble Gen time (seconds)	1.62	6.49	24.57	95.33
Verification time per signature (msec)	0.031			
Signature size (bytes)	64+ $\|m\|$			
Total dynamic memory usage (bytes)	1436	1520	1604	1678
Pebble struct memory usage (bytes)	840	924	1008	1082
Program memory usage (bytes)	596			
Signature computation time (msec)	49.82	49.88	49.95	50.00
Average total verification time per signature (msec)	64.15	64.25	64.26	64.32
Communication cost (msec)	14.3			

Figure 1: Evaluation for sensor-aggregator protocol 5000 verifications

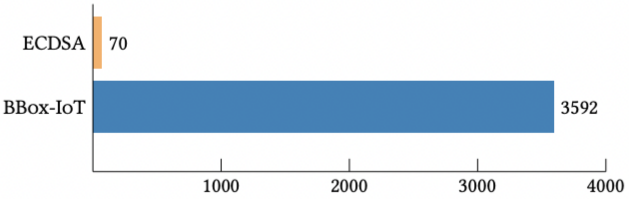


Figure 2: Number of signing operations for a 20mWh battery

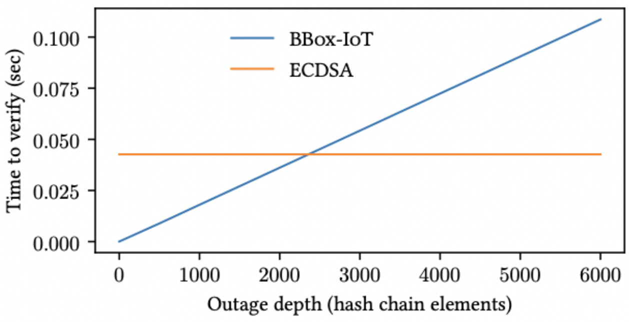


Figure 3: Aggregator verification costs in network outages

Considering a single transaction the time passed from the aggregator proposed a value until consensus is reached on it is 0.5 sec for Hyperledger Fabric.

We want to estimate the time from a value being proposed by an aggregator until consensus has been reached on it (assuming the block contains a single transaction). Again we can adopt previous evaluations in Hyperledger Fabric, which show an average of 0.5 sec for the complete process.

A block size of 2MB, a Hyperledger block could hold (at most) about 15800 signed sensor data using our hash-based scheme vs. 12700 using ECDSA.

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]

b. Blockchain as a Service for IoT:

In the experiments, an Edison board executes ten simultaneous write requests of 720 bytes to the python server. The arrival rate of the write requests are varied by adding different delays that are 0, 50,100, 150,200, 250 and 300 milliseconds and the result is observed.

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. The performance analysis clearly indicates that the network latency is the dominant factor. Observing the output charts of latency one can conclude that fog gives better performance with lower latency. Consequently, the fog outperforms the clouds' efficiency.

Performing complex blockchain operations on cloud/fog environments is efficient for the design of lightweight blockchain and IoT architectures.[5]

c. A Lightweight Blockchain-Based IoT Identity Management Approach

In this work, a permissioned blockchain is used to leverage a decentralized, secure, and fast solution. The average writing time of 1 MB transaction can take around 205 ms and the average reading time is 69 ms.

0.5 MB block size is tested for maximizing the throughput of both registration transactions and authentication transactions, executing 100 trials for each action. The average time of registration invocation transactions is 170 ms with a throughput of 6 transactions per second.The average time of query transactions is 52.5 ms with a throughput of 19 transactions per second.

The average time of authentication invocation transactions is 145 (Ms), with a throughput of seven transactions per second.

d. IoT blockchain for Smart Sensor

In this paper the focus of design is related to the security and accuracy of the architecture rather than efficiency.

e. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT

The addition of the management hub node in the blockchain system affects the latency of the access control operations. The performance evaluation is as follows;

In the first scenario, a set of virtual IoT devices are connected directly to the management hub and the virtual clients request the access information of a certain IoT device to a resource in another IoT device. Once the request is received the information is fetched from the blockchain and the virtual client gets a response. In the second scenario, the performance of an IoT device is connected to a management hub node and a set of virtual IoT devices request the resource information of another IoT device.

In both cases, all requests from the blockchain network are supplied to all resources. The tests measured five times, for 30 s each time, to calculate the average values and the number of concurrent clients ranged from 1 to 10 000.

In the first case, the throughput in the management hub increases from 500 requests per second until it achieves a steady throughput of 950 requests per second with ten concurrent clients reaching their maximum capacity. In the second case a steady throughput at 500 requests per second during all the tests and all the concurrent clients request the resource information from a single IoT device therefore the latency between the management hub and this single IoT client limits the whole performance of this case. Generally, in both experiments, the limiting factor is the latency to fetch the access control information from the blockchain network. That latency decreases the performance of our system.

5. Conclusions / Future Work

After analyzing the papers and their different approaches to utilizing Blockchain networks to manage the necessary data for IoT systems. We have recognized certain features and design decisions with implementation of Blockchain in IoT systems that leads to better performance in the areas of efficiency, scalability, and security.

The utilization of permissioned blockchains was prevalent in both BlackBox IoT and the Identity Management approach to IoT. A permissioned blockchain, as opposed to the standard permissionless blockchain, requires users to be approved before participating in the network and furthermore, adhere to a role or entity within the network. This lends nicely to IoT applications, because while permissioned blockchains take advantage of the decentralized data storage, it allows for certain classes of users to operate as administrators and manage the entities within the chain. [10] Furthermore, permissioned networks simultaneously address all aspects of security, scalability and efficiency. As the consensus protocol is less computationally expensive, permissioned networks are often far more efficient and scalable than permissionless networks. [4] On the security side, permissioned networks prevent any user without approval and verification from joining a network. Moreover, only entities of a certain privileged class have access to all of the data in the network, due to the partially decentralized nature of permissioned networks.[11] With this understanding, we believe that permissioned blockchain networks address many implementation challenges in IoT systems, and should be further explored in different applications and approaches.

In blockchain applications the number of transactions required can be very large. Therefore there should be powerful data processing services within the architecture to perform the transactions. In that sense cloud provides on-demand computing resources due to its high scalability. Hosting blockchain operations on IoT devices are not applicable due to resource constraint nature of the devices. There are problems of power limitations, lack of sufficient bandwidth and lack of computational resources. Therefore performing blockchain operations which are computationally heavy and complex can be realized by environments like cloud and fog. Cloud hosted applications scale out and can overcome resource constraints at the price of latency. Other advantages of combining blockchain technology with cloud computing are decentralization, improved security and scalability.

Most of our surveyed papers touch on blockchain workload per IoT node. Iot Blockchain for Smart sensors explores the idea that the responsibilities of a node should be low enough that all blockchain encryption can happen locally. This can be accomplished leveraging cloud technologies. Several papers utilize Consortium networks, as introduced by A Lightweight Blockchain-Based IoT Identity management approach, to distribute workloads among nodes in the network. This approach allows IoT nodes that have large computational needs and nodes that have low computational needs to efficiently distribute the blockchain workload

The contribution of our paper is the comprehensive comparison of multiple applications of blockchain in IoT from which we extricate that the utilization of permissioned blockchain networks, cloud technologies and minimizing local workload on IoT devices through the use of either the permissioned network or cloud computing, can help address the requirements of efficiency, scalability and security.

Future Work:

Our next steps to further our research in this paper is to test the specific design decisions that we have created and quantify their impact on security, scalability and efficiency. So we would construct a simple permissioned blockchain network, and a permissionless blockchain network and utilize them in a simple controlled IoT environment where we can measure how long it takes to handle data and process requests, how performance reacts to multiple new entities and nodes, and lastly analyze each network on it's resistance to common security threats to blockchain and IoT networks. We would perform a similar type of procedure with a cloud based application as well as with a network that minimized computational workload on the IoT devices themselves.

Isolating these features will help us quantify the individual impact that each of the features we extracted have on the areas of efficiency, scalability, and security.

Following this, we would like to implement our own solution to IoT data management leveraging a Blockchain Network that uses each of these features and compare it to existing solutions in the research space and industry.

6. 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.

[6] “Build trust in your IOT data with Blockchain,” *IBM*. [Online]. Available: https://www.ibm.com/topics/blockchain-iot.

[7] L. Horowitz and L. Rosencrance, “How blockchain technology can benefit the internet of things,” *IoT World Today*, 31-May-2021. [Online]. Available: https://www.iotworldtoday.com/2021/05/31/how-blockchain-technology-can-benefit-the-internet-of-things/.

[8] “What is ‘proof of work’ or ‘Proof of stake’?,” *Coinbase*. [Online]. Available: https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake. [Accessed: 12-Dec-2021].

[9] J. Frankenfield, “Proof of stake (POS),” *Investopedia*, 05-Oct-2021. [Online]. Available: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

[10] J. Frankenfield, “Permissioned blockchains,” *Investopedia*, 19-May-2021. [Online]. Available: https://www.investopedia.com/terms/p/permissioned-blockchains.asp.

[11] “Introduction to permissioned blockchains,” *101 Blockchains*, 01-Nov-2020. [Online]. Available: https://101blockchains.com/permissioned-blockchain/. [Accessed: 2021].

[12] "IoT Blockchain for Smart Sensor," https://ieeexplore-ieee-org.ezproxy.lib.vt.edu/document/9120915 [Accessed: 2021].

[13] “A Lightweight Blockchain-Based IoT Identity Management Approach”

https://mdpi-res.com/futureinternet/futureinternet-13-00024/article_deploy/futureinternet-13-00024-v3.pdf

[14] “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT”
https://ieeexplore.ieee.org/abstract/document/8306880