Surveying Blockchain Designs for IoT devices

Satish Venkatesan, Jamous Bitrick, Deniz Aytemiz

Introduction and Background

- The Internet of Things is a rapidly growing concept where devices all around the world are interconnected
- Internet of Things, however, requires a system to manage the data
- Blockchain is one proposed solution
  - Maintain Data
  - Scalable
- However, any design needs to address
  - Security
  - Efficiency
  - Scalability

Approach and Outline

- We analyzed five different research papers with criteria of
  - Security
  - Efficiency
  - Scalability
- First, we will summarize the papers we analyzed
- Second we will offer our analysis on the areas of security, scalability and efficiency
- Then, we will list our conclusions and contributions
- Lastly, we will discuss future steps

BlackBox IoT

BlackBox Iot focuses on the concept of Blockchain for access management.

- Suggests that access management through lightweight IoT devices will be a critical part of infrastructure going forward.
- Suggests that Blockchain will be critical in enforcing non-repudiation for access control systems.
- Uses a novel hash-based digital signature algorithm with a one time hash chain.
    - The network will use this digital hash to synchronize nodes on the network, allowing computation to be done when the workflow is light, rather than instantaneous or with a synchronized clock.

Blockchain as a Service for IoT

This paper identifies blockchain as a critical service for transactions now and in the future. It analyzes the impact of Latency on the network using both Cloud and Fog servers.

- A fog network is a network close to the original source. For this paper the researches build servers on the same LAN as the IOT devices
- For this paper researchers also built blockchain servers in the cloud.
- The results of this research determined that arrival time and latency between and IoT node and a blockchain server, had no effect on improving performance or reducing the workload of the network.

IoT Blockchain for Smart Sensor

This paper approaches the problem of Blockchain for IoT devices with the concept of limiting the number of transactions on a device.

- Explores the operation of blockchain.
- Suggests that IoT devices are critical for access control.
- Suggest limiting responsibilities of an IoT device to the extent that all blockchain operations can be performed on that device.

A Lightweight Blockchain-Based IoT Identity Management Approach

This paper introduces the idea of a Consortium blockchain, a network type being adopted across the industry.

- A consortium blockchain is a network with individual nodes with different tasks.
- Certain nodes in the network are designated management nodes
  - Management nodes are responsible for letting members enter and exit the network.
  - They are also responsible for assigning functions to members of the network.
- This network type allows the most efficient use of each node in the network, and has been implemented in other networks and papers, such as BlackBox IoT paper, which was also surveyed in this project.

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

Blockchain Meets IoT is a novel approach to creating a decentralized distributed blockchain network.

- IoT devices talk with local management hubs, who perform blockchain actions.
- Management hubs are part of a larger, decentralized blockchain network.
- Managers create policies for the network and management hubs.

Security

Black-Box IoT:

- Permissioned Network
- The use of a novel hashing solution ensures data confidentiality and integrity
- Design is resistant to Man in the Middle Attacks and Denial of Service attacks

A Lightweight Blockchain-based IoT Identity Management Approach

- Consortium Network
- Identity management system resists bad actors from joining network
- Use of hashing for identity verification

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

- Susceptible to multiple attacks, however utilization of signature scheme would increase security

Scalability

One critical component of Blockchain networks is scalability. A scalable network can be implemented in many distinct systems easily and repeatedly.

- BlackBox IoT operates on the principle that all transactions can be tied to one has function rather than time. THis approach is scalable, because the hash function is valid regardless of the size of the network. This is the most scalable model in our research.
- A Lightweight blockchain-based IoT identity management approach introduces the concept of consortium blockchain. A consortium blockchain uses management nodes to add members and delegate tasks. The consortium can scale up or down as fast as the management nodes will allow, and may require additional nodes as the network grows.
- IoT Blockchain for smart sensors focuses on individual nodes in the network, and suggests that devices should only process as much input as they can compute. This model does not scale, and crumbles if a device requiring high resource utilization is added to the network.

Efficiency

Black-Box IoT Consensus Performance:

The most important metric in the system is the transaction throughput which heavily depends on the ability of the SWaP sensors to transmit data in a group setting.

	BBox-IoT		ECDSA	
Message length	Sensor Sign	Aggr Vrfy	Sensor Sign	Aggr Vrfy
50	50.43	0.0339	4200	42.55
100	53.47	0.0349		
150	56.40	0.0357		
202	59.33	0.03687		
218	60.06	0.0369		
Signature size	32		64	

Table 6: Signing and verification costs (in milliseconds) compared with message and signature sizes (in bytes). Note we assume hash-based signatures are aggregated as discussed in Section 5.3. Signer is ATmega328P microcontroller and verifier is RPi 3.

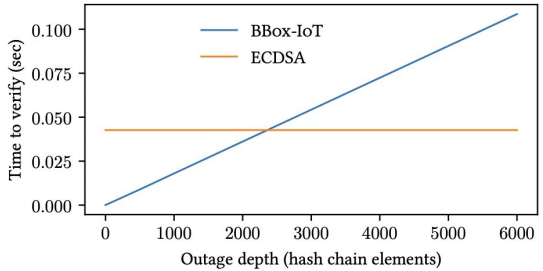

Figure 4: Aggregator verification costs in network outages. BBox-IoT is more expensive when more than about 2400 signature packets are lost.

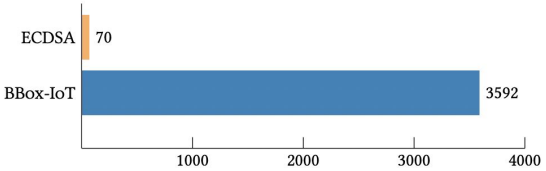

Figure 5: Number of signing operations for a 20mWh battery.

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.

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-IoT can do more than 5000% signing and verification operations with the same amount of power.

Efficiency

Blockchain as a Service for IoT: Fog or Cloud?

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 cloud.

A Lightweight Blockchain-Based IoT Identity Management Approach

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.

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

The latency between the management hub and this single IoT client limits the whole performance.

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.

Conclusion & Future Solutions

In our research we were able to identify several new methods of applying blockchain technology to IoT devices. Some key technologies are:

- Consortium blockchains: A secure, scalable, and robust solution that efficiently distributes blockchain computation across the network.
- Blockchain meets Iot: A decentralized network for access control with local IoT devices where computation is sent to a local manager, which is part of a larger decentralized blockchain network.
- BlackBox Iot: A novel has algorithm that replaces the need for time synorchy between blockchain nodes, allowing distributed and underpowered blockchain nodes to compute and add entries without being real time.