Computers, Materials & Continua
DOI:10.32604/cmc.2021.018942
Article

Tech Science Press

A Lightweight Blockchain for IoT in Smart City (IoT-SmartChain)

Zakariae Dlimi*, Abdellah Ezzati and Saïd Ben Alla

Hassan First University of Settat, Faculté Sciences et Technique, LAVETE, Settat, 26000, Morocco
*Corresponding Author: Zakariae Dlimi. Email: Zakariae.dlimi@gmail.com
Received: 27 March 2021; Accepted: 27 April 2021

Abstract: The smart city is a technological framework that connects the city's different components to create new opportunities. This connection is possible with the help of the Internet of Things (IoT), which provides a digital personality to physical objects. Some studies have proposed integrating Blockchain technology with IoT in different use cases as access, orchestration, or replicated storage layer. The majority of connected objects' capacity limitation makes the use of Blockchain inadequate due to its redundancy and its conventional processing-intensive consensus like PoW. This paper addresses these challenges by proposing a NOVEL model of a lightweight Blockchain framework (IoT-SmartChain), with a lightweight consensus and a lightweight structure. The framework architecture presents a role hierarchy of connected objects according to their computational and storage capacity. This organization allows all things to be linked even indirectly via different interfaces and to benefit from the power of high-capacity objects such as Fog and Edge computing nodes. Data is validated and added to the blockchain ledger by running a lightweight consensus called Proof of Random Participation (PoRP), which reduces the blockchain nodes' high computing power requirement. The TOPIC subscription-based data storage strategy called Assisted Selected Relevant Data in Local Ledger (ASRDLL) reduces the data size of a node's local ledger and the entire network's data size. This strategy is assisted by a centralized algorithm that optimizes the overall network size by adjusting the choice of TOPICS. The storage capacity, computational power, and energy consumption have been evaluated by a proof of concept implementation under NodeJS.

Keywords: Smart city; Internet of Things; blockchain; lightweight consensus; lightweight ledger; Iot-SmartChain

1 Introduction

The smart city is a technological framework used by the different city stakeholders to achieve different goals such as better governance, improving daily living conditions, optimizing the resources use, or creating new business opportunities. The contributors of the smart city, whether they are technology providers, managers, or researchers, have carried out several designs, standardization, and improvement studies to respond to the challenges of smart city development

in terms of scalability, heterogeneity, security, or connectivity [1]. As a major direction, IoT is considered as an enabler of smart city maturity [2], and different architectures have been identified [3]. Different studies in different use cases have proposed integrating Blockchain technology in IoT architectures [4], providing security, decentralization, and traceability. For example, the authors in [5] propose the transfer of IoT sensor data via Bitcoin transactions. Application areas include smart transportation [6–8], smart home [9], smart healthcare [10–12], and smart agriculture [13]. The Blockchain, a distributed ledger, replicated by all nodes in its peer-to-peer network, without a centralized trust entity, and keeping the history of all transactions performed, provides security through its consensus that all nodes have adopted [14]. The most conventional consensus, PoW, is based on cryptographic algorithms for authentication, transaction validation, and ledger creation. This way makes it very computationally intensive [15]. These characteristics of the conventional Blockchain model make it unsuitable with IoT components with limited capabilities [16].

The main challenges of integrating Blockchain with IoT are:

- The consensus algorithm needs large computational capacity, increasing the size of the peer-to-peer blockchain network.
- With its replication and exponential evolution, the linear structure of the ledger needs large storage capacity, either for a single node or for the whole smart city network.
- Not all IoT components can participate in the peer-to-peer network to replicate the ledger or the consensus algorithm.

To overcome these problems, several studies have explored the field of lightweight Blockchain structure [17], or outright a model without Block or Mining, as Direct Acyclic Graph, with a central entity that decides the regulation of the network's sustainability. The study is motivated by the IoT domain's monetization and proposing the IOTA crypto-currency [18]. The consensus algorithm used in the Blockchain also impacts its complexity, which motivated the researchers to study alternatives to the conventional proof-of-work (PoW) consensus characterized by its very high complexity [19]. Integrated with IoT, the choice of nodes that participate in the Blockchain consensus is important because connected objects are known by their limited capacity in computation and storage resources. In an integration model with a private Blockchain, the Proof of Block & Trade (PoBT) algorithm has been proposed as a lightweight consensus [20]. On the other hand, IoT can take advantage of the resources of Fog computing, a technology that brings computational capacity closer to connected objects and gains response time in the network [21].

1.1 Research Aim

This research work is mainly motivated by the existing problems in IoT at a smart city scale. Indeed, most of the Blockchain techniques focus on lightweight consensus algorithms. Simultaneously, the conventional structure does not follow the scalability at the IoT size, which increases the solution complexity and its size in the network due to the replication aspect in all Blockchain nodes. Although some studies have taken resource consumption optimization to a considerable level, they have put the Blockchain's trust at risk by the involvement of a decisive central body in the validation of transactions. This work's main objective is to minimize the complexity and consumption of the existing Blockchain technology to make it suitable for the IoT context while keeping the Blockchain features: decentralization, disintermediation, security, and traceability. This research work focuses on a lightweight Blockchain algorithm and a smaller ledger structure to achieve this goal.

1.2 The Main Research Contributions

The design of a novel Blockchain framework for the IoT environment in a smart city (IoT-SmartChain) is the major contribution. The following items decline it:

- An architecture presents a roles hierarchy of the connected objects according to their computation and storage capacity. This design allows to link all things, even indirectly via different interfaces, and to capitalize on the power of high capacity objects such as Fog and Edge computing nodes.
- A lightweight consensus called Proof of Random Participation to validate Blockchain data in a random and non-predictive way, without giving control power to a node privileged by its computing capacity or reputation. This way reduces the need to hold large amounts of computational capacity by nodes in the Blockchain network.
- A data storage strategy based on a TOPIC subscription called Assisted Selected Relevant Data in Local Ledger (ASRDLL) reduces the data size of the node's local ledger and then the whole network data size. This strategy is assisted by a centralized algorithm that optimizes the global size of the network by adjusting the choice of TOPICS.

1.3 Paper Structure

The rest of this content paper is organized as follows: Section 2 presents the related works and their summary. Section 3 explains in detail the proposed work of the research. Section 4 presents the simulation framework and performance analysis. Section 5 to conclude the contribution.

2 Related Work

In this section, we discuss a review and summary (Tab. 1) of interesting research works that have addressed the topic of integrating the Blockchain with the IoT. A decentralized authentication mechanism based on Blockchain has been used with IoT [22]. To reduce the overhead at IoT devices, the author proposes a lightweight blockchain based on Fog Computing technology. The Fog nodes are considered active nodes of the Blockchain, which authenticate the IoT devices. For key and hash generation, the conventional ECDSA and SHA-1 algorithms are used. For authentication, the system is based on the ID and MAC address. PoW consensus is not suitable, and the security has been decreased by the authentication based on System ID and MAC address, especially since the administrator publishes the addresses.

For the industrial internet of things (IIoT), the author proposes integrating a Blockchain system (LightChain), efficient in resource consumption and suitable for IIoT with limited resources [23]. The Consensus green is proposed, aiming to reduce the difficulty of the challenge and push most nodes to participate in block validations with a remuneration based on collaboration times to maintain the network. A rule is also put in place to delay a node's participation that has just validated a block in the next round to leave the chance of participation to others. The lightweight block structure is proposed, consisting of broadcasting a light content of the block after validation instead of the whole block, accompanied by a block data reduction filter. This strategy consists of storing only relevant data at the node level, with a backup of all history in the cloud. The local data filtering strategy will have no storage reduction effect when all data is relevant. The presence of a cloud data backup will only be an unnecessary double cost to the network, as the data will be replicated to all nodes. The proposed consensus is only suitable for the use case of collaboration without monetization.

Table 1: Summary of related works

Paper	Contribution	Limitation
[22]	Designing blockchain integration model with IoT with reduced overhead on IoT devices	Using PoW increases complexity and resource consumption
[23]	Maintien du réseau de la Blockchain avec l'incitation à la collaboration et à moindre effort.	Maintaining the Blockchain network with the incentive of collaboration and less effort.
[24]	Applying a network flow management strategy	The reduction of block creation iterations impacts the data validation time and the block size
[25]	Securing network access and data through Blockchain.	The use of Pow increases complexity and resource consumption
[26]	Designing scalable Blockchain by network layers	Using Pow increases complexity and resource consumption

A lightweight blockchain model (ELIB) has been proposed for IoT privacy and security [24]. It is based on a strategy of restricting the number of blocks to be generated in order to reduce the computational and processing effort of machines. The author also applied the use of the uncertificated cryptographic model and the management of the flow by a Distributed Throughput Management scheme that adjusts the number of Transactions to be validated concerning the number of Nodes of the network. Reducing the number of block validation iterations will increase the data validation time, which is not adapted to contexts that require reactivity and short processing times.

Blockchain and Fog computing structure has been proposed for the Internet of Everything (IoE) applications [25]. This work secures the smart city network through encryption, authentication, and Blockchain. Here, Fog computing is used only to reduce the latency of the smart city nodes. A decentralized Blockchain validates IoE nodes to maintain network security. The IoT nodes participate in the chosen Blockchain consensus, which is the PoW. This consensus is too computationally intensive and is not adaptable to the IoT context at a smart city scale.

A scalable, lightweight blockchain (LSB) is proposed for the IoT network [26]. The author presents a framework organized in Cluster and whose network traffic and energy consumption are optimized. The network traffic has been reduced by clustering. Power consumption has been reduced by applying a distributed trust approach, positively impacting the load and delay of mining processing. The framework is assumed to work in public Blockchain. Here, PoW consensus was used, which was inappropriate for the IoT environment.

3 Proposed Framework

3.1 Design and Architecture

The present framework has been designed to take advantage of all the Blockchain benefits, whether it is public or permissioned, and to meet the constraints of all connected objects. That said, the Blockchain integrated into our IoT network interconnects the different devices via the most used interface protocols and allows these network devices to participate following their capabilities.

The proposed framework is an IoT network whose components define three logical levels, according to their computational and storage capacities, which we cite, Low Capability Level (LCL), Medium Capability level (MCL), and High Capability level (HCL). In these logical levels, the objects of the network can choose one of these three roles according to their capacities, which we note Perception Activity (PA), Passive Blockchain Activity (PBA), Validation Blockchain Activity (VBA). Tab. 2 lists the possibilities of the roles concerning the logical levels.

Table 2: Roles and logical levels

Logical levels / Roles	LCL	MCL	HCL
PA	V	–	–
PBA	V	V	–
VBA	V	V	V

The Perception Activity role is adopted by connected objects whose mission results in a final action at the physical object level. It does not participate at any time in maintaining the Blockchain network. The Passive Blockchain Activity role is adopted by connected objects whose capacity allows authentication to the Blockchain, transaction creation, transaction signature to be submitted to the Blockchain, and optionally the local storage of the ledger. It does not participate in the validation consensus of new blocks. When the connected object has sufficient computational capacity, it can then participate in the validation consensus of the Blockchain, that what defines the role Validation Blockchain Activity. Authentication of nodes in the Blockchain network is performed in the same way as in conventional Blockchain models, via private and public keys. The nodes whose roles are PBA and VBA, are equipped with MQTT, CoAP, and REST type connection interfaces, which positions them as gateways to the objects whose role is PA, in other words, to expose the Blockchain services directly to them. In the context of smart city, the use of Fog and Edge Computing components has been proposed for network traffic reduction. The different levels of the model architecture are presented in Fig. 1.

The nodes whose roles are PBA and VBA are composed of the following modules and illustrated in Fig. 2, to ensure the functions of the Blockchain: Security module for storing keys and signing, Control module for verification and consistency, Transaction Pool module for storing data not yet added to the Block, Consensus module for validating new data, Ledger module for local data storage, Peer-to-Peer Interface for communication between Blockchain nodes, IoT Interfaces for communication with connected objects, and Configuration module for the various

possible settings such as the choice of role between BVA and PBA, and the choice of storage strategy which will be described in the following paragraphs.

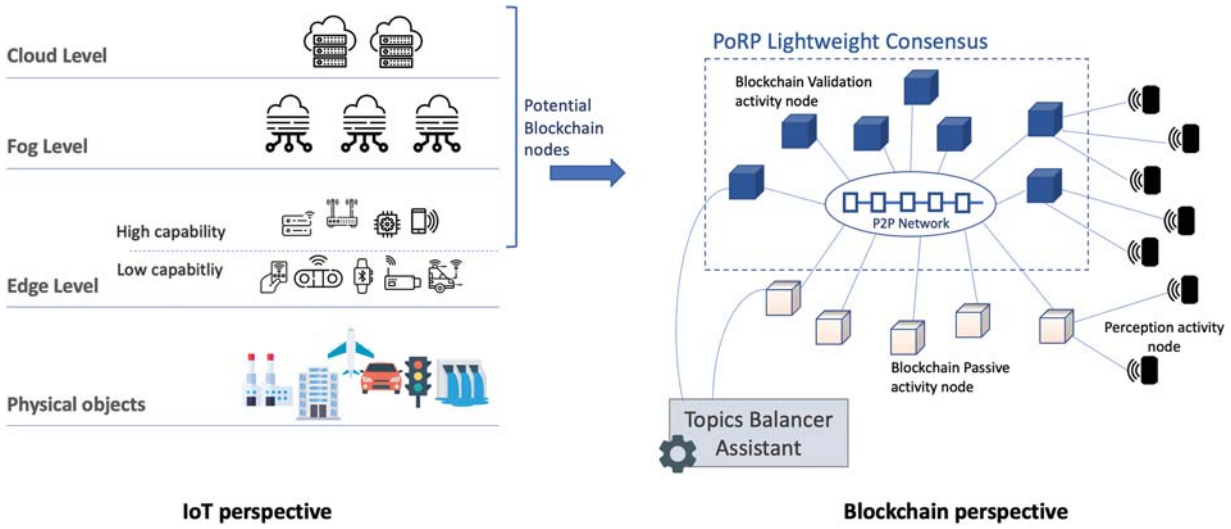

Figure 1: The proposed model architecture

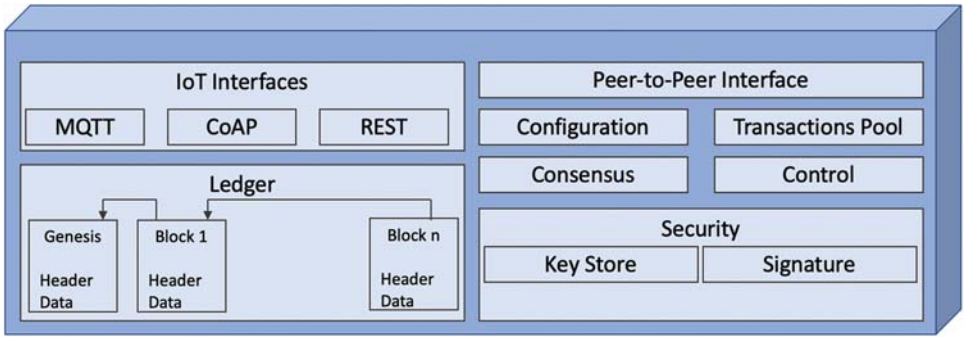

Figure 2: Components of the Blockchain node

The proposed framework ensures its objectives through the following processes:

- Blockchain nodes apply a lightweight consensus called Proof of Random Participation (PoRP)
- The storage of data in the local lightweight ledger, which follows the optimization strategy called Assisted Selection Relevant Data in Local Ledger (ASRDLL).

3.2 Lightweight Consensus

Conventional PoW consensus operates by launching the challenge computation effort by all the Blockchain nodes, followed by the new block creation from the node that first completes the challenge. The cost of validating the new block is accompanied by a waste of energy and time and limits the consensus participation only to machines with very high computational capacity. As an alternative, we propose a new consensus that involves a larger set of machines with a lower computational capacity to validate the new blocks. This participation is performed randomly via an election step of the next validator. The algorithm of this election is not predictable, and all the blockchain nodes participate decisively. The block structure has been modified to add the information of the future validator, as illustrated in Fig. 3.

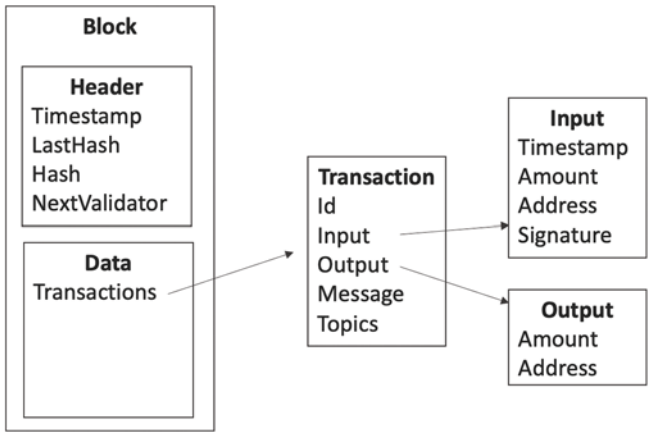

Figure 3: Main elements of the block structure

In a Blockchain network (NBC) composed of n nodes (N1, N2, N3, …, Nn) whose role is VBA, and which contains a Ledger composed of m Blocks (B1, B2, B3, …, Bm), with n and m are greater than 1, the validation of the Block Bm+ 1 according to the PoRP consensus is explained by the following steps, and by the pseudo-code. 1:

Step 0 (triggering validation): The new block creation is triggered by reaching the maximum block size (Block_size_max) or the maximum block time (Block_time_max). These data are defined in the Configuration module and recorded in the Genesis Block.

Step 1 (Mystery Number Generation): The validator node of Block Bm called Master Node, proceeds to generate a random number (M) and shares its Hash (F(M)) with the rest of the NBC nodes. The SHA256 algorithm is used for the generation of F(M).

Step 2 (Participation in the next validator node selection): each of the NBC nodes (called Participating Node) other than the Master Node proceeds to the selection of a random number and shares it with all the NBC nodes. We mark the set of these broadcasted random numbers as (R1, R2, R3, …, Rn-1). After that, the Master Node calculates the index of the elected node (I) by the formula known by all the nodes of NBC: $\mathrm{I} = \left(M + \sum_{k=1}^{n-1} R_k\right) mod(n) + 1$.

Step 3 (Sharing and proving): The Master node shares with the rest of the NBC nodes the index I, the number n, and the number M. At this step the rest of the nodes can recalculate the

index I and verify it with the index received by the Master node. At the end of step 3, each node broadcasts its verification verdict throughout the NBC network.

Pseudo-code 1: PoRP Consensus steps

Master Node
1. M := Random number from 1 to n
2. Share SHA256(M) with all Nodes

Node Participant i
3. Ri := Random number from 1 to n
4. Share Ri with all Nodes

Master Node
5. I := 1 + (M + Sum(Ri)) modulo (n)
6. Share (I, M, n) with all Nodes

Node Participant i
7. Ii := 1 + (M + Sum(Ri)) modulo (n)
8. If Ii ! = I Verdict = KO
9. Else Verdict = OK
10. Share Verdict with all nodes
11. If all Verdict are OK, all nodes accept to pass to the next block iteration

Master Node
12. Complete Current Block Content
13. Share Current Block content with all Nodes

Node Participant
14. Verify Block content
15. Add Block to the local ledger

Step 4 (Move to the Next Validator Node): If all the verdicts received by the Master Node are OK, it adds the information of the Chosen One's index in the Bm +1 Block header, calculates the last Block Hash, and broadcasts the Block in the network. When the new Block is received, each node verifies its conformity, particularly the Validator and next Validator information of the Block. If one of the verdicts is not equal to OK, the Master node repeats the election process (Fig. 4).

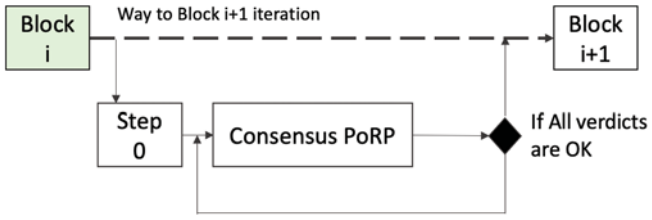

Figure 4: PoRP consensus iteration validation logic

3.3 Lightweight Ledger

The data storage model in conventional Blockchain is based on replicating all transaction history across all nodes, which gives it the character of robustness against tampering. This way

is advantageous in an asset transfer context such as crypto-currency, but in the IoT framework where the use cases are not limited only to monetization but also to other contexts such as data collection, sharing, and processing, a storage optimization strategy is needed. The approach proposed in the IoT-SmartChain framework aims to reduce data storage in the node's local ledger and also throughout the network. This strategy offers two possible levels of optimization.

The first level is a behavioral solution that lets the node choose whether to store the ledger locally or not, using the Design and Architecture section's role model.

The second level is a solution based on the subscription to TOPICS (Ti), which lets the nodes choose to store only the data they are interested in. In this way, the data is no longer present in the network in a redundant way proportional to the number of nodes but reproduced at the limit of the usage expressed through the TOPICS. To avoid the worst-case scenario where all nodes subscribe to all TOPICS, which will result in total data redundancy, and under the motivation of optimizing the overall storage size in the whole network, the IoT-SmartChain Framework introduces the Topics Balancer Assistant (TBA), a brick whose mission is to assist nodes in the choice of storage TOPICS, intending to ensure a Reduction Level (RL) of the global storage size in the network concerning a chosen Optimization Objective (OO) and to ensure a minimum of data redundancy in the network.

Data of interest selection

A new piece of information is added to the transaction structure, called TOPICS, and contains the list of topics defining the context of the transaction creation written in the ledger. A node can then save its interesting context in the configuration module, i.e., the topics to which it wishes to subscribe. When the validator receives a new block containing a set of validated transactions (TRX1, TRX2, TRX3, …, TRXn), each node cleans up the data in this block before adding it to its local chain. According to its configuration topics, the node keeps the complete content of the corresponding transactions and replaces the other transactions' content with "Filtred data" and keeping only their transaction ids. The transaction id allows the transaction content to be retrieved from other nodes if needed. The logic of the relevant data selection is structured by the pseudo-code 2.

Pseudo-code 2: Data of interest selection

```
In the Perception Activity Node
Send data to Blockchain (data, Topics)
In the Blockchain Validation Activity Node
Until Block_Size_Max or Block_Time_Max do
    Creat and Sign Transaction from IoT Data
    Share Transaction with other nodes
Create new Block with Transactions data
Share the new Block
Blockchain Validation & Passive Activity Node
For each Transaction in the new received Block
    For each TOPIC in localConfig
      If LocalConfig.TOPIC ! = TRX.TOPIC
          Transaction.content := Filtred data
```

Topics selection assistance

Two main objectives are to be ensured by the TBA. The first one is to keep a minimum of redundancy of the transactions of a given Topic in the network, to maintain the data history availability. The TBA will consider the total number of nodes in the blockchain network (Nb), the number of existing Topics (Nt), and the number of Topics already subscribed by the nodes (NTs). Other parameters can be considered such as the relevance of the topic (TW) or the volume of transactions of a topic compared to all the transactions of the network (TR). The second objective is to ensure that the total storage size of the network remains below the optimization target threshold defined at the beginning. The TBA is consulted each time a node wants to initialize or modify its topic subscription configuration, to get the optimization index (IO) which must be lower than the network optimization objective (OO). The concept of this processing is illustrated by the sequence diagram in Fig. 5.

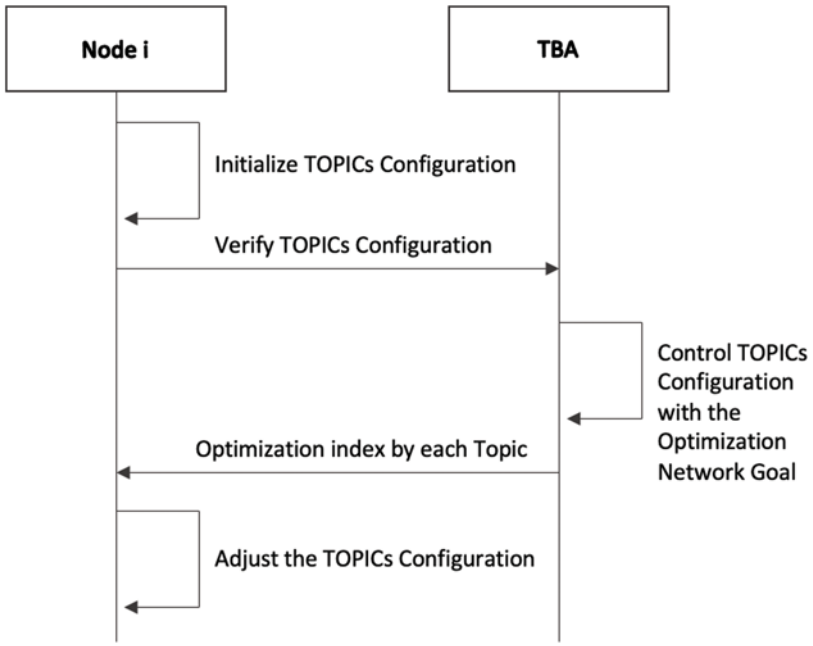

Figure 5: Processing concept of selection assistance to TOPICS

In this way, the IoT-SmartChain framework mainly differs from the conventional Blockchain model in the points listed in Tab. 3.

Table 3: Differences between conventional Blockchain and IoT-SmartChain

Property	Conventionnal Blockchain	IoT-SmartChain
Consensus algorithm	PoW	PoRP
Block creation speed	Takes from minutes to hours	Takes a few seconds
Mining time	Slow	Fast
Block validation	Hash verification	Hash verification
Chain size	Redundant	Optimized

4 Performance and Analysis

4.1 Use Case

The proposed IoT-SmartChain framework has been applied in a case example related to the smart city context. The simulation goal is to federate all smart city components in an IoT system accelerated by a Blockchain layer that brings orchestration, security, and trust. This integration should eventually create new business opportunities between stakeholders. The imagined smart city is composed of ten main entities including University (E1), Transit Company (E2), Railway Station (E3), Public Administration (E4), Sports Center (E5), Fuel Station (E6), Surveillance and Security Company (E7), Manufacturing Plant (E8), Residential Housing Cluster (E9), and Hospital Center (E10). Each entity has a set of IoT sensors (Oi), a node participating in the Blockchain with the VBA role (NODi), and its own information system (the entities' IS is not covered or instantiated in this simulation). The number of IoT sensors is 49, and they are of two different categories. The first category gathers objects that only serve as state change sensors such as speed (O1), affluence (O2), temperature (O3), liquid level (O4), gas level (O5), weight (O6), and humidity (O7). The second category includes objects with both a sensor capability and a processing capability, such as local video processing (O8), human voice interaction (O9), and scheduling actions of several other connected objects (O10). The objects in this category are considered nodes of Edge Computing. Tab. 4 represents the overall matrix of IoT entities and objects. The roles of the network components in the IoT-SmartChain framework are chosen based on their computational and storage capabilities. Nodes with the VBA role are present at the Fog Computing level, nodes with the PBA role are present at the second category, and nodes with the PA role are present at the first category.

Table 4: Entities and IoT objects of the simulation

Entities	IoT Objects										
	Sensors							Edge			Fog
	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	NODi
E1		X		X						X	X
E2	X	X		X	X				X		X
E3	X	X		X						X	X
E4		X		X							X
E5		X	X	X			X			X	X
E6		X		X	X			X		X	X
E7				X				X		X	X
E8	X		X	X	X	X	X	X	X	X	X
E9				X							X
E10		X	X	X		X	X	X		X	X

4.2 Simulation Environment

The simulation was run in two scenarios. The first scenario aims at evaluating the CPU/RAM utilization, the evolution of local storage, and the energy consumption over time. In this experiment, the smart city starts with all nodes and will be running for 3 hours. The sensors have been

simulated with Shell scripts that send random messages to the Blockchain at a frequency of 3 messages per minute. The second scenario aims at evaluating the global storage evolution of the network along with the evolution of the number of nodes. Different from the first experiment, this scenario starts with two entities and then activates two new entities every 3 hours until the ten entities of the simulation are completed. The Fog Computing nodes and the TBA were instantiated on t2. micro machines from AWS with the configuration of 1 GB of RAM and 1 CPU. The Edge Computing nodes were instantiated on t2. nano machines of the AWS service with the configuration of 0.5 GB of RAM and 1 CPU. The Blockchain was configured to validate the Block every 2 minutes. We set the network storage optimization objective (OO) to 70%, where 100% corresponds to zero optimization. The IoT-SmartChain framework was developed from scratch with the NodeJS framework, based on the Bitcoin Blockchain model, and using NPM modules including mainly 'crypto-js' for the SHA256 algorithm, 'elliptic' for the secp256k1 algorithm, 'coap' for the CoAP interface, and 'mqtt' for the MQTT interface, 'ws' for the Peer-to-Peer interface, and 'systeminformation' for recording certain evaluation metrics such as CPU and RAM usage.

4.3 Analysis and Comparison

CPU utilization, storage cost, and energy consumption were evaluated to serve as an analysis of the proposed work. The observed results are compared with the existing models ELIB [24] and BFAN [25]. Tab. 5 shows the main differences between the present work and the existing work.

Table 5: Comparison between IoT-SmartChain, ELIB and BFAN

Axis	IoT-SmartChain	BFAN	ELIB
Objective	Modeling and development of lightweight Blockchain solution for IoT in the smart city	Development of IoT environment security through Blockchain	Design of a lightweight blockchain for the smart home
Network levels	Blockchain, Fog, Edge, IoT	Blockchain, Fog, IoT	Blockchain, IoT
Consensus algorithm	Lightweight PoRP	PoW	Lightweight consensus by DTM
Redundancy	Optimized by ASRDLL	Not optimized	Not optimized
Outlines	- Improves scalability - Minimizes power consumption - Improves storage capacity - Minimizes consensus complexity	- The complexity is high - Energy consumption is high - Not scalable - Storage requirement is not optimized	- Increases energy consumption - Storage requirement is not optimized - Minimizes complexity of consensus

4.3.1 Ressource Consumption Analysis

The measured resource consumption is the power and CPU consumption by the network components that participate in the Blockchain Consensus. To facilitate the measurement of energy

consumption, a unit weight W is mapped to the approximate value of Watts consumed for a type of processing function, such as arithmetic, hashing, encryption, or network broadcast operations. The unit weight W increases proportionally with the power consumption.

In Fig. 6, we present the CPU consumption requirement for both the IoT-SmartChain and BFAN models during the simulation period. We see that the IoT-SmartChain model significantly improves the CPU requirement for nodes that wish to participate in the Blockchain Validation Consensus, measured at an average of 0.7% compared to an average of 300% for the BFAN model. This decrease in CPU usage is explained by the low complexity of the Consensus algorithm, which is considered a motivating factor to expand the scope of the network machines in terms of hardware requirements to integrate the Blockchain application. This improvement has led to energy efficiency, proven and presented in Fig. 7. Throughout the simulation, the energy consumption remained low is stable, with no impact from the number of validated Blocks. We analyzed the energy consumption with respect to the number of transactions. It can be seen that the number of transactions has no impact on the proposed work, so that the energy consumption remains reasonably between 110 W and 120 W, while the energy consumption increases with the ELIB and BFAN models, which by operating concept, the computational power is increased throughout the Blockchain network with the increase in the number of nodes to ensure the security of maintaining the network. Their consumption reaches 930 W for a number of 60 blocks, so we can deduce that in the present simulation, the energy consumption has been reduced by a ratio close to 9/10.

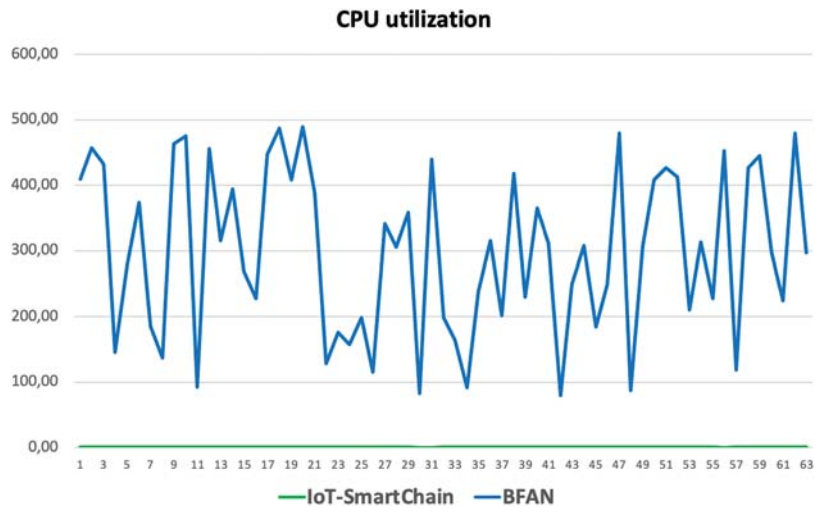

Figure 6: CPU utilization (IoT-SmartChain, BFAN)

4.3.2 Storage Capacity Analysis

The storage cost is defined by the amount of data generated for storage in the blockchain ledger. In our work, we analyze two levels of storage. The first one is the local storage of a Blockchain node, and the second one is the storage of all the Blockchain nodes. For the first level, we compare the size evolution of the local ledger throughout the simulation. For the second level, we compare the storage size evolution in the whole network, with a check at each step of node

number increase during the simulation. The comparison is made against the ELIB and BFAN models.

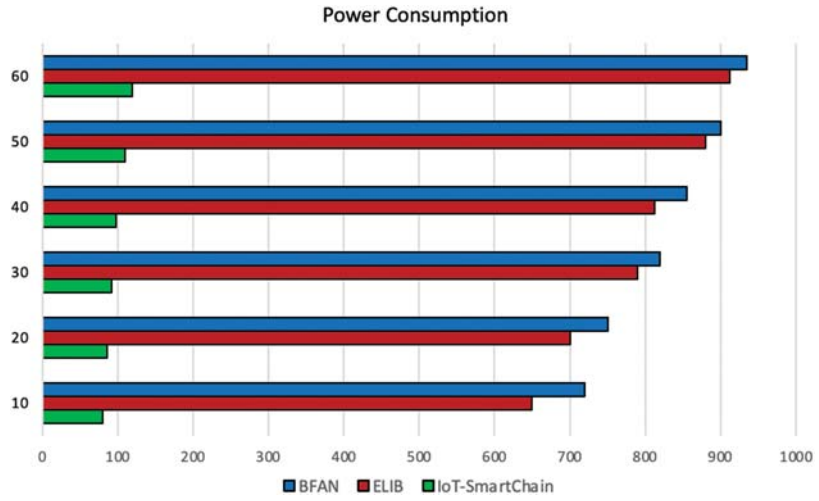

Figure 7: Energy consumption (IoT-SmartChain, BFAN)

In Fig. 8, storage is analyzed in relation to the number of blocks containing transactions in the life of the Blockchain. When the number of Blocks increases, the size of the local ledger of a node increases. With the model of the proposed work, the size of the local ledger reaches 25 MB when the number of Blocks is 60, while for this same number, the size of the local ledger reaches 60 MB with the ELIB model. For the same number of Blocks, the storage cost is 240% higher than that of the proposed work model.

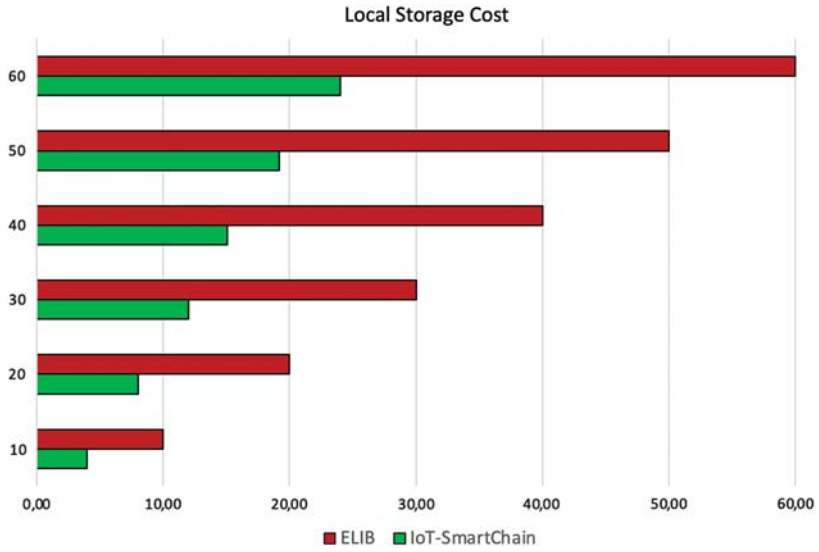

Figure 8: Evolution of the local ledger storage (IoT-SmartChain, ELIB)

In Fig. 9, storage is analyzed with respect to the evolution of the number of nodes in the Blockchain. The analysis shows that the storage size in the whole Blockchain network increases when the number of nodes increases. With the existing models, the storage cost reaches 120 MB when the number of nodes is equal to 10. While with the proposed model, the storage cost under the same conditions is 65 MB, respecting the network optimization objective (OO), which is 70%. With BFAN and ELIB models, data is replicated throughout the network and also in the cloud without redundancy optimization, which poses a problem of high storage cost. However, the proposed model optimizes the storage across the network, verifying the data redundancy to ensure the optimization objective defined by the Blockchain.

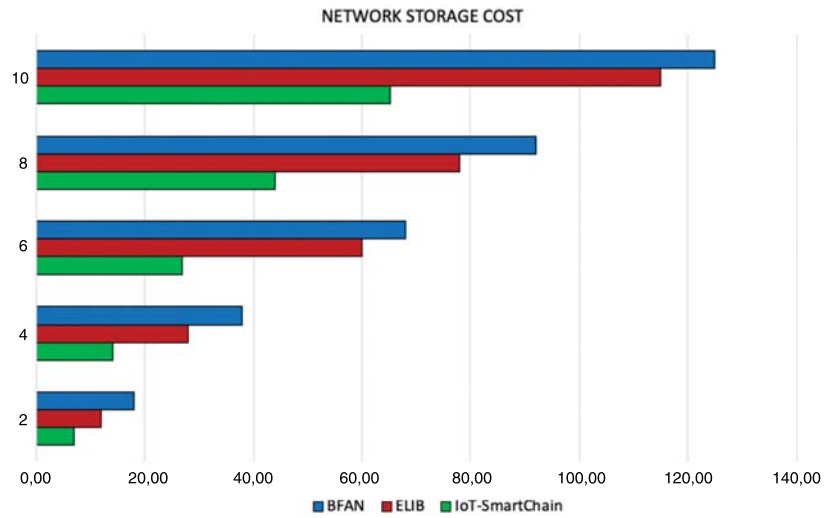

Figure 9: Storage evolution in the whole network (IoT-SmartChain, BFAN)

4.3.3 Discussion and Result

The average of the results obtained in our experiment for our model and existing works is summarized in Tab. 6.

The analysis shows that the model of the proposed work achieves better performance for the evaluated metrics, and it is well suited for the IoT environment at smart city scale. The main aspects of the present work are:

- Energy consumption and CPU usage are reduced by implementing lightweight Blockchain consensus, Proof of Random Participation (PoRP), based on the secure participation of all nodes in the validator node election, and thus eliminating the large computational effort and complexity of conventional PoW consensus.
- Storage capacity is optimized at the node's local ledger level by TOPICS subscription and at the network-wide level by TOPIC selection assistance that controls the level of data redundancy to not exceed the defined storage optimization target.
- The requirements for computing.

Table 6: Numerical result of the proposed model and existing work

Metrics		IoT-SmartChain	BFAN	ELIB
Required CPU (%)		0.7	312	283
Energy consumption (W)		119	935	912
Storage (MB)	Number of blocks	24	61	58
	Number of nodes	65	125	115

5 Conclusion

A In this paper, we proposed a novel lightweight Blockchain framework called IoT-SmartChain for the IoT environment and its resource-constrained objects at the Smart city scale. The proposed model achieves a high level of CPU usage and energy consumption optimization by its lightweight consensus and brings the possibility of data storage cost optimization across the network by TOPICS subscription strategy and data redundancy level checking. The proposed model has been modeled, implemented, evaluated, and verified in a smart city use case. In the future, we plan to improve the TOPICS selection strategy by adopting a machine learning mechanism that can improve these decisions over the life of the smart city and share its knowledge with other smart cities of the same size.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Sánchez-Corcuera, A. Nuñez-Marcos, J. Sesma-Solance, A. Bilbao-Jayo, R. Mulero *et al.,* "Smart cities survey: Technologies, application domains and challenges for the cities of the future," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, pp. 155014771985398, 2019.

[2] E. Park, A. del Pobil and S. Kwon, "The role of Internet of things (IoT) in smart cities: Technology roadmap-oriented approaches,," *Sustainability*, vol. 10, no. 5, pp. 1388, 2018.

[3] P. P. Ray, "A survey on Internet of things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.

[4] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo *et al.,* "A survey of IoT applications in blockchain systems," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–32, 2020.

[5] D. Wörner and T. von Bomhard, "When your sensor earns money," in *Proc. the UbiComp 14 ACM Conf. on Ubiquitous Computing*, Seattle, WA, USA, pp. 295–298, 2014.

[6] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. on Intelligent Transportation Systems*, Rio de Janeiro, Brazil, pp. 2663–2668, 2016.

[7] A. Arora and S. K. Yadav, "Block chain based security mechanism for Internet of vehicles (IoV)," in *Proc. 3rd Int. Conf. Internet of Things and Connected Technologies*, Jaipur, India, pp. 26–27, 2018.

[8] T. Su, S. Shao, S. Guo and M. Lei, "Blockchain-based Internet of vehicles privacy protection system," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–10, 2020.

[9] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. on Pervasive Computing and Communications Workshops*, Kona, HI, USA, pp. 618–623, 2017.

[10] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. on e-Health Networking, Applications and Services*, Munich, Germany, pp. 1–3, 2016.

[11] M. S. Munir, I. S. Bajwa and S. M. Cheema, "An intelligent and secure smart watering system using fuzzy logic and blockchain," *Computers & Electrical Engineering*, vol. 77, no. 8, pp. 109–119, 2019.

[12] Y. Wang, J. Li, W. Liu and A. Tan, "Efficient concurrent execution of smart contracts in blockchain sharding," *Security and Communication Networks*, vol. 2021, pp. 1–15, 2021.

[13] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *Proc. 14th Int. Conf. on Service Systems and Service Management*, Dalian, China, pp. 1–6, 2017.

[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Paper*, 2008. [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper.

[15] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. 12th Int. Conf. on Open Source Systems and Technologies*, Lahore, Pakistan, pp. 54–63, 2018.

[16] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT," *Challenges and Opportunities, Future Generation Computer Systems*, vol. 88, no. 3, pp. 173–190, 2018.

[17] T. Kim, J. Noh and S. Cho, "SCC: Storage compression consensus for blockchain in lightweight IoT network," in *Proc. IEEE Int. Conf. on Consumer Electronics*, Las Vegas, NV, USA, pp. 1–4, 2019.

[18] S. Popov, "The Tangle," 2018. [Online]. Available: https://iota.org.

[19] M. U. Zaman, T. Shen and M. Min, "Proof of sincerity: A new lightweight consensus approach for mobile blockchains," in *Proc. 16th IEEE Annual Consumer Communications & Networking Conf.*, Las Vegas, NV, USA, pp. 1–4, 2019.

[20] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty *et al.,* "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343–2355, 2020.

[21] A. Adel, "Utilizing technologies of fog computing in educational IoT systems: Privacy, security, and agility perspective," *Journal Big Data*, vol. 7, no. 1, pp. 194, 2020.

[22] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq *et al.,* "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.

[23] Y. Liu, K. Wang, Y. Lin and W. Xu, "A lightweight blockchain system for industrial Internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[24] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar *et al.,* "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

[25] P. Singh, A. Nayyar, A. Kaur and U. Ghosh, "Blockchain and fog based architecture for Internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, pp. 61, 2020.

[26] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, no. 3, pp. 180–197, 2019.