Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Design and Implementation of Collaborative Framework of Blockchain and Cloud of Things

Ranu Pandey,

Ph.D Research scholar, Shri Rawatpurasarkar university Raipur C. G.

Dr. Rajesh kumar Pathak,

Professor Shri Rawatpurasarkar university.

Article Info

Page Number: 3709 - 3720

Publication Issue:

Vol 71 No. 4 (2022)

Article History

Article Received*: 25 March 2022*

Revised*: 30 April 2022*

Accepted*: 15 June 2022*

Publication*: 19 August 2022*

Abstract

The Internet of Things (IoT) has progressed from its infancy to full maturity alongside the equally rapid advancement of communication technologies; IoT tends to develop in an explosively rapid manner, with ever-increasing amounts of data being transmitted and processed. So, the capacity to oversee gadgets is essential has been subjected to more stringent and sophisticated requirements for actual use as it is being rolled out on a performance. Existing IoT platforms, in which most devices are managed by a central hub, have several drawbacks. cyber-attack, single point of failure, and other technical restrictions. Different approaches a clear path forward is crucial for expanding data accessibility, while government mandates for confidentiality and safety. In this paper, we propose a blockchain-based, all-inclusive Internet of Things platform technology to ensure the reliability of sensing data. This service aspires to provide the device owner with a functional program that keeps track of all of their transactions in an immutable log and gives them quick access to the data apparatuses sent out into the world in a variety of roles. It also provides traits shared by all Internet of Things systems, enables, so that the user and the gadget can keep tabs on each other in real time. Strategic thinking behind the smart contract specifies the parameters of the application.

Keywords: Blockchain, Design, Cloud of things, Cyber attack

I. Introduction

There are six steps involved in conducting a systematic review, including formulating the research question, selecting the appropriate research methods, screening the relevant articles, analysing the abstract and keywords, retrieving the relevant data, and processing the maps. The appropriate articles are analysed by keywords using the Atlas.ti software. There are a total of 70 codes applied to a corpus of 262 quotations that have been manually coded to establish categories. In the end, 20 options were retrieved, primarily falling into two broad categories: decentralization and security. Only three of these ten solutions were concerned with safety, while the remaining seven were distributed.

Opportunities in home automation, smart transportation, and industrial production are just a few areas where the Internet of Things can be used [1]. Large-scale autonomous IoT systems are made possible by the convergence of embedded computing hardware and network technology, both of

which have advanced in recent years [2]. In general, the Internet of Things is made up of disparate gadgets that generate and transmit copious amounts of private and potentially dangerous data. In light of this, the importance of the network is growing.

Working in unattended environments makes wireless sensor networks especially susceptible to cyberattacks [3]. Present-day Internet of Things solutions typically utilize a centralized architecture reliant on interfacing with cloud servers over the web. As IoT systems become more complex, Despite its impressive elastic compute and data management capabilities, this system has a number of security flaws. The broad adoption of Internet of Things (IoT)-based infrastructure, for instance, may introduce a single point of failure which may put at risk the data center's availability. Due to the sheer volume of IoT devices, a secure and reliable infrastructure is required[4].

1. Blockchains and Decentralized Services

S. Nakamoto [5] formally theorized blockchain technology, and the Bitcoin cryptocurrency is the first practical application of this technology. Unlike fiat currency, digital currency can be spent twice by the same stakeholder, so safeguards are an essential part of cryptocurrency networks. Without relying on trusted third parties, double spending can be prevented by using blockchain technology. Transaction records in a blockchain are held by each individual node in the network. These transactions are recorded in blocks, and each block in the chain is connected to the next via its hash.

Distributed ledger technology (DLT) uses consensus algorithms to ensure that all nodes in a network are in sync with one another. Nodes in a blockchain network

2. Conceived layout for conducting experiments

From the vantage point of the vehicle communication system's infrastructure, Blockchain was first introduced by Yuan and Wang3 as a decentralised network architecture for implementing a ride-sharing system on the blockchain-based It, which provides a seven-layer hierarchy structure. Singh and Kim presented a blockchain-based incentive system to establish Trust Bit as a ledger recording of trustworthiness of vehicle behaviour, enabling for a safe and reliable friend vehicular information transmission cloud, from the perspective of application-oriented vehicular communication. Implementing modular components of mentoring vehicle-based communication is an important step in realising the topological extensibility of such a decentralised system.

II. Related Work

Production facilities have been early adopters of IoT technology for Talking to machines. While modern technology has made the concept of the Internet of Things possible, there are still several roadblocks preventing its widespread adoption in the actual world. The blockchain has garnered considerable attention from academics and corporations in recent years because to the trustworthiness and openness it provides. The blockchain does have the ability to support the decentralised, time-stamped data network at the heart of Industry 4.0. [6]. In this study, we explore the potential of blockchain technology for overseeing IoT gadgets. We have not been able to find many academic studies that investigate this question because blockchain has been very well in the financial services industry. This article reviews the current state of knowledge concerning blockchain technology's application to the IoT.

There are 18 different uses for blockchains [7], four of which are unique to the Internet of Things: trading in create a data, trading in IoT gear, or authenticating IoT devices require an immutable log

of occurrences and access to data management. In this article, we discuss the possibilities of combining blockchain and the IoT, along with its advantages, disadvantages, and future developments (IoT). Especially in terms of resolving issues with data integrity and security, the blockchain may prove to be a revolutionary tool for the IoT. They explain in greater detail why it is preferable to move away from a centralised IoT system and toward a decentralised one. It is proposed should LoRaWAN network servers use a blockchain technology in order to build something honest and decentralised and secure against interference. There is no space for dispute on the accuracy of the data associated with a transaction at a given period in the system.

The authors claim that this is the first practical implementation of blockchain technology integrated with LoRaWAN Internet of Things technology. Using LoRa nodes as a proof of concept [9] for facilitating access to Ethereum's blockchain-based infrastructure from The concept of low-power, resource-constrained Iot edge is offered. To this aim, the authors suggest an event-based messaging system for low-power IoT end devices and employ an IoT gateway as just a blockchain node so make it all happen. The authors introduce the concept of smart contracts and explain how they might be used to support the proposed autonomous sharing of resources among IoTdevices[10]. The ways in which the Internet of Things (IoT) can benefit from blockchain networks are outlined, with a focus on commerce, billing, shipping, and inventory management. The authors of this work present a system of traceability for monitoring the flow of agricultural products in China. The proposed system combines RFID and blockchain technology to improve food quality and safety while cutting down on transportation costs. The proposed IoT device management system allows for remote management and setup of IoT gadgets.

III. Blockchain Platform for the Internet of Things

1. IoTBlockchain Platform Hypothetical Scenario

The Internet of Things (IoT) server is a third-party service provider that interacts with users and other nodes in the blockchain network using local bridges. Some examples of such tasks are data collection from the bridge's sensors, actuator command transmission, data querying, data storage in the blockchain's distributed ledger, etc. Physical device profiles, sensor data, and owner information can all be kept in the immutable ledger of the blockchain network. Both physical media like hard drives and virtual ones like databases are used to store information. Clients are the endpoints through which users interact with the blockchain, and they can be anything from mobile phones and laptops to personal computers. Users at home can, for instance, check the blockchain for information about the condition of their various home appliances at a given time. Developers of Internet of Things products and systems can pick from a variety of available communication protocols, including Connectivity options include 2G/3G/4G cellular, Wi-Fi, Bluetooth, and ZigBee. By utilising one or more of these protocols, local bridges act as the service agent for a collection of IoT devices and link them to the server. Raspberry Pi and other embedded devices can now directly consume web services by calling RESTful application programming interfaces, thanks to advancements in hardware technology (REST APIs). Two techniques of information transfer to real-world hardware: local bridges and direct wireless connections. In contrast to other ongoing initiatives, which center on building bridges to link IoT gadgets to the blockchain, the proposed work places more emphasis on straightforward communication. There are two main types of Internet of Things devices, sensors and actuators. In response to user input, actuators perform the

specified action (e.g., turn just on light), while sensors gather environmental data (e.g., temperature) and transmit it to servers for analysis.

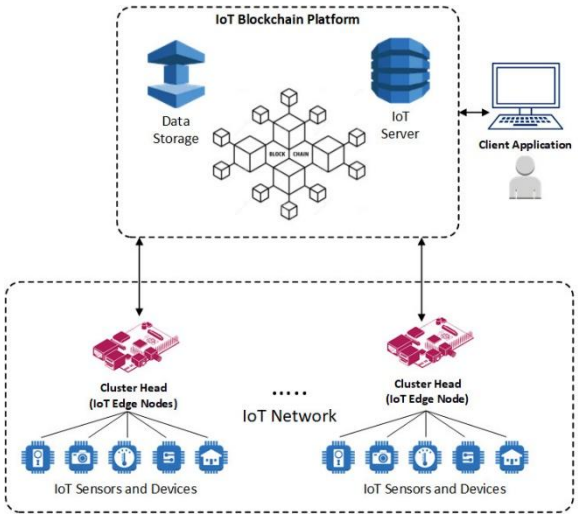


Figure 1. System Architecture for a Blockchain-Based Internet of Things

Modular architecture allows developers to swap out or add new components independently of the whole without breaking anything else. A wide variety of interconnected devices that can send and receive data, perform computations, and store information make up the IoT's physical layer. Due to the lack of built-in global Internet protocols in most physical devices, the connectivity layer's primary service is routing management (IPs). At this level, you'll find service modules like a messaging broker, network administration, and security administration. The Identity-as-a-Service (IDaaS), Consensus, or Peer-to-Peer (P2P) Communication (blockchain) modules are housed in the IoTblockchain - based layer. Participants in a blockchain can each keep a copy of a distributed ledger, and these versions will be identical to one another. It also provides safe space for storing information about the device's settings and the readings from any attached sensors. In a matter of minutes, or even seconds, all copies of the ledger will reflect the latest changes. Permissionless ledgers allow anyone to run a peer to validate transactions, while permissioned ones limit validation to a select group of users.[11] The blockchain can serve as an effective medium for online data storage thanks to the inclusion of a big data analytics module. Ledgers are a great resource for analysts because they compile and organize a large amount of transactional data from multiple sources. Assigning them all access to a single network makes sharing and retrieving this information much simpler. A client application on the outside of the ledger invokes the smart contract, which is a kind of code that controls who can access the ledger and how. Typically, each node in a network will have it installed and instantiated on their own machine.

2. Technologies like blockchain and distributed ledgers

Distributed ledger technology (DLT) distributed database runs on a network of computers rather than just one.Distributed ledger technologies (DLTs) log transactions involving numerous parties and their respective asset transfers. By making databases inherently unhackable, they reduce the price of conducting trustworthy transactions.

Data transactions are hierarchically stored in DLT systems.

Accounts record changes at the transaction level [12]. Every action modifies the accounts' state, so this model of accounts is analogous to a state machine that operates on transaction data.

By using cryptographic hashes and asymmetric encryption, we can ensure that the transactions cannot be altered in any way. Subsets of transactions are grouped together into larger units called blocks. A block contains three things: (1) a make a link to the preceding section, (2)a list of operations to commit, (3) a tamper-evident digest of a transaction history attesting the integrity and ordering of the blocks [13]. Different ledgers are born from the cryptography block-linkage that is ultimately selected. Blockchains are discussed in the context of linear dependencies.

The consensus protocol used implementation of deterministic scripts (the smart contracts) to propose a set of services to users, and the ability to add new blocks to the chain (e.g., launch a transaction under a set of conditions), are the foundations of the blockchain system's trusted behavior [14]. The consensus protocol, on the one hand, details the method used to reach an agreement on a common reality. Using this protocol, your database will expand safely and reliably. Increases the DLT's resistance to node failures, thanks to the fact that a predetermined protocol guarantees that no undesirable outcomes will arise. It handles all transaction requests, keeps correct committed blocks from being rolled back, and allows for node failure recovery [15]. To contrast, distributed ledger technology's (DLT) scripting capabilities enable autonomous contracts tied to stored assets [16]. Transactions submitted for validation can make use of the SC they were computed with for security purposes. If the miner's copy of the SC produces the same output as the original transaction, then the miner has successfully validated both transactions. There is room for development on top of SC capabilities for applications and services.

IV. Cloud of Things

The main topics of this work, "Cloud of Things" or "CoT." Indeed, the framework and infrastructure mentioned above are intended to aid in the formation of a CoT. This is because things with RFID tags or smart (or not-so-smart) sensors and actuators are typically mobile, and a stack like this would be prepared to provide all of the technologies required to address this issue. It is worth noting that such an architecture would be extremely useful even in the absence of a CoT level. The CoT level, on the other hand, can be viewed as a killer application for this type of infrastructure, leading to a more context-rich IoT scenario, releasing degrees of freedom for discovery and allocation, and eventually leading to a marketplace of things.

The provided tools and mechanisms must be able to search for anything that meets certain criteria (vehicles within specific areas, devices with specific monitoring features, people or things whose placement or movement follows a predefined pattern, etc.) based on the application domain per request specification; preprocess and filter data to trigger tailored algorithms and offer new value-added services (traffic management, goods tracking, emergency management, on-line monitoring). Because things require names, ontologies and the taxonomies they represent are required.

V. Cyber-physical systems

The term "Internet of Things" is commonly used to describe the proliferation of internet-enabled devices in everyday life. The environment is filled with sensors, tags, and actuators that can detect, monitor, and act upon objects [17]. Cyber-physical systems [18] are systems that combine the real world with virtual communication networks. IoT networks can be fine-tuned by modifying a predefined set of service characteristics to improve business implementing innovation and

compliance testing. More pervasive manufacturing systems can be achieved through the integration of numerous technological building blocks, such as service-oriented architectures, cloud-based infrastructures, business process management systems, and compliance monitoring [19].

Database	Initial Queries	Filtered Queries
ScienceDirect	316	4
ACM Digital library	54	6
IEEE	25	4
SpringerLink	357	17
AISel	159	6
Total	911	37

Figure 2. Search Query Result

VI. Methodology

Peer-to-peer process monitoring with blockchain and the Internet of Things is the subject of a survey [20]. For the most comprehensive catalog of BPMS platforms that make use of blockchain technology, use-case demonstrations, we employ a personalized search string to databases most relevant to business process management [20]

We generated a set of interchangeable keys by brainstorming possible replacements for each one expression (specifically BPM, BC, and IoT), and combined them into a single boolean query. The Results Lookup Business Process Management OR (string) OR "In this context, "business process" and "IoT" both refer to the internet of things Cyber-Physical Systems" OR "Things" "AND Intelligent) AND In other words, (Blockchain OR "Distributed Ledger").

We look in the most important databases for info on the subject of BPM using the given query. Duplicates are weeded out by us using the following criteria for inclusion: (1) is it review by experts in the field? In (2), we find an empirical investigation performed? In the third and final question, does the text discuss both blockchain technology and BPM? After that, we went back and forth, in a recursive fashion, on the related tasks incorporated works cited references into these papers. Outlined in Table 1, the total number of papers retrieved from each source and then some sort of filtering was done based on the inclusion criteria. A total of ten is ours. papers, after discarding carbon copies. A look into the past result in the recovery of five additional documents. As a result of taking out paper copies, the group that gets saved for further study includes fifteen total papers In Table 2 below, you'll find a articles published in conferences or journals that have been subjected to a rigorous peer review process.

VII. Design method

We classify blockchain-based BPMS development strategies as either empirical or model-driven.Multiple methods provide empirical support for blockchains' value in asset management. These methods involve creating SCs from scratch, tailoring their structure and features to meet a specific company requirement. A Hyperledger Fabric chaincode (a SC variant) based on a Business

Process Model and Notation (BPMN) collaboration diagram is used to simulate an asset monitoring process in a luxury supply chain [21].

Wherever RFID chips are used, the network is part of an EPC-based IoT network used for tracking assets. Similarly, a private blockchain based on Quorum is successfully implemented for a food delivery process [22]. However, scalability and privacy issues arise in both scenarios. IOTA is one example of a block-free directed acyclic graph proposed as a solution to these problems [23]. Each new transaction verifies previous transactions, so when blocks are deleted, miners are also deleted. If miners are taken out of the equation, the centralization risk posed by mining pools disappears. There is empirical evidence of peer-to-peer energy trading using this DLT, despite the fact that its architecture slows transactions down [24].

Due to the intricacy of the empirical creation of process SCs, which requires advanced programming abilities, the design phase is time-consuming and resource-intensive.Abstrating SCs into sublayer stacks is a viable solution to this problem. The design process is sped up and improved in quality when the business modelers are not required to understand the specifics of the SC code.

1.Sequencing of activities

When taking an imperative stance, one views business processes as a series of mandated, sequential steps. The business process modeling notation (BPMN) is widely accepted as the de facto standard for illustrating command-driven process models. Two BPMN-based BC monitoring systems are reported in the literature. Business operations at Caterpillar [5] are carried out entirely in the blockchain. An integral part of the framework, the translator, converts business process modeling notation (BPMN) diagrams into a simplified Petri net that can be coded in Ethereum's Solidity SC.

Instances of both processes and parties are created during runtime. In order to maintain credibility, each party generates its own copy of the contract and then compares the two. The process log is stored on IPFS, a decentralised network protocol that offers storage facilities, and API calls are linked to blockchain transactions via a local trigger in real time . The execution costs have also been reduced thanks to data structure optimizations [25]. In a similar vein, Lorikeet is concerned with the transformation of Business Process Modeling Notation (BPMN) choreography processes into Service Chains (SCs). Only the conversation histories of the communicating parties are kept in the blockchain. There is some consideration given to security and privacy approaches, the Caterpillar and the Lorikeet, use methods like participant engagement and asymmetric data exchange, albeit to varied degrees.

In response the limitations of imperative & semi-imperative procedures, declarative procedures were developed.

When a process is modelled, the rules that govern it are specified; in this way, the proper order of operations is indirectly enforced. The ADICO protocol, for example, is grammar-centric in an institutional setting. Institutions, in a broader sense, are symbolic representations of established norms of group behaviour.

These motifs are framed by a set of rules, strategies, and cultural norms. SCs are produced during the translation process as a result of the semi-automatic translation of textual inputs [26]. The method of execution has two parts. To begin, this is a semi-automatic translation, meaning that the developer has some leeway in adjusting the SC that is generated to account for special cases. The next step in the execution of a SC is to compile it into an EVM bytecode.

2. External services

The importance of a blockchain-based BPMS that can communicate with other blockchain services externally cannot be overstated.

Enterprises can take advantage of the potential of multi-BC scenarios with blockchain-agnostic BPMS, which allows them the advantages of various technologies, such as permissioned as well as permissionlessblockchains, to combine.

The use of blockchains is viewed as akin to using an external service. To separate the various blockchains from the BPMS, BlockMe2 [27] implements a blockchain access layer. In order to facilitate communication between the blockchain and the BPMS during execution, a subscription manager and a callback manager are implemented.

A URI scheme is used to activate each ledger and its SCs. To model blockchain functionality, Business Process Modeling Notation (BPMN) diagrams are used. The parameters required using the confidence score and the smart contract to verify the transaction are referred to on Page 4294. In terms of durability, the latter is what you get from a transaction. Errors such as timeouts and failed invocations can also set off parallel processes.

The importance of a blockchain-based BPMS that can communicate with other blockchain services externally cannot be overstated.

Enterprises can take advantage of the potential of multi-BC scenarios with blockchain-agnostic BPMS, which allows them to take advantage of the best features of various technologies all at once, like permissioned as well as permissionless.

The use of blockchains is viewed as akin to using an external service. To separate the various blockchains from the BPMS, BlockMe2]28]implements a blockchain access layer. In order to facilitate communication between the blockchain and the BPMS during execution, a subscription manager and a callback manager are implemented.

A URI scheme is used to activate each ledger and its SCs. To model blockchain functionality, Business Process Modeling Notation (BPMN) diagrams are used. This duty makes mention of the URI scheme's intended SC function, the smart contract's required parameters, and the validation confidence score. In terms of durability, the latter is what you get from a transaction. Errors such as timeouts and failed invocations can also set off parallel processes.

3. Challenges induced by the blockchain technology

The cost of trust may be too high or too low depending on the specifics of the blockchain-based BPMS architecture (proof-of-work, proof-of-stake, and similar mechanisms, in and out monitoring, etc.). On-chain data storage, for example, can be quite costly compared to cloud-based alternatives because many systems employ pay-per-instruction mechanisms. The road to decentralised trust should have manageable upfront and ongoing costs, lock-in effect risks1, privacy concessions, as well as scalability performance. As the amount of transactions and consequent need for monitoring rises in tandem with the incorporation of IoT devices into the creation and execution of the a business process, the importance of the latter grows proportionally. Decision trees are useful for determining how beneficial a blockchain-based BPMS is, whether in an IoT setting or elsewhere.

To facilitate computation with neighbourhood gateways and peer-to-peer (P2P) communication among IoT devices in intelligent swarms, so these are two of the criteria to be checked.

Smart Contract Modeling

The Hyperledger Composer is used to create and execute the smart contract. This is a large collection of open development tools and a framework that make it easier to implement blockchain applications. Participants are part of a business network and have the ability to own assets and submit transactions. They can be device owners with access to and ability over their devices in the proposed case study. Assets can be goods, services, or property in general, and they are kept in registries. These two types are represented by an identifier and can have any additional properties that are required. A device asset that represents an IoT device, for example, is made up of a sensor and an actuator, and it typically contains general information such as the device's ID, name, and owner, as shown in Table 1.

Table 1 Device asset definition in the smart contract.

Category	Component	Type
Sensor	sensor_ID	String
	name	String
	device_owner	String
	unit	String
	event_threshold	Integer
	timestamp	DateTime
	value	String
Actuator	actuator_ID	String
	name	String
	device_owner	String
	state	Boolean

Table 2. Sample transaction definition in the smart contract.

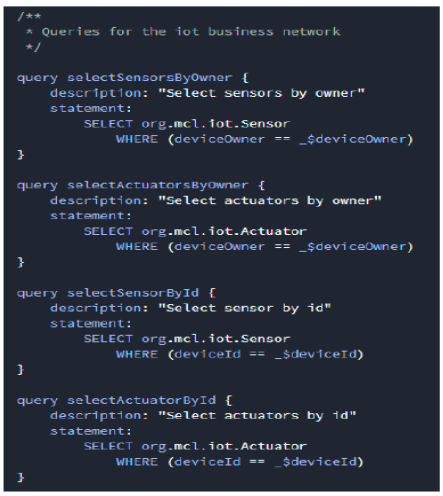
Component	Type	Participant	Condition
Sensor reading	Transaction	Sensor	Asset = Sensor
Actuator writing	Transaction	Actuator	Asset = Actuator
Device creating	Transaction	Device owner	Participant = Device owner
Device updating	Transaction	Device owner	Participant ID = Device owner ID in device asset
Device deleting	Transaction	Device owner	Participant ID = Device owner ID in device asset

The smart contract specifies how a transaction should be carried out logically. The transaction process function is what it is. Figure 3 depicts the structure of the transaction processor functions, which includes a JavaScript function. For example, the transaction processor's function in the actuator writing transaction is to update the status of the actuator asset. This function, in particular, replaces the actuator asset's status with the value passed from the physical device, updates the actuator asset in the registry, and then sends out an event.

```
function ActuatorWriting(tx) {
    var assetRegistry;
    var id = tx.actuator.deviceId;
    var t_actuator;

    var factory = getFactory();

    return getAssetRegistry('org.mcl.iot.Actuator')
        // Get asset that will be updated in this transaction
        .then(function(ar) {
            assetRegistry = ar;
            return assetRegistry.get(id);
        })
        .then(function(actuator) {

            if (tx.newState) actuator.state = tx.newState;
            if (tx.enabled != null) actuator.enabled = tx.enabled;

            // Update the asset in the asset registry
            // (Update Device object in the blockchain)
            t_actuator = actuator;
            return assetRegistry.update(actuator);
        })
        .then(function() {
            // Actuator event
            var actuatorEvent = factory.newEvent('org.mcl.iot', 'ActuatorEvent');
            actuatorEvent.actuatorId = id;
            actuatorEvent.newState = t_actuator.state;
            actuatorEvent.enabled = t_actuator.enabled;
            actuatorEvent.ownerId = tx.deviceOwner.ownerId;
            actuatorEvent.msg = 'Actuator with ID ' + id + ' changed its state: ' + t_actuator.enabled.toString();
            emit(actuatorEvent);
        });
```

Figure 3. Transaction processor function for actuator writing transaction

Queries are defined in a single query file within a smart contract definition and written in a custom query language. It is simple to obtain information from the blockchain network by using queries. Figure 10 depicts queries with a description and a statement. The query description is a string that describes what the query does, while the query statement contains the operators and functions that govern how the query operates.



```
/**
 * Queries for the iot business network
 */

query selectSensorsByOwner {
    description: "Select sensors by owner"
    statement:
        SELECT org.mcl.iot.Sensor
            WHERE (deviceOwner == _$deviceOwner)
}

query selectActuatorsByOwner {
    description: "Select actuators by owner"
    statement:
        SELECT org.mcl.iot.Actuator
            WHERE (deviceOwner == _$deviceOwner)
}

query selectSensorById {
    description: "Select sensor by id"
    statement:
        SELECT org.mcl.iot.Sensor
            WHERE (deviceId == _$deviceId)
}

query selectActuatorById {
    description: "Select actuators by id"
    statement:
        SELECT org.mcl.iot.Actuator
            WHERE (deviceId == _$deviceId)
}
```

Figure 4. Query definition in smart contract.

4. Comparison

We assess the difficulties of blockchain technology in terms of minimizing costs, ensuring the integrity of code, ensuring the reliability of transactions, and integrating multiple blockchains.

In, the execution of SCs is achieved off-chain for cost optimization. Off-chain and on-chain processing methods are proposed on-chain processing techniques are suggested. Off-chain or on-chain storage strategies are chosen. Model engineering is used in most of the presented works to guarantee proper implementation. A preliminary verifying step of the modeling techniques to be transformed into SCs solves the verifiability problem. To ensure the smooth implementation of SC schemes, developers of BPMSs frequently rely on tried-and-true templates. The level of certainty in an action's completion can be adjusted independently.

This study was developed for implementation in public block chain technology, where malicious activities are more common. As a result, the other examined BPMS do not give any thought to the

confidence of execution issue. Using permissioned blockchains does alleviate some of the unspoken fears that tenants have about security. When talking about connecting different blockchains, it's important to keep in mind the confirmation of service in. Multi-blockchain integration is not addressed by the remaining prototypes.

These works view mono-blockchains as internal facilities where various stages of the process are executed.

How to help decide which crypto is better adapted to a particular function is a topic that frequently comes up in preliminary discussions.

VIII. Conclusion and future scope

We reviewed the literature to find out how far along the way to progress reliable blockchain-based BPMS are now. In order to identify the knowledge gaps that still need to be filled, we conducted a survey to identify the challenges of trusted decentralised process monitoring, to catalogue the testable theories already developed in the writings, and to compare and contrast the two. There has been a paradigm shift with in literature against data-centric processes, and the proofs-of-use for blockchain-based BPMSs highlight usability & simplicity of use through model engineering, as shown by the results of this poll.

(iii) A unified front has not been established to standardise the declarative methodology, which seeks to lessen modelling complexity while providing more wiggle room in the execution of processes.

(iv) To functionality IoT data flows, more work needs to be done on satisfactory modelling or system scalability. (v) despite the importance of multi-blockchain integration for maximizing the potential of each blockchain, it has not yet been implemented in blockchain-based BPMS. Our future work will be driven by the market need for data-centric processes that can't currently be met with existing solutions. The ability to track a truck's temperature as it makes deliveries, for instance, and use that information to automatically generate invoices or dispute cases, is an example of smart logistics in action. The challenges of modulization with respect to flexibility, usability, and IoT consciousness will be explored.

As such, we intend to launch a BPMS that is template, declarative, resource-aware, and connected with the Internet of Objects. Specifically, we plan to incorporate a DCR-based method into the creation of our platform.

IX. References

[1] K. Hara et al., “A data-driven analysis of workers’ earnings on amazon mechanical turk,” CHI ’18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2017.

[2] A. A. Casilli and J. Posada, ThePlatformization of Labor and Society, pp. 293–306. Oxford University Press, 2019.

[3] H. Wang et al., “Blockchain challenges and opportunities: a survey,” International Journal of Web and Grid Services, vol. 14, no. 4, p. 352, 2018.

[4] T. Astigarraga et al., “Empowering business-level blockchain users with a rules framework for smart contracts,” in Service-Oriented Computing, pp. 111–128, Springer, Cham, 2018.

[5] I. Weber et al., "Untrusted business process monitoring and execution using blockchain," in Business Process Management, pp. 329–347, Springer, Cham, 2016.

[6] R. Hull, "Blockchain: Distributed event-based processing in a data-centric world: Extended abstract," in Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems, DEBS '17, pp. 2–4, ACM, 2017.

[7] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, 1997.

[8] C. Janiesch et al., "The internet-of-things meets business process management: Mutual benefits and challenges," arXiv:1709.03628 [cs], 2017.

[9] J. Mendling et al., "Blockchains for business process management - challenges and opportunities," ACM Transactions on Management Information Systems, vol. 9, no. 1, pp. 1–16, 2018.

[10] O. López-Pintado et al., "CATERPILLAR: A business process execution engine on the ethereumblockchain," arXiv:1808.03517 [cs], 2019.

[11] J. Mendling, "Artifact-driven process monitoring: Dynamically binding real-world objects to running processes," CAiSE 2017 Forum and Doctoral Consortium, 2017.

[12] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.

[13] A. Singh et al., "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," Computers & Security, vol. 88, p. 101654, 2020.

[14] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, EuroSys '18, (New York, NY, USA), 2018.

[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[16] K. Wüst and A. Gervais, "Do you need a blockchain?," in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54, 2018.

[17] I. Mistry et al., "Blockchain for 5g-enabled IoT for industrial automation: A systematic review, solutions, and challenges," Mechanical Systems and Signal Processing, vol. 135, p. 106382, 2020.

[18] L. D. Xu and W. Viriyasitavat, "Application of blockchain in collaborative internet-of-things services," IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1295–1305, 2019.

[19] V. Pureswaran, "The business of things: Designing business models to win in the cognitive IoT," p. 24, 2015.

[20] J. Webster and R. Watson, "Analyzing the past to prepare for the future: Writing a literature review," MIS Quarterly, vol. 26, 06 2002