IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 18, 2019, accepted October 8, 2019, date of publication October 18, 2019, date of current version November 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2948269

Estimating Service Quality in Industrial Internet-of-Things Monitoring Applications With Blockchain

ANANDA MAITI[1], (Member, IEEE), ALI RAZA[2], BYEONG HO KANG[2], AND LACHLAN HARDY[2]
[1]Discipline of ICT, University of Tasmania, Launceston, TAS 7250, Australia
[2]Discipline of ICT, University of Tasmania, Hobart, TAS 7005, Australia

Corresponding author: Ananda Maiti (anandamaiti@live.com)

ABSTRACT Internet of Things (IoT) plays a big role in automating information generation and consumption in industrial monitoring applications. Blockchain can allow this information to be stored in a manner that is both accessible and reliable for the IoT devices to work with. Blockchain has the capability to collect data from IoT devices and store it in a distributed manner that prevents tampering with the data. This paper discusses the use of blockchain to calculate the Service Quality (SQ) in an Industrial IoT for monitoring application. The proposed framework looks at the blockchain as a finite number of fragmented pieces of data corresponding to a specific industrial *process*. The SQ is expressed as penalties which is the difference between the expected IoT sensor values and the actual sensor data in reported events from the IoT devices. It also moderates the penalty between similar industrial processes based on each other. The moderation allows better understanding of the system functions and identification of specific problems rather than simply recording the sensor data for a single process. Furthermore, this paper analyzes private blockchains for suitability in IIoT and summarizes some key challenges for IoT to be used with blockchain in context of the proposed framework. The paper uses supply chain as a use case scenario for describing the proposed framework and presents results on its technical feasibility.

INDEX TERMS Blockchain, internet of things, cyber-physical systems, logistics, p2p network, smart contract.

I. INTRODUCTION

Internet of Things (IoT) is making big changes in industries by improving monitoring, traceability and transparency of related events [1], [2]. Such IoT systems have been termed as Industrial IoT (IIoT) also called Industry 4.0 in some contexts [3]. IIoT differs from other IoT systems as it requires extensive automation often without any or minimal interaction with human users. As with any IoT application, IIoT devices are designed and installed to collect massive amount of data about a system which can be analyzed to understand and control the underlying events in a better way.

In IIoT, devices can be *fixed* i.e. installed for a dedicated purpose or *re-configurable* where the device setting can be changed and it is re-used for a similar but different purpose. One such application area is 'Asset Tracking' [4] in supply chains. Asset tracking is the practice of using low cost, usually battery powered IoT devices to track the location and status of a specific package being transported from one place to another. In this paper, asset tracking in terms of supply chain is considered as an example application for describing a generic IIoT system with a blockchain to estimate Industrial Service Quality (SQ) [5] or simply performance quality of the multiple *processes* in an industrial system. Service Quality is defined as the difference between the *actual* and *expected* performance from a consumer perspective of the industrial service. The discussions in this paper are limited to industrial *monitoring* systems [6].

Blockchain is a promising and developing technology to ensure the transparency of recorded data in a data-oriented web application. Blockchain is a distributed storage mechanism where ideally each node stores an identical chain of

The associate editor coordinating the review of this manuscript and approving it for publication was A. Taufiq Asyhari.

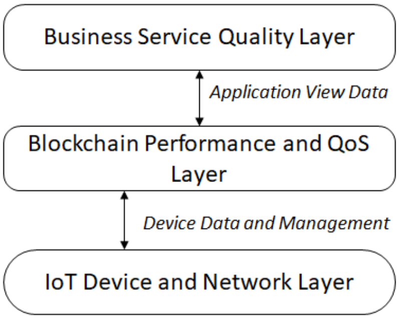

Business Service Quality Layer
Application View Data
Blockchain Performance and QoS Layer
Device Data and Management
IoT Device and Network Layer

FIGURE 1. Different layers of information exchange in an Industrial IoT: IoT and device layer, blockchain layer and SQ layer.

blocks containing a set of data. Each *block*, once created, is final and immutable. Each block contains related information i.e. the hash from the previous block preventing any tampering with the chain of data. Blockchain has the capability to implement *smart contracts* as a distributed application which enables automated and reliable transactions between different parties: *humans* or *devices*.

Blockchain's use with IoT is concentrated around identity management [7], privacy, security and applications in supply chains [8]–[10]. Some blockchain applications have been implemented for asset tracking as well but often include only methods of entering data serially into the system [11], [12]. This paper introduces a method to measure Service Quality (SQ) for IIoT with blockchain as a database. The key focus in the proposed system is that a poor SQ does not equate to a financial penalty, but instead creates an opportunity to improve the service. Without any financial penalties in the blockchain, it can be geared specifically towards recording SQ. This can be done with greater throughput and the system can handle a high volume of transactions for recording. Using a database with blockchain also enables highly configurable searching mechanism that can be easily served to customers and other businesses. The ultimate goal is to moderate SQ parameters of the IIoT systems based on collective information from various IoT nodes with respect to time.

Blockchain's applications in the IoT area are primarily focused on providing a data platform which is shared and immutable [13]. In this context the performance of the IoT device and network is separate from the blockchain's performance and QoS in terms of computing as shown in Fig 1. The IoT layer generates data and blockchain provides a mechanism to manage the devices and collect/store the data. Data exchanged between the IoT and blockchain layers concerns the device management e.g. authentication and identification or formatting of sensor data. Collectively the blockchain and IoT layers form the monitoring system to serve the specific business domain where the IoT-blockchain is applied with the application view data. This data has meaning for the business application logic regarding its operation and service quality based on data from the sensors.

This paper focuses on the business or industrial *service quality* layer at the top, when using a blockchain and IoT. We first analyze the basic performance of a *private* blockchain platform [14] to establish whether it is suitable to achieve a minimum level of the Service Quality for the asset tracking application. Then we propose a smart contract-based method to establish and compare relations between related events with the data recorded in the blockchain from IIoT devices.

The key contributions of this paper include the concept of Finite Transaction Series (FTS) based on the relationship of *assets* and their *attributes*(or *information/properties*) for IIoT monitoring applications. An FTS is a fixed set of blocks containing information regarding a specific *asset* and its *attributes* corresponding to a fixed time-period. Another contribution is the concept of post processing of FTS extracted from the blockchain. As the blockchain is stored in database style (digital ledger), it is much easier to extract and compare data for finding relations between multiple FTS to *normalize* or *moderate* the outcomes of a single FTS. This is done with a reconfigurable IIoT device that can be used to serve a multitude of requirements and still communicate with the blockchain-database.

The remainder of the paper is organized as follows: Section II discusses the related work on service quality and blockchain implementations in the industries. Section III introduces the new proposed generalized framework for IIoT with blockchain. Section IV presents a use case of IIoT to illustrate the implementation and use of proposed framework to configure IoT devices, record data, and process data to *moderate* the data with implementations and results in Section V. Section VI discusses the advantages and critical challenges of the proposed system and future work.

II. RELATED WORK

This section discusses the related work regarding blockchain and its use in Industrial IoT.

A. SERVICE QUALITY IN IoT

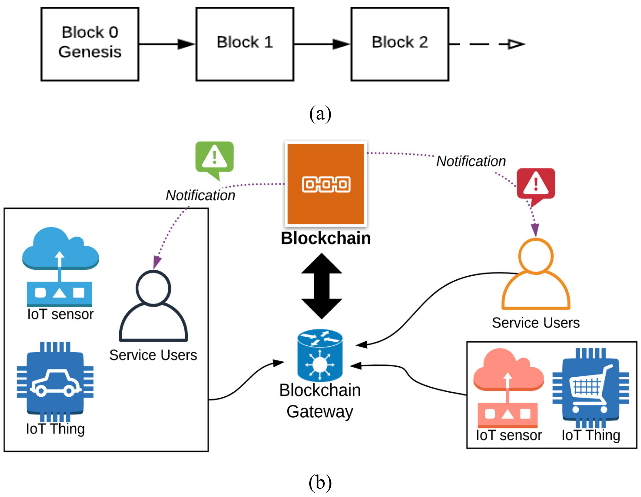
Service quality is depended on two factors: the actual performance of the industrial processes and the performance expectation from the industrial process [15]. Service Quality (SQ) is the difference between the *actual performance* (P) and *the expected performance*(E). Hence, SQ = P − E. For asset tracking, this is about the proper handling of items being transported from one location to another with respect to customer requirements and timeliness. Customers specify a set of requirements regarding the conditions of the items that should be transported. An estimated time of shipment is decided. Using IoT, all the data can be collected and monitored in near real time through a cloud and/or blockchain [16]. If an item is incorrectly handled, then the final Service Quality (SQ) is negative as the *actual performance*(measured sensor values) is lower than *performance expectation*(customer requirements for ideal sensor values). Thus, in this paper we focus on measuring and moderating *actual performance* based on the *expected performance* i.e. customer requirement.

IoT has been used for various kind of service-based applications e.g. smart cities [17], health care, smart home [18] and smart factories [19]. Managing IoT devices using blockchain has also been reported in [20]. This work uses Ethereum as a blockchain platform. A blockchain application is proposed for smart home, mainly focusing on the privacy and security aspects of combining multiple IoT systems into one big system [9], [21]. Several IoT applications have proposed blockchain as a means to meet security and privacy requirements of the IoT systems [9], [10], [13], [22]. While security and privacy can be a factor in the service quality parameter, it is primarily a component of the blockchain and IoT layers as shown in Fig 1. Hence, it is assumed to be static in the current context of estimating Service Quality (SQ) of industrial processes solely concentrating on the IoT sensor data recorded in the blockchain. In order to establish whether a blockchain system is good enough for handling the flow of data in a IoT solution and calculate a Service Quality estimation, the performance of the blockchain as a service is analyzed in the proposed scenario [14] in Section V C. Some methods of performance measurement using a public blockchain e.g. Ethereum is presented in [14], [23] with regards to security attacks and response times.

B. BLOCKCHAIN IN INDUSTRIAL IoT

Blockchain has been around for a decade and its emergent applications in industrial supply chains has occurred over the last few years [24]. Blockchain is a data recording mechanism that has some in-built features to ensure the data integrity. The data is stored in blocks at regular intervals forming a blockchain (see Fig 2(a)) [25]. The whole blockchain is stored by a distributed set of computers preventing its corruption by a few nodes. New blocks are created by participating nodes. A block, once created, cannot be altered and any new update on the information must be freshly written in a new block to maintain integrity and continuity. Each block's hash is stored in the next block, beginning with a *genesis* block that marks the beginning of the blockchain. Blockchains are mainly public i.e. anyone with a computer can join the set of nodes storing/maintaining the blockchain with a consensus mechanism [26]. Blockchain has been used for 'access management' for IoT systems [27] which proposed a management layer between the IoT and Blockchain layer for setting access control rules. In the proposed new approach in this paper, the sensor parameter management mechanisms are implemented between the IoT and Blockchain layer to measure the SQ.

Another type of blockchain is the private blockchain where the participating nodes are fixed and related to the specific application for which the blockchain is created [26]. Private blockchains are typically faster and more configurable in terms of setup and maintenance compared to public blockchains. In this paper, the private blockchain is considered for the IIoT. In [28], [29] Quality of Service (QoS) is defined in context of blockchain itself rather than the application being used for. Both proposes to enhance the use of QoS measurements within the blockchain's architecture including smart contracts to improve its performance. This concept is extended in this paper to measure SQ for the target application and moderate them over time. Blockchain has been proposed to be used for enhancing supply chain management in [30]. It mainly focuses on the business elements of supply chain that can be incorporated into blockchain but does not use any IoT devices.



(a)

(b)

FIGURE 2. (a) Typical blockchain (b) Common architecture of industrial applications using IoT and Blockchain.

Blockchain has been proposed to be useful in industries for automated transactions in manufacturing [31]. The aim of the proposed framework is to make the orders and payments for items to be stored in the blockchain for transparency and automation [32]. In [33] the three goals of using IoT in industries have been stated as confidentiality, integrity, and availability. It describes the usefulness of IoT in various areas from smart homes to smart grids and self-driving vehicles. It mainly focuses on manufacturing company updates for autonomous smart objects in a secure and reliable way [34]. A case of logistics monitoring in Pharmaceutical utilities is presented in [35]. In this, a model is discussed which combines smart contracts and a multi-agent system to improve logistics system, but it does not use IoT devices.

C. BLOCKCHAIN, IoT AND SUPPLY CHAIN

In [25], [36], [37] a range of applications are discussed for many industries including food, pharmaceuticals and postal services. An Ethereum based tracking system has been proposed where a sensor is used to track the status of medicines. If they are not within a specified range, a set of penalties are applied for accountability [34]. However, this approach does not propose a relation between different data sets from multiple assets. In [36] a method is proposed to use IoT and blockchains to create secure, shared economy distributed applications mainly focusing on the exchange of currency for services.

Fig 1(b) shows the typical system architecture of IoT and Supply chains as reported in several works [16], [25]. The system contains IoT sensors and human users who upload data directly to the blockchain through a blockchain gateway. In other cases, the human users work with the IoT devices e.g. authenticate manually before the IoT data is sent to the blockchain gateway. The blockchain gateway is a special node that accepts the data from the devices/human typically with HTTP communication and then posts in the blockchain. Periodically, the blockchain sends some notification to the users when some conditions are reached.

A use case about fresh food delivery with blockchain is demonstrated in [38]. This work focuses on showing the critical aspects of implementing a specific blockchain solution in terms of Business Strategies. It however does not discuss any moderation methods to operate over multiple sets of transactions in the blockchain. Post processing of blockchain data is discussed in context of a pay slips calculation application in [39]. However, this work is not focused on Industrial IoT. In [40] a credit system is discussed to rate the participant in a food supply chain. This work discusses effectiveness of supervision and management in the food supply chain. It does not include any IoT, but instead relies on textual data entered by people as the source for determining the value of credit for the peers in the food supply chain blockchain system.

Many previous works [41], [42] in supply chain focus on the traceability of items between different parties in the supply chain. They often do not enable post processing to moderate the effects of traceability to determine the Quality of Service, as is the aim of this work. Some works have concentrated on the provenance of products in a supply chain, but not on the moderation of application data in the blockchain [43], [44]. In [45] a method to use blockchain for data accountability and provenance tracking focuses on the data and its storage which is not sufficient in an IIoT monitoring application. Blockchain has also been proposed to be used for auditing in industries and business [46], [47], but not with IoT devices. These systems enable the auditors to check the details of any entity, trace it back to its origin, find discrepancies in records, and settle disputes. This paper focuses on a similar outcome by post-processing blockchain data corresponding to industrial processes.

III. NEW GENERIC FRAMEWORK FOR IIoT AND BLOCKCHAIN

This section provides the details of the new proposed framework for creating an IIoT blockchain application.

A. BLOCKCHAIN AND DATABASE: ASSET VS INFORMATION

As the origin of blockchain lies in crypto currency, blockchain primarily deals with *assets* such as coins. An asset, such as a coin or similar product in the current context, is exchanged between multiple owners in the blockchain represented by an account with a public/private key or an address. Such assets are also referred to as UTXO or Unspent Transaction Output in some blockchains. Assets can be divisible items such as coins, or non-divisible items which must be exchanged in whole. Other blockchain platforms e.g. Hyperledger Fabric [48] are primarily geared to store the information only. The lack of inherent assets, e.g. coins, that can be *locked* to a specific owner, means the developers must create corresponding software layers in chaincode or smart contract to enforce the ownership and exchange of assets.

The key to implementing a successful IIoT and blockchain is the ability to maintain the ownership of an asset and update its associated *attributes* i.e. *information or metadata*. While an asset may be possessed by a specific owner at a given time, its attribute or information may change while still in possession of the owner. To do this, a proper data storage feature is required. An asset should not be accessible once it has been de-activated. It should be updatable without having to transfer the item out to some other account or address. Data must be extractable from the blockchain with direct queries. The aim of the proposed system is to identify related transactions from the blockchain corresponding to similar set of transactions. Once the related transactions are identified, the subsequent related transactions are *moderated* accordingly.

B. IoT DEVICE SETUP

The description of the IoT device is kept generic to suit any kind of requirements. An *asset* in the proposed blockchain is the *logical* representation of objects associated with a corresponding IoT device attached to physical objects. Each IoT device consists of a set of sensors $\kappa = \{k_0, k_1, \ldots k_n\}$. The sensors measure a specific parameter from the environment. Each sensor k_i has a specific upper and lower limit in terms of measurement. The limits are stored in two matrices L and U such that,

$$L_i < k_i < U_i \tag{1}$$

L and U form the range of desired customer expectation from the industrial processes in terms of the SQ. Each device has a micro-controller and communication mechanism. The micro-controller in the device monitors the sensors and determines if any rule has been broken i.e. if a sensor returns a value beyond a desirable range with respect to the application. If a sensor reports an event, then a message is created with a timestamp and all the sensor values in a JSON format.

The communication mechanism can be – WiFi/Ethernet with direct Internet connection, LPWAN such as LoRa, or cellular connection. In the latter two, the data is sent to an Internet gateway. The data is ultimately transmitted to a set of servers running the blockchain. The IoT devices may have problems with sensor monitoring and the transmission of data if it is battery powered or placed in low or intermittent communication coverage areas. IoT device identity can be created in two ways:

i. The IoT device can have a *static ID* put in by manufacturer. When a static ID is used, the IoT devices download the information from the blockchain when initiated. However, this method requires a new asset information to be associated with the IoT device. With a static ID there is an increased chance of forgery by other devices using the same ID.

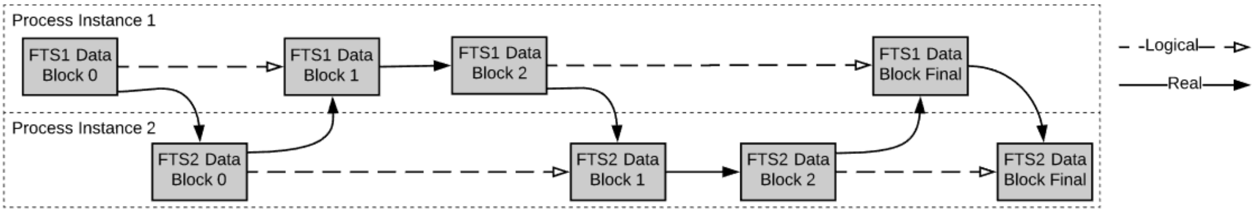


FIGURE 3. The finite sized transaction series for FTS1 and FTS2 within the same blockchain representing two different instances of industrial process.

ii. A *dynamic ID* that is loaded into the device each time it is initiated. A dynamic ID is assigned by loading a new ID every time an IoT device is initiated for a new set of transactions. This method requires manual entering of data into the IoT devices.

Unlike some IIoT applications, where sensor nodes are blockchain peers, in the proposed framework this is not required. The devices are low-cost external nodes generating data in specific conditions. The devices communicate with the blockchain through a gateway. The IoT device can upload data:

i. at regular fixed intervals of time. This could lead to higher power consumption, but it can generate more data points if required when the change in environmental parameters is slow.

ii. only when a specific condition happens e.g. sensors generating an interrupt to record an event.

C. PROCESS AND FINITE TRANSACTIONS SERIES

A Finite Transaction Series (FTS) consists of a *finite* set of blocks $\{B_0 \dots B_f\}$. An FTS is stored in a blockchain as shown in Fig 3. The blocks belonging to an FTS is a subset of all blocks and interleaved with blocks from other FTS. The FTS is always associated with a specific repeatable "*process*". The "*process*" is finite in terms of time and series of events associated with an *asset*. A *process* can be repeated multiple times, each time with a new FTS. A process can have some common properties with another process. A new *process* is started when an IoT device is initiated and associated with an *asset*. The *process* is composed of a series of transactions, ordered chronologically, corresponding to each event with the IoT device. Each transaction is stored in a block B_i. A block B_i consists of a set of data for a set of sensors associated with the *process*.

The FTS starts when the *process* starts at t_0 and ends when the process ends at t_f. Once the process is over, the asset is de-activated, uninitialized and the FTS is archived for read-only purposes. Each FTS is associated with at least one *Smart Blockchain App*(*SBA*). The *SBA* monitors the content of the messages containing sensor values and invokes a sub-routine accordingly to determine a SQ *penalty* $\alpha(p)$.

Two FTSs can be equivalent, if they are associated with the same type of *process*. For this, all the sensors have to be same or similar, measuring the same parameters within the process' environment with a one-to-one relationship between sensors for FTS_1 and FTS_2. Two FTSs can be partially related if there is at least a subset of sensors that measure the same parameters for the two processes. A process can be defined as

$$p = \{pid, start, end, \{conditions\}, L, U, \kappa\} \tag{2}$$

where, *pid* is a unique process id, L and U are the sensor limits. *start* and *end* are the starting and ending conditions for the process. This could be typically a time stamp e.g. t_0 and t_f. Thus,

$$\begin{aligned} &p_i \equiv p_j, \text{ if} \\ &k \ \exists \ k \in \kappa_i \wedge k \in \kappa_j \text{ and} \\ &c \ \exists \ c \in \{conditions\}_i \wedge c \in \{conditions\}_j \end{aligned} \tag{3}$$

{conditions} is a set of optional values. This could be simple static set of markers relating to the processes.

Service Quality (SQ) in any industry is a measure of the performance of the agents within the industry from the customer or the service users' perspective. There are multiple ways to measure and quantify the SQ for different industries [49]. In this paper only a linear measurement model is considered where a set of sensors report the current state and condition of a process which is directly considered as the service quality of the process.

D. SMART BLOCKCHAIN APPS

In the current context, the smart contracts [11] are termed as a generic '*Smart Blockchain Apps*' (SBA). They are responsible for entering data into the blockchain and maintaining ownership of the *logical* assets. Smart contracts in Ethereum or similar platforms aim to transfer coins upon satisfaction of certain conditions within blockchain. This is not necessary in the current context as no transfer of currency takes place. The data is simply recorded in a transparent manner for SQ. The critical point is that the data stored in blockchain must be sourced properly i.e. it must be ensured that the data entering the blockchain is correct and known to all peers in the system.

SBA for the IoT application must allow programming capabilities and be able to read from and write to the blockchain. SBA are designed by a peer and agreed by other peers before the contract or its '*hash*' is stored in the blockchain. This means the SBAs need not be executed from within the blockchain. The SBAs are run by dedicated nodes maintained by the peers of the IoT application communicating with the blockchain. The SBAs must have a set of functions:

i. '*create*' function to create a new asset or re-initialize an old IoT device after it has finished a process.

ii. '*record*' function enters new information updating the attributes of an asset.

iii. '*query*' function checks if a variable and its values exist in the blockchain and returns the value if it exists.

iv. '*status*' function to determine the final information of the FTS such as the height of the FTS. This is useful when an FTS is archived for read-only purposes.

v. '*burn*' an asset i.e. make an asset un-initialized i.e. its attributes cannot be updated.

SBA can interact, communicate with, or affect other SBA if they are associated with the same type of *process*. The data stored in an old FTS is still available for other SBAs running on a new instance of the same process.

E. SYSTEM SETUP

The proposed system is operated with a proof-of-authority (PoA) consensus or similar. The PoA is the most suitable as the privacy of the data is not critical because the IIoT system is used for industrial purposes and accessible to only the relevant participating industrial entities. The main attributes of blockchains [50] that are useful in this case are:

- '*Transparency*' in sharing the events and data related to the processes among the peer industrial entities. The blockchain stores the data securely. As the blocks are immutable, the data available cannot be altered or misinterpreted by any peer.
- SBA that automatically records events and provides notifications and feedback to human users.

Previous works have suggested multi-organization based blockchains [51]. In line with that, the proposed IoT system can be operated by a set of peer businesses and clients (see Fig 4). Each peer can host a server for the blockchain. They can all access the data in the blockchain. PoA mechanisms assume that the number of nodes is known to all and each node in the system is uniquely authorized to access the blockchain. This prevents any malicious nodes to enter the system and create a problem with consensus. Each peer has a *public/private* key to identify itself in the blockchain network. It uses the public key to create/update assets in the blockchain. A peer is a *view-only* peer if it can only view the blocks' contents and optionally validate the blocks before they are added. But it does not propose a new block. Other normal peers can both propose and validate a block in the blockchain.

Apart from industrial peers, there can be some other related nodes to help with the consensus. These peers could be authorities or regulators that monitor the industrial transactions between the industrial peers. A *client* node is a view-only node which commissions a *process*. A client node accesses the data from the blockchain through a web interface. Unlike peer nodes, client nodes can only view details from the blockchain that concerns the process commissioned by them. A *client* can also become a view-only or normal peer node depending on its involvement and investments with respect to other peers.

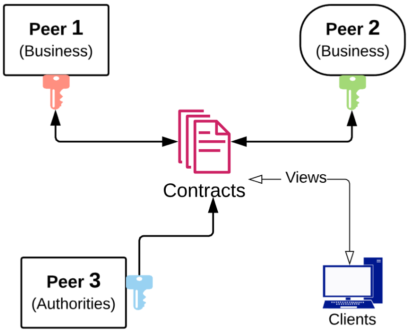


FIGURE 4. The components of proposed IIoT-Blockchain: (a) multiple business peers (b) authority (non-business) peers (c) clients.

F. SQ MODERATION MODEL

For the proposed framework, we define SQ penalty like SQ. While SQ tries to measure how good the service is, SQ Penalty tries to calculate how bad the service is. If there is no penalty, then the service is as expected and if SQ Penalty is greater than 0, then the service is poor. As the data is collected through IoT, the framework does not capture any performance data outside what is being observed by the IoT for a process. This means that the SQ penalty is the deviation of the sensor values from the expected sensor values as set by the peers or clients. Each time the *SBA* detects an anomaly in the sensor data in the FTS, a penalty α is calculated depending on the sensor values. The final cost is determined by accumulating all the penalties α. The raw penalty $\alpha\,(p)_u$ for a state of κ is calculated according to the deviation from the permissible limits of κ. $\alpha\,(p)_u = 0$ if the sensor states u i.e. an instance of κ is within the limits, otherwise $\alpha\,(p)_u > 0$. The moderated penalties are calculated with the values from older FTSs. The final SQ penalty for a process p is

$$Final\ SQ\ penalty = \sum_{u=0}^{\varepsilon} \beta\,(p)_u \tag{4}$$

where, ε is the total number of cases when the device reported an event for process p; and u is the state of a sensor reported by the IoT devices in those events. The moderation $\beta(p)_u$ is determined by:

1. Searching for all process y in the blockchain such that $y \equiv p$.

2. If $\alpha\,(p)_u = 0$ then $\beta\,(p)_u = 0$, otherwise if $\exists\alpha\,(y)_u > 0$ i.e. there is a sensor state u for which there is any event report for value u in other processes, assign $\beta\,(p)_u$ with a positive value e.g. $\beta\,(p)_u = function(\alpha\,(p)_u)$ where *function* is part of the business logic as collectively defined by all peers using the blockchain.

In the current context, no digital currency is required for the penalty. The peers can decide on the actual monetary values associated with the calculated penalties and cost as part of a mutual agreement. The cost and penalties that are calculated by the SBAs are only indicators of the SQ. No real monetary cost may be associated with the processes in the FTSs.

In order to estimate the SQ of an IIoT the following must be ensured:

- The IoT-blockchain system must be able to handle a large number of requests, possibly in bursts when multiple events occur around the same time. The data to be stored must be propagated through the network and the blockchain updated on every node. This aspect of blockchain is technical depending on the characteristics of the chosen blockchain and discussed in detail in Section V C.
- The industrial process must be identified, and the corresponding attributes must be set accordingly to create the corresponding moderating functions. This is illustrated with an example in the next section.

IV. USE CASE SCENARIO

In this section, a use case is discussed with respect to the transport and delivery industry. The IoT device is constructed and tested to generate the data in real time. The system is emulated in a blockchain with 4 peer nodes and the data is presented in the next section.

A. THE PEERS

There are 3 peers considered in the model (see Fig 5) with an option of the client being 4th peer if they wish to, making it a 4-peer use case scenario. Each peer is capable of setting up a peer node with a server for running the blockchain. Each node can store the full blockchain. Each peer node is authorized to access the blockchain with a unique 'private key' to authorize itself. The 3 peers act as validators for the FTSs. The 3 peers are:

1) TRANSPORT

This peer is the key player in the industry. They have to send the certain items e.g. 'furniture' or 'glassware' to different geographic locations i.e. source to destination. The items i.e. assets have to be transferred in a safe manner. An IoT device is attached to every carriage every time a delivery is made. The IoT device consists of a gyro sensor and GPS module.

$$\kappa = \{k_{gyro}, k_{gps}\}$$

The aim is to measure the amount of dis-orientation of the cargo. Each time the cargo is dispatched a new 'process' is initiated. The process in this context has a schema:

$$p = \{id, source, destination, \{cargo\_type\}, L, U, \kappa\}$$

where cargo_type is an application specific condition (from Eq 2) defining the type of cargo e.g. if it is glass furniture or wooden furniture. *source* and *destination* locations of the objects being transported are the *start* and *end* parameters of the process. Each time the IoT device is (re-)initialized, the process is (re-)started with a new value for each element in p. The corresponding FTS can store the gyro sensor values and the corresponding GPS locations. If a sensor reports a dis-orientation beyond acceptable levels $\{L, U\}$, a new transaction is created for it. The SBA then calculates the cost and penalties as described later.

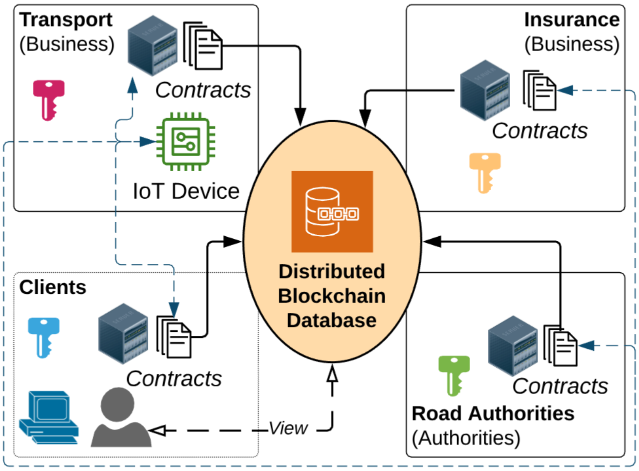


FIGURE 5. The 4-peer transport use case scenario.

2) INSURANCE

Insurance is concerned with recording the SQ. Any real damage to the items during and after transportation is compensated accordingly. The insurance company wants to calculate the SQ penalty as the data is important to determine which peer is more responsible for any real damage.

3) ROAD AUTHORITIES (RA)

In this use case the transportation is done by road and the quality of the road affects the SQ of the transport company. Also, the data from the sensors can help the road authorities to identify any problem with the roads. The road authorities also own the road assets i.e. 'road (source, destination)' which are non-transferable. But the road authorities can add information to the blockchain if the road is currently all good or any incident has occurred at a specific GPS location on the road between source and destinations.

4) CLIENTS

The clients are the customers who use the transportation service for delivering the items. They can view the status of the process and can act as a 4th peer node if they can. Otherwise they can view the status in a web interface. The clients see the end cost and penalties calculated by the SBAs for their deliveries. They also set the acceptable limits of disorientation that are put into the blockchain by the Peers and stored in the blockchain. As the SBA is run with the blockchain, the clients are guaranteed the expected SQ or a suitable penalty, if applicable.

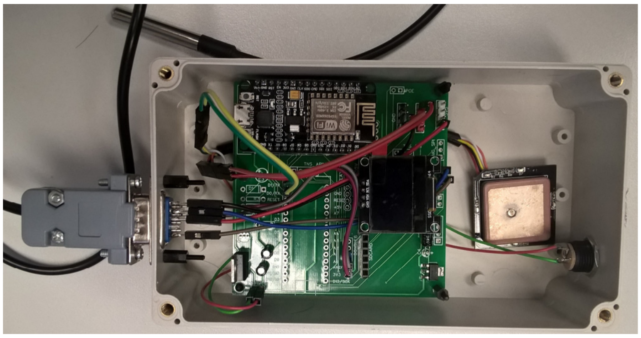


FIGURE 6. **The prototype reconfigurable IoT device. It is connected to a temperature sensor.**

B. IoT DEVICES AND GATEWAYS

The physical IoT devices are owned by specific peers. In this case, the transport peer owns the devices and is responsible for resetting it when required. The clients practically hire the IoT devices by attaching a *logical* asset to it for a specific *process*. The ownership of the corresponding asset must be managed correctly. Only owners of an asset should be able to add information for that asset. Also, only owners can transfer assets to another peer in the blockchain, losing the ownership is a one-time only process. A non-owner is neither able to add information nor transfer it.

The device is designed with a microcontroller (e.g. NodeMCU) and a multi-purpose port. The port is able to connect to a variety of sensors. The exact type of sensor used for a specific *process* and FTS is fetched from the blockchain at the beginning of the process with the asset. The information regarding the sensor type and upper and lower limits (L, U) are specified by the client while creating the logical asset and transferring it to the transport peer. Once the transport peer receives it, only the 'Transport' peer updates the information of the asset. Once a process is finished, the IoT device is detached from the logical asset. It can be re-used for another process for the current use case scenario of furniture transfer or completely different application scenario by attaching it with a new logical asset.

The physical device is shown in Fig 6. The device constitutes of NodeMCU which is based on ESP8266 running at 80 MHz. It is battery powered. It can connect to WiFi when in range in order to upload sensor information or download customer settings. It also has two PORTs one is connected to a dedicated GPS module (ublox NEO M8N). The other PORT is open and can be connected to various sensors. In a practical scenario, there can be multiple sensors connected to the IoT device. In the picture the device is connected to a temperature sensor DS18B20. The device is reconfigurable i.e. the settings for the desirable transport conditions can be set by the customers in the blockchain. Depending on the current association of the device to an item, the corresponding settings are downloaded.

C. SBA VERIFICATION STRATEGY

SBAs have the primary task of authenticating any change in ownership of an asset between peers. Besides that, the SBAs also enter the metadata into the blockchain. SBAs are created or technically offered by one or more peers, in this case a business peer i.e. the 'Transport' peer. The SBAs rules of calculating the SQ penalty in terms of incoming IoT data is open knowledge and the code is available to every peer.

For IIoT the data is generated autonomously and remotely. Also, the corresponding appending metadata of any asset is autonomous as well. This means that end users. clients or other peers (different from the peer owning the IoT device) have no control over the data that enters the system through the blockchain IoT gateways. An SBA is either a smart contract or similar mechanism is used to enter the incoming IoT data into the blockchain. However, a malicious business peer can set up separate proxy SBAs to enter fake transactions to populate the blockchain with "favorable" data that benefits them when calculating the SQ penalties. In such a case, non-owner peers cannot tell the difference between the real IoT data and the fake data entered in to the blockchain even though the original smart contracts or SBA are working as decided unanimously. Thus, an additional safety feature is required.

The SBAs must allow the peers to validate the data that is generated by the IoT device and the data that was entered in the blockchain. In the current scenario, the Furniture company owns the devices and operates them. Thus, they are primarily responsible for entering the IoT data into the blockchain. However, the IoT device sends the data simultaneously to all three peers and optionally to the client SBAs as well. These SBAs can then check whether the data entered by Transport peer into the blockchain is the same as what they received from the IoT device.

D. PENALTY FUNCTION (α)

Penalty function (α) is calculated independently of any other transactions in the blockchain. It is a raw value calculated based on a single event report from an IoT device. The SBA compares the reported sensor value u_{gyro} to the corresponding upper and lower limits. If the sensor value is not within limits, a penalty is recorded along with the sensor values. In the current use case for a process p at the GPS coordinate g,

$$\alpha\,(p)_g = \begin{cases} \{u_{gyro} < L\} \vee \{u_{gyro} > U\} & 5 \\ Otherwise & 0 \end{cases} \tag{5}$$

The final penalty without any moderation is the sum of all penalties i.e. $\alpha\,(p) = \sum \alpha\,(p)_g$. In the current scenario, the GPS sensor is not measured for discrepancies. However, the GPS may also be passed through a function to determine if the items have been in any unwanted GPS locations and penalized accordingly.

E. PENALTY MODERATION

Once the penalties are calculated, they can be moderated depending on the other similar process/FTS. The adjustment to the penalties is calculated based on the GPS locations of the reported disorientation k_{gps}. If multiple disorientation is reported at the same GPS location for multiple FTSs,

Algorithm 1 *Moderate* (Process p, GPS Coordinate g, Day d)

```
if there is any current incident report at g from RA in Blockchain
        $\beta (p)_g = 0$
else
    $\upsilon = 1$
    For each process $y \in$ Blockchain
        if $y \equiv p$ and $d = today$
            if $g \approx g'$ and $\alpha (y)_{g'} \neq 0$ and $\alpha (p)_g \neq 0$
            $\upsilon \leftarrow \upsilon + 1$
    $\beta (p)_g = \frac{\alpha (p)_g}{\upsilon}$
```

it indicates there is a problem with the road at the specific location g. Two process/FTS i, j can be related using Eq 3:

$$\begin{aligned} &p_i \equiv p_j, \text{if} \\ &\{k_{gyro}, k_{gps}\} \subset \{\kappa_i \cap \kappa_j\} \text{ and} \\ &\left\{cargo_{type}\right\}_i = \{cargo\_type\}_j \end{aligned} \tag{6}$$

The penalty is divided by the number of processes that reports the same location k_{gps} in their respective FTSs to calculate the adjustments β according to Algorithm *Moderate*.

The above algorithm is explained with a typical scenario for the *moderation* as shown in Fig 7. Two trucks A and B are delivering items from source to destination. Both contain same type of furniture with GPS enabled IoT devices. Truck A faced disorientation e.g. skid off the road or has a sudden brake at two GPS coordinate g_1^A and g_2^A. It accumulates two penalties of 5 for the lower than expected quality of service, hence final penalty without moderation $\alpha(\mathrm{A}) = 10$. Later when truck B goes through the same path, it faces an incident in $g_1^B \approx g_1^A$. At this point, $\alpha(B) = 5$. But the SBA operating on the blockchain finds the FTS for the process of truck A recorded earlier. So, there are 2 related FTS/processes each corresponding to a truck. Once the FTS data is analyzed, the SBA finds that truck A and truck B faced a similar incident in the same GPS coordinates g_1 and moderates the penalties with $\beta_{g1} = 2.5$ ($\upsilon = 2$). Thus, the actual penalties are calculated as 7.5 for truck A and 2.5 for truck B. If there is any current incident report from RA in the blockchain then no SQ penalty is applied. This algorithm can be further expanded by including, the trucks that make it alright without reporting any problem at g_1. υ is the count of common FTS with $\alpha > 0$.

The key point here is that despite poor SQ, the furniture may be delivered in good condition, hence no real penalty may be applied to the transport company. But moderating the SQ penalties generate new information regarding road condition which is useful for a third peer – road authorities. Alternatively, the road authority's information helps moderate the penalty on the transport company. If there was initially no incident report at g_1 then the penalties are calculated and applied. In this use case scenario, it is possible for the RA to validate a road problem at g_1 after a process is finished and this could affect the originally calculated moderation and possibly restore the original penalties for g_1. Calculating the penalties in real-time enables real-time feedback to other nodes as well.

V. IMPLEMENTATION AND RESULT

This section discusses the implementation of the described system. The choice of a proper blockchain for a specific application is very important. Some applications require currency inherently while others mainly aim to store records. Ethereum is the staple choice of blockchain, but it requires users to pay to store the information on the main Ethereum. Setting up a private Ethereum chain may be similar to using a Hyperledger Fabric (HF) [48]. HF has been used for asset tracking but does not inherently support the asset management of ownership and transfer. As it is more of a ledger, chain codes have to be created to check and maintain ownership of devices. Thus, BigchainDB [51] is used for this implementation, *although* it can be implemented using any of the blockchain discussed here.

A. BIGCHAINDB AND TENDERMINT BLOCKCHAIN

BigchainDB is a combination of Tendermint and MongoDB. Tendermint is used for consensus between peers and maintain the states of the blockchain. MongoDB is used to store the data. Storing data in MongoDB allows various queries to be executed and data retrieved in various ways. Tendermint and BigchainDB is a private blockchain using a private/public key for authorizing access to the blockchain. Tendermint uses a form of Proof-of-Stake consensus where the peer with the highest stake has priority while creating a new block. However, the voting power of each node is the same. Thus, it becomes a simple PoA consensus mechanism.

BigchainDB does not have an inbuilt smart contract system as a Dapp (Decentralized Application) that runs within the blockchain. Instead, the underlying Tendermint has an API called *Application Blockchain Client Interface* (ABCI) to call various methods to be executed on the blockchain from an external application. BigchainDB provides more HTTP APIs and other drivers to communicate with the blockchain from the blockchain apps. BigchainDB itself is like a smart contract based on the Tendermint as it enforces some rules for maintaining data integrity. For e.g. an asset created in the blockchain is created by a specific user and initially owned by that user. BigchainDB then allows the item (identified with a unique hash) to be transferred to another peer, but it prevents double spending i.e. the original owner cannot re-transfer the same asset again. Information about an asset can only be updated by it's owner.

It is very easy to track an asset in the blockchain with its ID in BigchainDB. BigchainDB allows implementation of the FTS as shown in Fig 3 inherently, by allowing the users to view a series of transactions connected by *transaction id*. It also allows retrieval of all the assets currently and previously owned by a peer. BigchainDB allows retrieval of all the transactions related to each asset and determine its FTS.

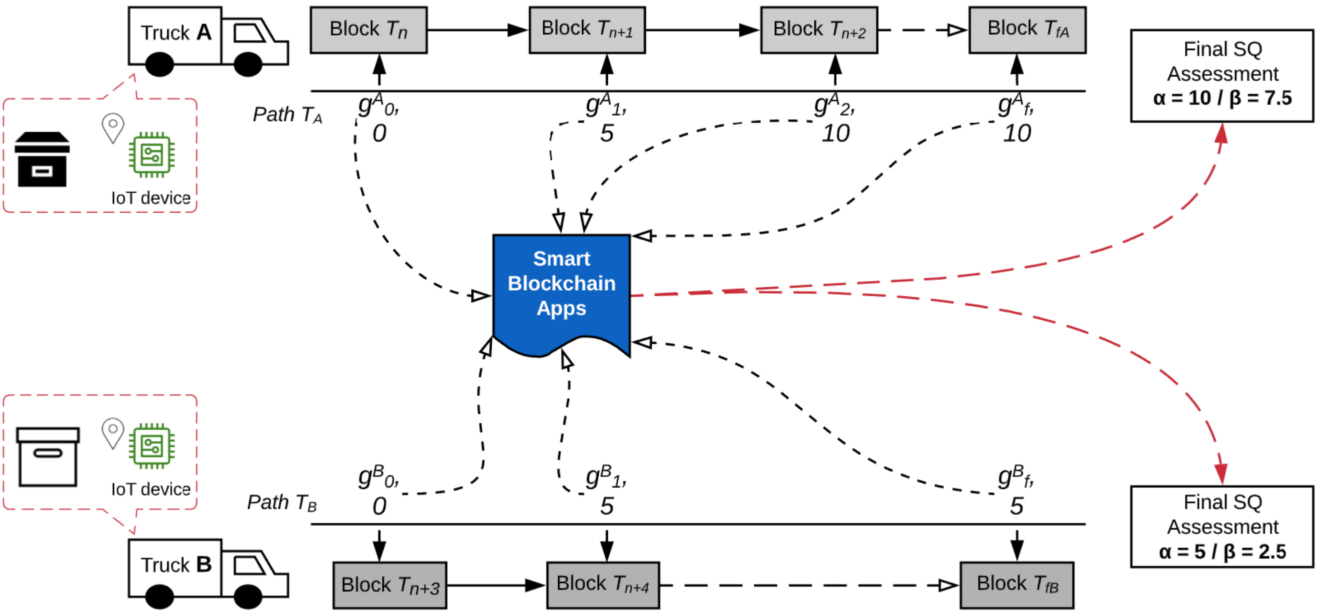


FIGURE 7. A typical scenario for recording IoT data in blockchain; calculating Service Quality (SQ) penalties and then moderating the penalties with respect to data from other devices. Initially Truck A accumulates a SQ penalty α of 10, but this is moderated to 7.5 after comparing the FTS data with another FTS from truck B. Truck B also benefits from the moderation.

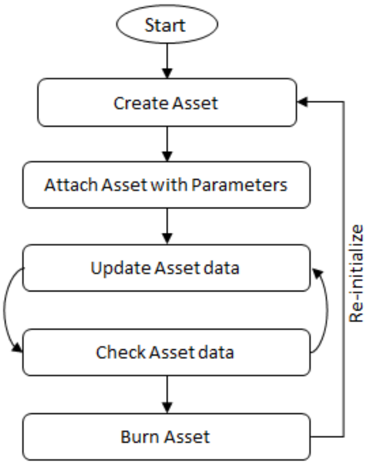


FIGURE 8. The flow diagram for an asset's *process* with an IoT device.

B. MANAGING IoT DEVICES AND ASSETS

The process flow is shown in Fig 8. Initially the *logical* asset is created and owned by the client in the BigchainDB. Then the client transfers or registers it to the transport company, attached with metadata which is the parameters of the process i.e. $\{pid, source, destination, cargo\_type, L, U\}$. This is termed as (re-)initialization of the IoT device. When the IoT device is switched on, it first downloads the *process* parameters from the blockchain. The device also receives the idetification *pid* and peer gateway information from the blockchain as part of the asset's process data. After that, the device can update the status of itself which is maintained as metadata in subsequent blocks of the blockchain. Once initialized, the asset is possessed by the transport company in the blockchain. In a more elaborate scenario, the asset may be transferred to other transport peers if there are more than one transport company involved in the supply chain. Only the current owner can add the incoming IoT data into the blockchain.

The device records data $\{g, u_{gyro}\}$ for a period of time and uploads data at regular intervals of 10 mins. When new data is appended to the metadata of the assets, SBAs calculate the raw penalty $\alpha\,(pid)_g$ from Eq 5 and perform the moderation on the stored data as discussed earlier with algorithm *Moderate(pid, g, current_day)* to append moderated penalties with passing time. When the item reaches the destination, the logical asset in the blockchain is *burned* and the IoT device is un-initialized. After some time, the same IoT device is used for another process which may be same as the previous one i.e. with the furniture and gyro sensor or a completely new asset e.g. food with temperature sensors. The new client then creates another asset and the process repeats itself.

The SBA verification strategy is used with the IoT devices as shown in Fig 9. The IoT devices sends the data to all 4 gateway nodes each hosted by corresponding peers. Each host run the same SBA as a dapp. The SBA is created by the transport company and agreed upon by the peers before being deployed. Other peer nodes verify that the incoming IoT data entered into the blockchain by the 'Transport' company, as they also receive this same data from the IoT device in their SBA.

To create the SBAs, another layer of consesnus has to imeplemnted such as lotionJS [52] or chaincode in HF using oracles. lotionJS based SBA can work with Tendermint as

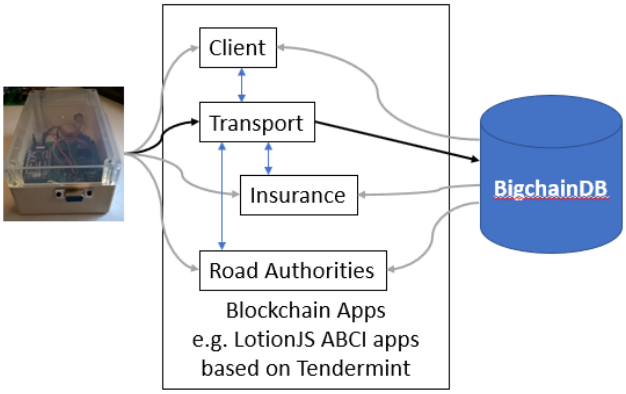


FIGURE 9. SBA verification with data from IoT device to BigchainDB through SBA.

well and provides a mechanism to send transactions to the blockchain while maintaining the blockchain states for an FTS regarding the asset's metadata within the lotionJS program. Each lotionJS SBA program has a unique identifier called GCI that can be used by other lotionJS program to obtain its state for an IoT device. The same SBA must be run by all peer nodes and each node's FTS state data is synchronized. If a peer alters the program, then the states in other peer nodes will lose synchronization. Thus, it prevents the SBA to be altered by someone without alerting all peers.

C. RESULTS

A test was done to measure the transaction rate for the system with 4 nodes. This test was done to establish the first requirement of estimating service quality for IIoT on whether the blockchain is able to handle large quantities of data and transaction requests. Each node was a 3.2 GHz machine with 2 GB RAM running the BigchainDB software. There were 3 rounds of tests with different latency or round-trip time (RTT) between each node 10ms, 50ms, and 250ms, with a tolerance of 40ms and 15% co-relation between successive requests. The RTT was established with ubuntu's *netem* module. In each round of test, a total of 500 transactions were sent to the blockchain in different frequencies of 10 transactions/second (or 10 Hz), 50 Hz and 100 Hz. In one part of each test run all requests were send to a single node and in the second part of the test the request was equally distributed to two nodes in the system.

Fig 10 (a) shows the corresponding results. The blockchain missed multiple transactions when transactions are sent at a higher frequency. But it is also clear that when the requests are shared between two nodes the success rate for the transactions to be successfully stored is much higher. In Fig 10 (a), the X axis shows the frequencies for two cases (a) *Distributed* request between 2 nodes and (b) *Undistributed* using only one node. The Y axis shows the success in percentage of the total request from the IoT devices. The time taken for all successful transactions was under 1 second, meaning they have an advantage over the public blockchain like Ethereum, in context of the IIoT applications. The impact of larger RTT is not much when the RTT is 10ms and 50ms. It drops to 90% when the RTT is 250ms. With an undistributed strategy, the success rate is always very low and the impact of the RTT is slightly larger.

Regarding implementations, it is necessary to measure/estimate the maximum possible transactions in a system with a fixed number of peers and known network architecture. Also, in a real implementation, the Transport peer SBA must ensure that the transaction requests are distributed equally among the peers' BigchainDB on the system to avoid a DDoS style attack on the system.

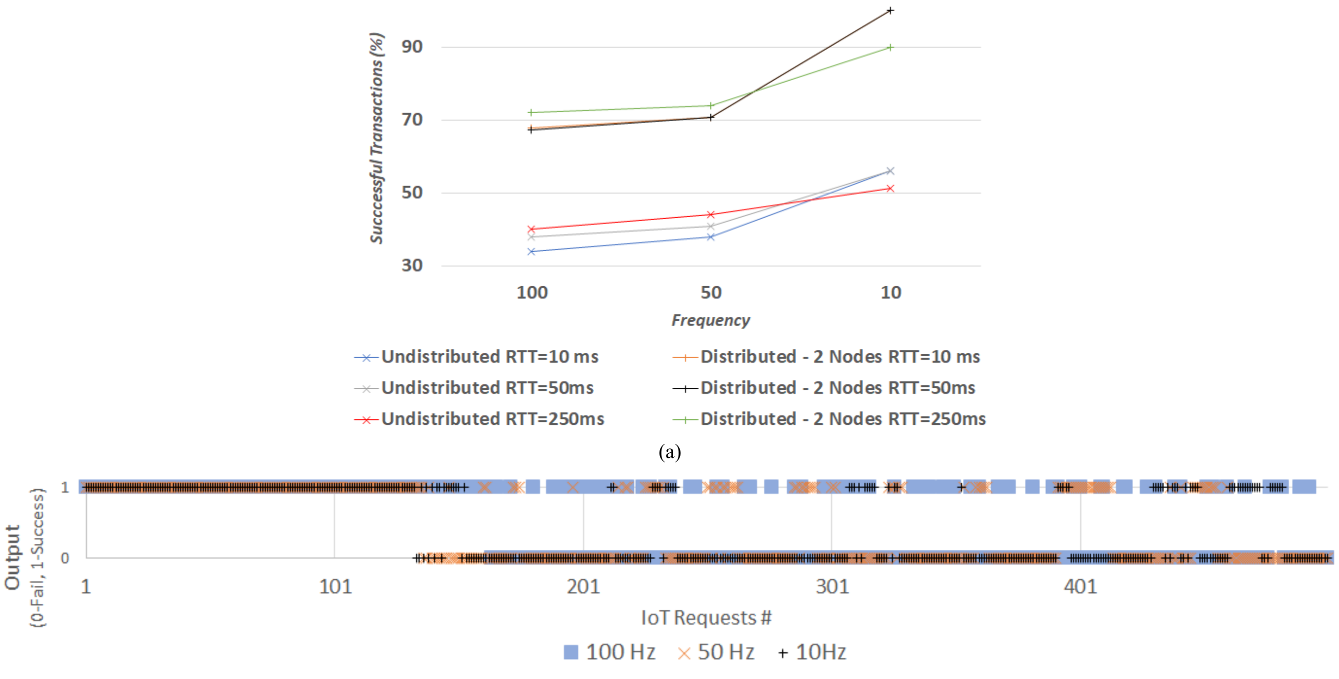
Fig 10 (b) presents the sequence of requests in case of the undistributed requests. In all scenarios of undistributed requests, the blockchain the system is able to register more than first 100 requests before it starts to drop out. This indicates that the memory pool available for the blockchain affects the storage capability more than latency between the nodes. For the IIoT, this is acceptable if the rate of inputs is distributed and data is pushed in to the blockchain in bursts, e.g. 100 data points from sensors almost simultaneously, which will get stored without fail. Note that the above presented data is based on the BigchainDB only, as an example of private blockchain to implement an IIoT.

Fig 11 shows a simulation of a typical scenario for absolute moderation. It is considering 5 trucks A, B, C, D and E moving through the same route. Each is carrying an IoT device as specified earlier reports sensors values at certain points of time - a GPS location and disorientation using a motion sensor. The disorientation was associated to the corresponding truck for that specific journey (i.e. process or FTS) at that GPS coordinate. In the simulation, each truck starts with an hour lag i.e. truck B leaves around an hour after truck A and so on. The actual time gap is irrelevant but decides the order of data entered into the system. As truck B started later, the data for specific GPS coordinates will be recorded at a later time. It is assumed that no truck overtakes another one during their respective journeys.

This form of penalty calculation is *absolute* as the penalties are calculated at certain periods covering all data until then, in this instance, after the 5th truck E has reached destination at time t_f. The SQ Penalty keeps increasing (even if it is moderated increment) as there is no provisions for compensating faults in the described scenario and framework.

Truck A accumulated a penalty at location 2 along with B and C and the penalty for A was normalized to 1.67 instead of 5. However, truck B and D accumulated penalties at location 1 and had a 2.5 penalty to start with. This way at every location if there are multiple trucks reporting dis-orientation, then there is an appropriate amount of SQ penalty applied.

At time t_f when truck E has reached the destination, a decision is made regarding payment to all the trucks simply based on the available data. It is not necessary that a monetary penalty is applied on the transport peer as no real damage may have happened to the items, even if there was an unexpected dis-orientation reported by the IoT device. If an item is really damaged, then the corresponding monetary compensations



(a)

(b)

FIGURE 10. (a) Success rate of transactions in various configurations with requests distributed between 2 nodes and 1 node. (b) Success condition of transactions in various frequencies with undistributed requests.

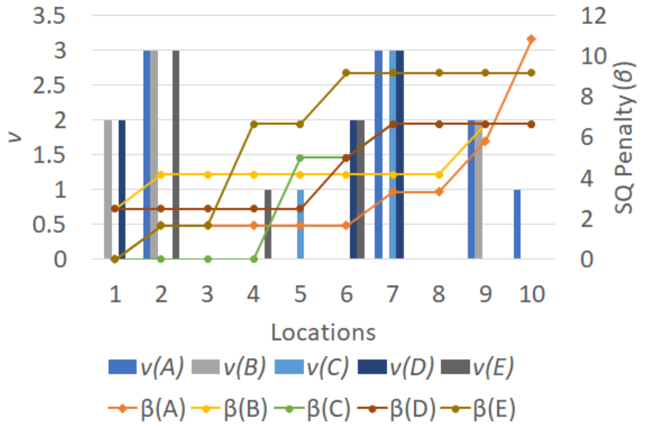


FIGURE 11. The υ (common FTS count) on Y1 axis and the change in SQ Penalty (β) on Y2 axis with time for a set of trucks A, B, C, D, E.

for the clients are calculated corresponding to the SQ i.e. the number of times the sensors reported a dis-orientation and the exact amount of disorientation.

VI. CHARACTERISTICS OF THE PROPOSED IIoT BLOCKCHAIN

This section discusses the advantages and critical challenges of the proposed Industrial IoT Framework for Blockchain.

A. ADVANTAGES

The main advantage of the system are as follows:

- The cause and effect of the events in an industrial system can be identified with the blockchain. The use of blockchain ensures that the moderation process can be automated. As blockchain is reliable in terms of data integrity, the involved parties can all agree to the data obtained from the sensors. The system can also allow for greater flexibility with actual financial penalties or payments in a justified manner, taking into account the performance of the whole system.
- The proposed solution can identify problems and help avoid them. The blockchain enables the system to identify the specific cause of the problems and possibly avoid them. In the described example (Fig. 11) locations 2 and 7 seems to be the most problematic, trucks can be advised in real time to avoid those locations or be careful based on the previous trucks data.
- The proposed system can work with re-configurable IoT devices. This is very important in terms of cost for the industries using IoT. The number of IoT devices can increase exponentially, cooresponsing to the number of parallel industrial processes being monitored and the actual number of sensors used. Being able to re-configure the IoT device means the same IoT device can operate in multiple processes. Also, using the same device makes it more reliable to relate to similar processes.
- Separating blocks from the assets and attributes at a conceptual level provide a better understanding of the related event that originate from the IoT system.

- Using a private blockchain allows for the system to run fast. In the case of a DDoS style attack, the transaction requests can be distributed properly and the service may be kept up to standard. The data can be written or manipulated only by the actual participating nodes of the blockchain using their public/private keys and thus preventing any manipulation of data by third parties even if they gain enough knowledge of the IoT device.
- It can allow for the IIoT system to record bursts of data in the blockchain when multiple events are expected to occur at around the same time. This can be handled by distributing the requests properly as shown in the previous section.

B. CRITICAL CHALLENGES

There are three main critical challenges identified by the proposed IIoT blockchain model:

i. The *blockchain gateways* between the IoT devices and blockchain. These gateways, if compromised can lead to fraudulent data entering the blockchain. This vulnerability is better understood in context of the asset and information discussed earlier. All blockchain can create and track assets e.g. furniture or coins in a reliable way. But for IIoT applications the focus is on the *attributes* and *information* of the *asset* which is constantly entered into the system. The blockchain has no way to defend itself from forged data originating in malicious IoT devices or gateways. The proposed framework allows each peer to validate the IoT data that is entered in the blockchain, but this does not prevent IoT devices from sending *fake* data. Even if the IoT device is a peer on the blockchain network, only that device is the source of the data and it can always manipulate the values from the sensor.

ii. In many IIoT applications the *start* and *end* of a process is easily identifiable. For each process with an IoT device and asset, the *start* and *end* play an important role in identifying the corresponding FTS. However, in some industries the boundaries of an asset's process may not be clearly defined.

iii. It is also important to decide the waiting time before an SQ penalty is finalized for a given process. In the case of systems that have discrete sets of events set apart in time, it is easy to determine the waiting time. As in the discussed example, the SQ may be finalized only at the end of the last truck of the day. But this waiting time may be difficult to determine in continuous systems.

C. FUTURE WORK

The proposed framework of estimating SQ can be enhanced in the following ways:

- Further work can optimize the penalty calculations by determining the best time when the SQ may be calculated with the data from the blockchain. The best time to calculate this would be determined using scheduling techniques. The application logic to determine the time would be embedded in the SBA of the blockchain.
- The proposed approach allows for determining the SQ in monitoring applications of IIoT. Eq 1-6 only consider sensors. Including actuators or other decision-making elements in the system will require additional features in the IoT system for blockchain. Such peripheral devices can manipulate the actual system being monitored. Thus, the service quality may be optimized accordingly by compensating for any degradation of performance of the IoT system.
- In cases where it is difficult to determine the *start* and *end* of a processes, advanced data mining techniques may be used to determining the common repeating sequence of the events for different asset/IoT devices which defines the start and end of the corresponding FTS.

VII. CONCLUSION

A framework to measure Service Quality for Industrial IoT and blockchain is discussed here. The system allows the IoT devices to send data to the blockchain through smart contracts or equivalent SBAs. Once the data is entered, the SBAs can then look up old data in soft-real time to identify data that are related to multiple IoT devices. This is done by associating digitalized representations of *assets* with their attributes, even if they are stored in separate blocks in a blockchain termed as the *Finite Transactions Series*. Through the industrial activities, the devices go through several processes – identical or similar, and the data generated by the devices with respect to their processes are *moderated* accordingly. This way an SQ Penalty can be accumulated over time for the participating peers in the IIoT-Blockchain system.

Multiple issues regarding the implementations of the IoT devices and how they need to be configured to be re-usable is also discussed as part of the proposed framework. The feasibility of private/permissioned blockchains compared to the public blockchains in context of the proposed framework is also analyzed. Private blockchains as a database can support IoT data management easily. Several critical challenges of combining IoT and blockchain is also identified and their potential solutions are discussed.

REFERENCES

[1] R. Y. Zhong, X. Xu, and L. Wang, "IoT-enabled smart factory visibility and traceability using laser-scanners," *Procedia Manuf.*, vol. 10, pp. 1–14, Jan. 2017.

[2] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, Jul. 2019, Art. no. 100081.

[3] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[4] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of Blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, Jan. 2018.

[5] S. Kamble, S. Shweta, and B. Ritika, "The relationship between service quality dimensions and customer satisfaction in E-tailing environment: An empirical study on Online travel and E-mart retail model," *Adv. Manage.*, vol. 2, pp. 1–17, Mar. 2009.

[6] M. Salhaoui, A. Guerrero-González, M. Arioua, F. J. Ortiz, A. E. Oualkadi, and C. L. Torregrosa, "Smart industrial IoT monitoring and control system based on UAV and cloud computing applied to a concrete plant," *Sensors*, vol. 19, no. 15, p. 3316, Jul. 2019.

[7] J.-H. Huh and K. Seo, "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," *J. Supercomputing*, vol. 75, no. 6, pp. 3123–3139, Jun. 2019.

[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[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. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[10] S.-K. Kim and J.-H. Huh, "A study on the improvement of smart grid security performance and Blockchain smart grid perspective," *Energies*, vol. 11, no. 8, p. 1973, Jul. 2018.

[11] N. Álvarez-Díaz, J. Herrera-Joancomartí, and P. Caballero-Gil, "Smart contracts based on Blockchain for logistics management," in *Proc. 1st Int. Conf. Internet Things Mach. Learn.*, Liverpool, U.K., Oct. 2017, Art. no. 73.

[12] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment," *Logistics*, vol. 3, no. 1, p. 5, Jan. 2019.

[13] M. A. Khan and K. Salah, "IoT security: Review, Blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[14] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun.(GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436.

[15] M. Kumar, F. T. Kee, and A. T. Manshor, "Determining the relative importance of critical factors in delivering service quality of banks," *Manag. Service Qual., An Int. J.*, vol. 19, no. 2, pp. 211–228, Mar. 2009.

[16] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.

[17] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 1, pp. 81–93, 2014.

[18] L. Li, S. Li, and S. Zhao, "QoS-aware scheduling of services-oriented Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1497–1505, May 2014.

[19] C. K. M. Lee, S. Z. Zhang, and K. K. H. Ng, "Development of an industrial Internet of things suite for smart factory towards re-industrialization," *Adv. Manuf.*, vol. 5, no. 4, pp. 335–343, Dec. 2017.

[20] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using Blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.

[21] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized Blockchain for IoT," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2017, pp. 173–178.

[22] S.-K. Kim, U.-M. Kim, and J.-H. Huh, "A study on improvement of Blockchain application to overcome vulnerability of IoT multiplatform security," *Energies*, vol. 12, no. 3, p. 402, Jan. 2019.

[23] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[24] *IBM Food Trust*, 2019. [Online]. Available: https://www.ibm.com/downloads/cas/8QABQBDR

[25] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within Blockchain technology: A systematic mapping study," *Telematics Inform.*, vol. 35, no. 8, pp. 2337–2354, 2018.

[26] J. Abadi and M. Brunnermeier, "Blockchain economics," Nat. Bur. Econ. Res., Cambridge, MA, USA, Tech. Rep. w25407, 2018. [Online]. Available: https://www.nber.org/papers/w25407

[27] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[28] P. Wang, X. Liu, J. Chen, Y. Zhan, and Z. Jin, "QoS-aware service composition using Blockchain-based smart contracts," in *Proc. IEEE/ACM 40th Int. Conf. Softw. Eng., Companion (ICSE-Companion)*, Gothenburg, Sweden, May/Jun. 2018, pp. 296–297.

[29] P. Wang, J. Meng, J. Chen, T. Liu, Y. Zhan, W.-T. Tsai, and Z. Jin, "Smart contract-based negotiation for adaptive QoS-aware service composition," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1403–1420, Jun. 2019.

[30] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A Blockchain-based supply chain quality management framework," in *Proc. IEEE 14th Int. Conf. E-Business Eng. (ICEBE)*, Nov. 2017, pp. 172–176.

[31] A. Bahga and V. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, Oct. 2016.

[32] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *Proc. 21st Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2017, pp. 321–329.

[33] M. Dobrovnik, D. M. Herold, E. Fürst, and S. Kummer, "Blockchain for and in logistics: What to adopt and where to start," *Logistics*, vol. 2, no. 3, p. 18, Sep. 2018.

[34] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a Blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2017, pp. 50–58.

[35] R. Casado-Vara, A. González-Briones, J. Prieto, and J. M. Corchado, "Smart contract for monitoring and control of logistics activities: Pharmaceutical utilities case study," in *Proc. 13th Int. Conf. Soft Comput. Models Ind. Environ. Appl.* Cham, Switzerland: Springer, 2019, pp. 509–517.

[36] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, Blockchain and shared economy applications," *Procedia Comput. Sci.*, vol. 98, pp. 461–466, Sep. 2016.

[37] M. Petersen, N. Hackius, and B. von See, "Mapping the sea of opportunities: Blockchain in supply chain and logistics," *It-Inf. Technol.*, vol. 60, nos. 5–6, pp. 263–271, Oct. 2018.

[38] G. Perboli, M. Stefano, and R. Mariangela, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

[39] L. Nicoletti, A. Margheri, F. Lombardi, V. Sassone, and F. P. Schiavo, "Cross-cloud management of sensitive data via Blockchain: A payslipcalculation use case," in *Proc. CEUR Workshop*, vol. 2058, 2018, pp. 1–5.

[40] D. Mao, F. Wang, Z. Hao, and H. Li, "Credit evaluation system based on Blockchain for multiple stakeholders in the food supply chain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 2, p. 1627, 2018.

[41] C. Di Ciccio, "Blockchain-based traceability of inter-organisational business processes," in *Business Modeling and Software Design*. Cham, Switzerland: Springer, 2018, pp. 56–68.

[42] R. Bettín-Díaz, A. E. Rojas, and C. Mejía-Moncayo, "Methodological approach to the definition of a Blockchain system for the food industry supply chain traceability," in *Computational Science and Its Applications—ICCSA*. Cham, Switzerland: Springer, 2018, pp. 19–33.

[43] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.

[44] H. M. Kim and M. Laskowski, "Toward an ontology-driven Blockchain design for supply-chain provenance," *Intell. Syst. Accounting, Finance Manage.*, vol. 25, no. 1, pp. 18–27, Jan. 2018.

[45] R. Neisse, G. Steri, and I. Nai-Fovino, "A Blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Reggio Calabria, Italy, Aug. 2017, Art. no. 14.

[46] P. W. Abreu, M. Aparicio, and C. J. Costa, "Blockchain technology in the auditing environment," in *Proc. 13th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2018, pp. 1–6.

[47] J. Schmitz and G. Leoni, "Accounting and auditing at the time of Blockchain technology: A research agenda," *Austral. Accounting Rev.*, vol. 29, no. 2, pp. 331–342, Jun. 2019.

[48] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned Blockchains," in *Proc. 13th EuroSys Conf.*, Porto, Portugal, Apr. 2018, Art. no. 30.

[49] Y. Wang, S. W. Wallace, B. Shen, and T.-M. Choi, "Service supply chain management: A review of operational models," *Eur. J. Oper. Res.*, vol. 247, no. 3, pp. 685–698, Dec. 2015.

[50] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing Blockchains: Characteristics & applications," Jun. 2018, *arXiv:1806.03693*. [Online]. Available: https://arxiv.org/abs/1806.03693

[51] T. Feng, "A supply chain traceability system for food safety based on HACCP, Blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–6.

[52] (Oct. 7, 2019). *Lotion Java Script*. [Online]. Available: https://lotionjs.com/api.html

ANANDA MAITI received the Ph.D. degree from the University of Southern Queensland, Toowoomba, QLD, Australia, in 2016. He has been a Lecturer with the Discipline of ICT, University of Tasmania, since 2019. His current research interests include the Internet-of-Things, embedded systems, and blockchain for industries. He is also interested in augmented and virtual reality and their application in e-learning.

ALI RAZA received the B.Sc. degree (Hons.) in communications engineering from the Institute of Space Technology Islamabad, Pakistan, in 2014. He is currently pursuing the Ph.D. degree in information technology (IT) with the University of Tasmania, Australia. He was a Satellite Engineer for a few years with Pakistan's national space agency SUPARCO and a Developer Support Engineer with Facebook.

BYEONG HO KANG received the Ph.D. degree from the University of New South Wales, Sydney, in 1996. He was a Visiting Researcher with the Advanced Research Laboratory, Hitachi, Japan. In addition, he has played a role in the foundation of several spinoff companies. He is currently a Professor with the School of Engineering and ICT, University of Tasmania, Australia, where he is also the Head of the Discipline of ICT, CoSE. He leads the Smart Services and Systems Research Group of postdoctoral scientists, which has carried out fundamental and applied research in expert systems, Web services, SNS analysis, and smart industry areas. He has been involved in the development of several commercial and Internet-based applications, including AI products, expert system development tools, intelligent help desk systems, and Web-based information monitoring and classification systems. His current research interests include basic knowledge acquisition methods and applied research in Internet systems and medical expert systems. He has served as a steering committee member and the chair in many international organizations and conferences.

LACHLAN HARDY is currently pursuing the Ph.D. degree with the University of Tasmania. His Ph.D. topic is in the fields of information systems, human-computer interaction, and education with a specific focus on providing a systematic framework for self-managed technical support to primary school teachers in new technology curriculums. His current research interests include applications of technology in society, how technology changes societies and societies change technology, and improving learning through the use of technology.