Blockchain Inspired RFID based Information Architecture for Food Supply Chain

Saikat Mondal, Kanishka Wijewardena, Saranraj Karuppuswami, *Student Member, IEEE*, Nitya Kriti, Deepak Kumar and Premjeet Chahal, *Member, IEEE*

***Abstract*—In this paper, we propose a blockchain inspired internet-of-things architecture for creating a transparent food supply chain. The architecture uses a proof-of-object based authentication protocol, which is analogous to the cryptocurrency's proof-of-work protocol. The complete architecture was realized by integrating a RFID based sensor at the physical layer and blockchain at the cyber layer. The RFID provides a unique identity of the product and the sensor data, which helps in real time quality monitoring. For this purpose, a small feature size 900 MHz RFID coupled sensor was fabricated and demonstrated for real time sensor data acquisition. The blockchain architecture aids in creating a tamper-proof digital database of the food packages at each instance. A detailed security analysis was performed to investigate the vulnerability of the proposed architecture under different types of cyber attacks.**

***Index Terms*—Blockchain, IoT, RFID, food supply chain.**

I. Introduction

INTERNET of Things (IoT) has huge potential to impact global food supply chain (FSC) by increasing productivity in terms of supply chain performance. Among many challenges, agri-food safety and its impact on the environment due to food wastage are of major concerns. The United States Center for Diseases Control (CDC) estimates that 48 million people get sick from foodborne illness, 128,000 are hospitalized, and 3,000 die each year in the U.S. alone. Apart from illness, economically and criminally motivated food adulteration is also a growing concern due to globalization and wide growing supply chain networks [1]. Real-time monitoring of the food quality and visibility of that quality index would prevent outbreak of food-borne illnesses, economically motivated adulteration, contamination, food wastage due to misconception of the labeled expiry dates, and losses due to spoilage, which have broad impacts on the food security [2]. In order to improve safety and prevent wastage, modern IoT based technologies are required to monitor the food quality and increase the visibility level of the monitored data. There are a number of IoT based tracking and tracing infrastructures such as Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID), and QR codes [3] which are primarily targeted for automatic package level tracking. However, the role of these technologies is limited in identifying the food package and does not provide any information pertaining to the state of the food quality. This limitation prevents quick removal of a defective product from reaching higher levels of the FSC. For example, when a quality control lapse is identified along the FSC, the company is forced to recall all the food products within a certain time frame leading to a huge economic loss, which can be mitigated with the availability of individual food package quality information resulting in targeted recalls [4].

In literature, a number of sensing techniques compatible with existing tracking and tracing infrastructure are proposed for monitoring food products. These sensors can be invasive or non-invasive in monitoring the physical or chemical properties of food such as pH [5], conductivity [6], and permittivity [7] or the packaging environment such as temperature [8], humidity [9], moisture [10] or aroma [11]. In general, these sensors are aimed to prevent defective products from reaching the consumers. Furthermore, these sensors help in identifying key bottlenecks in the FSC to improve the overall efficiency. Currently, little work has been done in integrating these sensors to the tracking and tracing infrastructures. Moreover, the collected tracking as well as sensing data is more centralized and selectively used by specific entities of the FSC. The consumers have to trust the quality of the product based on the printed expiry date without any additional knowledge of its current quality. To move beyond a "traceability-centric" or "income-centric" to a "value-centric" supply chain, a more decentralized approach is needed in terms of data sharing. However, a trade off exists between providing sufficient information to the consumer about an individual product and at the same time safe guarding the operational privacy of the FSC.

Blockchain has emerged as a decentralized public consensus system that maintains and records transactions of events that are immutable and cannot be falsified [12]. Blockchain technology has attracted attention beyond cryptocurrency due to its ability to provide transparent, secure, and trustworthy data in both private and public domains [13]. The technology is based on a distributed ledger, which is not owned or controlled by a single entity. Data in the public ledger is visible publicly and any authorized entities can submit a transaction, which is added to the blockchain upon validation. The advantage of blockchain technology can be applied in FSC to improve the digital data integrity which is obtained as the product passes through different entities of the FSC.

The complete food product visibility across different entities of the supply chain can become a reality with the integration of sensor based RFID technology and blockchain based

S. Mondal, K. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar and P. Chahal are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI, 48823 USA e-mail: s.mondal1043@gmail.com, chahal@egr.msu.edu.

Manuscript received

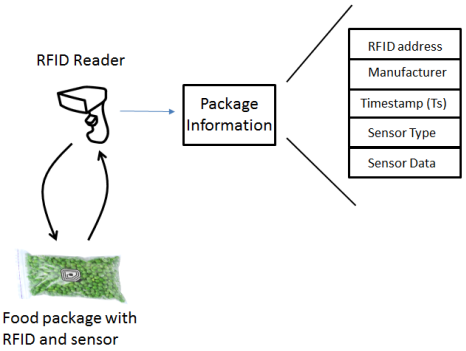


Fig. 1: An example of information extracted from a food package using RFID technology integrated with sensors.

data management systems [14]. The key benefits of applying blockchain technology in FSC are: (i) real time tracking and sensing of food products throughout the FSC, and allowing identification of key bottlenecks; ii) discouraging adulteration of food products, and identifying weak links on occurance; iii) determining the shelf life of food products leading to reduced waste; iv) providing end to end information to the consumer; and v) allowing specific and targeted recalls. A test prototype of the RFID integrated sensor is demonstrated experimentally in this work. The RFID integrated sensor can be attached to a food package to extract information regarding the package along FSC as shown in Fig. 1.

II. Related Work

Among many IoT devices, RFID was proposed earlier due to its low cost and small size to ensure food safety by increasing the traceability of the food products in the FSC [15], [16]. The importance of RFID based temperature sensor tags for cold FSC has been described in [15]. The sensor enabled tags can record the temperature of individual food packages and track the real time shelf life in case of any deviations in environmental conditions during storage or transportation. According to [15], if food products with reduced shelf lives arrive unexpectedly at a retailer, priority should be given to sell those items to reduce the amount of food wastage. In [16], a detailed review has been performed to discuss the potential of RFID technology in logistic development of different sectors for the FSC. However, the visibility of the food products is limited by the amount of information shared by each supply chain stage to its next stage. Implementing blockchain technology would provide a non-modifiable digital trace of the food products during their lifetime and thus making the FSC visible to everyone.

Blockchain has been proposed earlier to develop the data management architecture for IoT devices [17], [18]. A systematic survey was performed in [18] to find a computationally less expensive proof-of-work (PoW) for computationally lightweight IoT devices such as low cost RFID tags. However, compromising the PoW would increase the vulnerability of the network architecture to malicious attacks. To address this problem, a smart transaction based access control system was proposed for IoT device management addressing the issue of scalability [17]. In the proposed scheme [17], the IoT devices do not interact with the blockchain network directly but through a management hub and thus the data storage and computation tasks are leveraged to those management hubs.

In [19], [20], blockchain technology was proposed to improve the traceability of a food product along the supply chain using different IoT based technology such as Wireless Sensor Network (WSN), GPS and RFID. However, addition of a single block in existing blockchain has to go through extensive computation consuming lot of electricity. For example, only Bitcoin's annual energy consumption was comparable to Ireleand's electricity consumption in 2014 [21]. Hence, implementation of existing blockchain technology to FSC would increase the operational cost and hence the end food product cost. The work in [17], [19], [20] do not discuss how on maintaining the cost of food products while implementing the blockchain for FSC.

III. Modified Blockchain

The conventional blockchain framework has been modified to suit the FSC perspective. First the conventional blockchain is described briefly and then the modified blockchain is discussed.

A. Conventional Blockchain

A *blockchain* is a collection of blocks, where each block contains a hash of the previous block thereby creating a chain of blocks. The first block in the blockchain is called the *genesis* block from which the blockchain begins growing upto the most recent block. A single block contains a set of transactions between different participants in the network. All valid transactions are visible in the form of connected blocks creating a public ledger. The transactions are mined into a block by *miners* before including it into blockchain. Individual blocks must contain a PoW indicating consensus among the nodes about the validity of the transactions.

The concept behind *blockchain* is a mutual trust based on cryptographic PoW. A cryptographic proof of computational PoW was proposed in [22] using pricing functions for controlled access over a shared resource. This PoW idea later shaped the concept of mutual trust among several unknown participants sharing the resources. PoW based micro-payment architecture for peer to peer file sharing was proposed in [23]. The proposed model with PoW was augmented with digital signatures and a ledger in order to keep all the historical record incorruptible by malicious actors in the network. Later, Nakamoto introduced a similar PoW based secured value token, which became popular as Bitcoin's decentralized public ledger-the blockchain [24]. The blockchain has many potential advantages, which made Bitcoin a successful electronic cash or *cryptocurrency*. The primary advantages can be listed as 1) decentralized control and consensus, 2) transaction transparency, 3) distributed information, and 4) tamper-proof as mentioned in [25].

A standard blockchain network requires a consensus algorithm among the participating nodes to convert a new information into a block and include it in the existing chain.

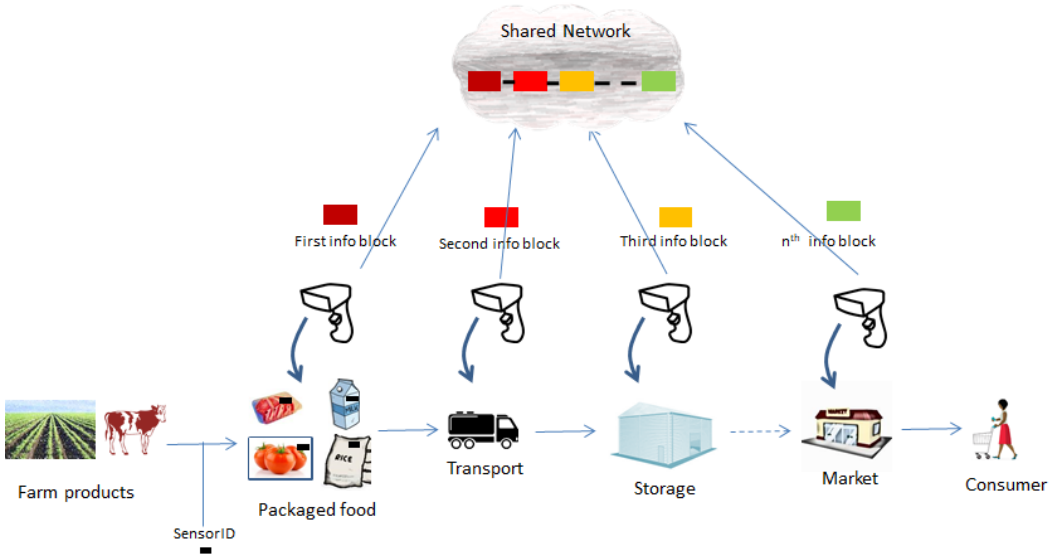


Fig. 2: Proposed architecture of blockchain implementation for FSC.

There are different forms of consensus algorithms apart from PoW such as proof-of-stake (PoS), delegated proof-of-stake (dPoS), proof of storage among others [26], [27]. PoS uses consensus based on the share of stakeholders rather than consensus of all nodes as in PoW.

B. Modified Blockchain

Implementation of the blockchain would provide an advantage to meet the transparency criteria of a FSC. However, implementing the conventional blockchain for the FSC would be disadvantageous from cost perspective. Mining is a computationally extensive procedure and the amount of computation performed for the creation of a block denotes the PoW by a miner and a miner is rewarded based on its PoW. If mining is introduced in the supply chain, the miner would be rewarded by the selling price from the product and it would increase the price of the product, which is not desired for a sustainable FSC.

Furthermore, the cyber data network should be immune to malicious attacks restricting unwanted transaction additions to the blockchain. There exists a fundamental difference between cryptocurrency and supply chain. In supply chain, there is presence of a physical object which does not exist in cryptocurrency. Hence, if someone with a physical object can cryptographically prove it, then it will negate the purpose of miners. A *proof-of-object* (PoO) based new consensus algorithm is proposed in this modified blockchain architecture.

1) Proof-of-Object: In cryptocurrency, PoW means enough computation has been performed to bolster the validity of a block in presence of other competing blocks. Similar to PoW, PoO means any node that claims the possession of the physical object, has to cryptographically prove it. Once a node claims for PoO, other participating nodes verify the authenticity of the claim. Likewise in blockchain, the new block is added once consensus is reached about the authenticity of the block.

2) Dual Addressing: In this architecture, dual addressing is proposed 1) cyber address: a public address in the blockchain memory, which can be viewed by any nodes in the network. 2) RFID address: a physical address, which is specific to a food package and is not shared publicly. Additionally, the physical and cyber addresses should be linked to each other in such a way that the cyber address can be derived from the physical address but the inverse operation is computationally expensive.

IV. Proposed Architecture

First, a few nomenclatures are provided, which will be followed throughout the paper. The sensor along with the RFID is termed together as a 'sensorID'. The sensorID can be a passive [28] or an active type [29], a single sensor [28] or multiple sensor type [30]. The data collecting and processing node, that scans a sensorID is termed as a 'terminal'. The common network shared by all the terminals is termed as 'shared network'. The scan of a sensorID by a terminal and enlisting the data is termed as a 'transaction'. Once a transaction is validated based on the consensus of participating terminals, the transaction is converted into a 'block' and included in the blockchain. Apart from terminals, there exists another type of node, a 'manager', that is responsible for policy making and processing requests based on consensus with other nodes. Finally, there exists a third type of node, called 'agent', that requests information about a sensorID from the blockchain by providing a proper cyber address. 'Address collision' is referred to the existence of a minimum of two identical cyber or physical addresses.

A typical food based supply chain is shown in Fig. 2. Each packaged food product with an embedded sensorID travels through multiple stages of transactions at different terminals starting from packaging through transportation, storage and finally to a consumer for purchase. A data block is created containing the information about the package at each valid transaction. Once the transaction is verified, the transaction

TABLE I: Important parameters of the proposed blockchain architecture.

Parameters	Description
G	General type terminals
M	Manufacturing type terminals
$h()$	hash operator
$h_n()$	n times hash operations
x_k	Physical RFID address
y_k	Cyber cryptographic address
MG	Set of all M and G type nodes except the current scanning node
T_j	Transaction information
D_j	Data set within the transaction information
H_j	Hash of the combination of x_k and D_j within T_j
z_{kq}	Derived hash address from locally stored x_{kq} during transaction verification
A_{jm}	Acknowledgment sent upon discovery of a sensorID
CL_{T_j}	Confidence level of each block after consensus
$R_{A_{jm}}$	Penalty term for computing CL_{T_j}

of the sensorID is converted into a block of information and appended to its pre-existing data blocks thus forming a chain of information blocks and thus a blockchain.

A. Address Allocation

The terminals performing transactions can be categorized mainly into two groups: 1) Manufacturing terminal, M and 2) General terminal, G. The M type terminals register a new sensorID in the network and provide a unique cyber address to it. For a k^{th} sensorID with RFID address of x_k, the cyber address y_k is derived as in (1), where h_n denotes the n times hash function $h()$ operation. The cyber address in the public network is shown as y_k. n is the smallest natural number to avoid cyber address collision. The M type terminals start with $(n = 1)$ and in case of address collision, n is incremented until a unique y_k is obtained. On the other hand, G type terminals are the retailer, seller, logistic or storage terminals in the FSC and scans the previously registered sensorIDs.

$$y_k = h_n(x_k),\ \left\{\min\{n \in \mathbb{N}\} \mid y_k \notin \{y_1, y_2, ..., y_{k-1}\}\right\} \quad (1)$$

B. Transaction information structure

Once a sensorID is registered, it is scanned by G type terminals in subsequent stages of the FSC. When the k^{th} sensorID is scanned by an i^{th} terminal G_i, a transaction information is broadcasted to all other participating terminals of the set MG in the network as denoted in (2). In (2), M_1 and M_2 represent the total number of G type and M type terminals respectively in the FSC. The transaction T_j has a specific information structure as shown in (3).

$$MG = \left[\sum_{m=1}^{m=M_1} G_m \cup \sum_{m=1}^{m=M_2} M_m\right] - \{G_i\} \quad (2)$$

$$T_j = [A_k \cup D_j \cup H_j], \{\forall j \in \mathbb{N}\} \quad (3)$$

where $(A_k = [y_k, n])$ and D_j represents the data accumulated by the terminal G_i. A_k is the address header with the cyber address and its specific n. H_j denotes the hashed value from D_j and RFID address denoted as x_k. The data structure D_j will be discussed later.

$$H_j = h(x_k \oplus D_j), \text{where } \oplus \text{ is bitwise XOR} \quad (4)$$

C. Transaction verification

Once T_j is broadcasted, each terminal of the set MG evaluates T_j. Now, each terminal verifies if a transaction on the particular sensorID was performed earlier. For this purpose, all the terminals maintain an individual local memory that contains RFID addresses of all the previously scanned sensorIDs.

$$z_{kq} = h_n(x_{kq}), \{\forall q \in [1, 2, ..., Q_m]\} \quad (5)$$

When a terminal MG_m, (where $MG_m \in MG$) evaluates T_j, cyber address z_{kq} is derived using previously stored Q_m sensorIDs and n of T_j as in (5). In case of a match of y_k with z_{kq}, it denotes that the sensorID was scanned before at the terminal MG_m. Then D_j and newly found x_{kq} are hashed together as in (4) and compared with data hash H_j for final confirmation. Upon final confirmation, the terminal M_{Tm} concludes the discovery of the broadcasted sensorID. Upon discovery, MG_m sends back its acknowledgment A_{jm} to the network, which denotes the acknowledgment of j^{th} transaction T_j and A_{jm} consists of the IP address of MG_m. The acknowledgment stage will be helpful to keep the product information upto date and prevent introduction of any products in the FSC other than the M type terminals. Naturally, counterfeiting of food products will be discouraged at the weak links of FSC. Additionally, the acknowledgment scheme is also computationally lightweight avoiding the need for high computation mining.

D. Consensus

After a fixed time, when all the acknowledged transactions are received at the network, the network validates the transaction into a block by authenticating all the A_{jm} and includes the block information in the blockchain. The manager within the network can solely perform the authentications. However, to take a more decentralized approach, instead of the manager performing the authentication, a node is selected randomly from the set $\left\{MG \cap \left\{\sum_{r=1}^{r=R} MG_{Ar}\right\}\right\}$ and asked to verify each A_{jm} independently, where MG_{Ar} represents the terminals that sent the acknowledgments.

Suppose in the blockchain, the k^{th} sensorID already contains n blocks. Now, the transaction T_j of sensorID with cyber address y_k should receive n acknowledgments as it has gone through n stages of valid transactions earlier. However, there can be multiple reasons of receiving p acknowledgments (where $p < n$) such as: 1) Loss of local memory at a terminal, 2) Temporary connection lost from the shared network, etc. Hence, a new parameter named confidence level is introduced to authenticate a transaction in case of lower number of acknowledgments is received from expected.

When a random node is evaluating one A_{jm} acknowledgment, it will hash the received IP address of MG_{Ar}

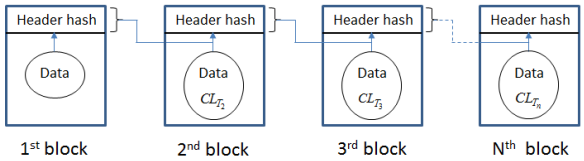


Fig. 3: Information arrangement along the blockchain.

and match it with previously hashed IP address information available in the blockchain. After computation, the node would return $R_{A_{jm}}$ as given in (6). The confidence level (CL_{T_j}) is computed based on all the $R_{A_{jm}}$. Ideally, (CL_{T_j}) should be 0 in case of perfectly operating condition. However, CL_{T_j} can be different from 0 for reasons described earlier. The maximum allowable value of CL_{T_j} is decided by managers in the network. If the CL_{T_j} is above a certain threshold value CL_{th}, the transaction will be denied.

$$R_{A_{jm}} = \begin{cases} 0, & \text{for a match} \\ n, & \text{for not a match} \end{cases} \tag{6}$$

$$CL_{T_j} = |n - p| + \sum_{m=1}^{p} R_{A_{jm}} \tag{7}$$

In (7), $R_{A_{jm}}$ signifies the penalty term of CL_{T_j}. If a malicious terminal spams with negative acknowledgment or there is a network error, it increases CL_{T_j}, which increases with more number of blocks. To avoid fake acknowledgments by malicious terminals, the network can repeat the A_{jm} evaluation process multiple times (N_{opt}) with broader node participation. Similar to CL_{th}, (N_{opt}) is also decided by the manager. The new CL_{T_j} is updated with the average of present and previously computed CL_{T_j}. Different kind of attacks are considered and will be discussed in the next section.

E. Block formation

Once consensus is reached with desired confidence level about a transaction, the transaction is validated into a block. A block B is defined as $\{HD_j \cup D_j \cup CL_{T_j}\}$, where HD_j is the header hash value, D_j is the transaction data information, and CL_{T_j} is the block level confidence value. HD_j is generated using a hash function h as shown below

$$HD_j = \begin{cases} h\big(HD_{j-1} \cup D_j \cup CL_{T_j}\big) & \text{for old sensorID} \\ h\big(HD_{j-1} \cup D_j\big) & \text{for new sensorID} \end{cases} \tag{8}$$

Implementing the headers of each block using hash function enables linking the blocks with irreversible hash value along the blockchain. When a M type terminal initially registers a sensorID, it creates the new block from old hash HD_{j-1} and the scan data set D_j. Else, HD_j is created for already registered sensorID from the previous block hash value HD_{j-1}, D_j and CL_{T_j}. Transaction verification and consensus stages are not performed during the registration of a new sensorID. The hash formation of the blocks along the blockchain is shown in Fig. 3.

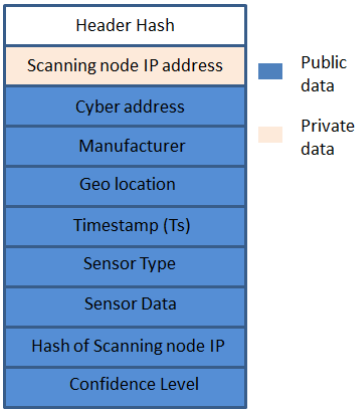


Fig. 4: Data structure within a single block.

F. Single Block Data Structure

The data structure D_j defined earlier within a single block consists of multiple information. D_j consists a set of public data PD_j and encrypted private data ED_j. Under PD_j, there is information regarding the 1) Cyber address of the sensorID, 2) Manufacturer of the sensorID, 3) Geo location of the place of the scan, 4) Timestamp of the scan, 5) Sensor type, 6) Sensor data, and 7) hash of the scanning node IP address. Under ED_j, there is encrypted information of the IP address of the scanning terminal, which initiated T_j. Anyone with a valid key can decrypt the scanning node IP address. The data structure D_j with the header hash HD_j and block confidence level is shown in Fig. 4.

G. Data Storage

The blockchain data is stored individually in all nodes and once a new block is added, it is updated in all the nodes. Apart from the commonly shared blockchain data, each terminal has its own private data, which consists of the physical RFID address x_k. When any G or M type terminal with existing local RFID memory storage scans a new sensorID or registers a new sensorID with physical address x_k, the local memory storage is updated as shown in (9), where Mem_{old} denotes the local memory storage before updating x_k and Mem_{new} denotes the local memory storage after updating x_k at the scanning terminal. When a transaction request T_j is received by any terminal, it hashes all the locally stored physical addresses to find a match of the requested cyber address. However, the agent and manager nodes do not locally store any x_k of a sensorID separately.

$$Mem_{new} = Mem_{old} \cup \{x_k\} \tag{9}$$

H. Computation Time

The computation time for a single block validation (t_B) in (10) depends on the local terminal computation time as well as the network latency time. In (10), t_{T_j} represents the scanning and transaction information formation time, which solely depends upon the local terminal computation time. L_t represents the network latency time and the information

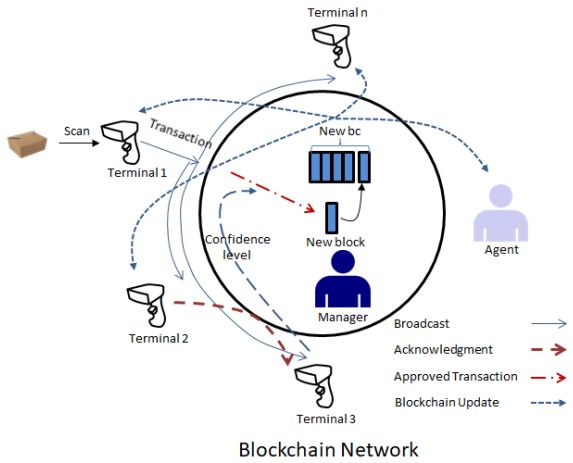


Fig. 5: Interaction among different entities in a blockchain network.

sharing is performed three times through : 1) Transaction broadcast, 2) acknowledgment sent, and 3) acknowledgment verification. The time $t_{A_{jm}}$ represents the computation time by a terminal to verify T_j and process A_{jm}. The time $t_{CL_{T_j}}$ represents the time required for a single consensus stage by the network, and N_{count} represents the number of consensus stages.

$$t_B = t_{T_j} + 3 * L_t + max\{t_{A_{jm}}\} + N_{count} * t_{CL_{T_j}} \quad (10)$$

I. Agent Request

An agent can obtain earlier transaction information from blockchain by using the cyber address. A typical example of an agent is a consumer, who wants to know more details about a food product prior to purchase. In that case, the agent can scan the sensorID and obtain the product details such as physical conditions of the package at different locations and time from the blockchain. A detailed report can be generated based on the single or multiple sensor values obtained at different time and corresponding locations. The sensor values can be further used to forecast on the lifetime of packaged products. Additionally, if any node in the supply chain fails to maintain the operating conditions, it can be readily identified.

A simple illustration of the architecture is shown in Fig. 5. When a food package is scanned at terminal 1, the transaction is broadcasted to every other terminals in the network. Upon discovery, terminal 2 sends back its acknowledgment, which is authenticated randomly by terminal 3. Once authentication is done, the transaction is accepted with certain confidence level. Once the transaction is validated into a block, it is added to the blockchain and broadcasted to all nodes in the network. The complete flowchart of the proposed algorithm is shown in Fig. 6.

V. SensorID and Reader Design

In literature, different mechanisms were proposed to integrate RFID technology with sensors for differentiating same

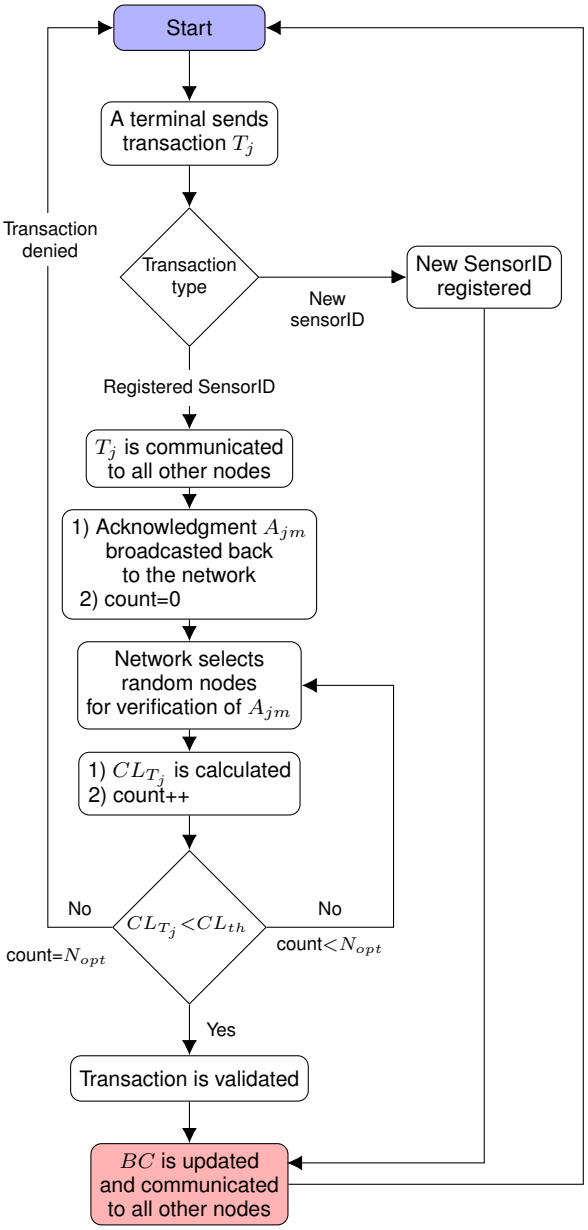


Fig. 6: Flowchart of the proposed architecture.

type sensors from each other [28], [30]. In this work, an active wireless sensorID was designed using a PIC12LF1822 microcontroller, a RF switch, a thermistor based temperature sensor and an antenna. Temperature is a key parameter, which should be maintained for cold FSC. The microcontroller generates a 8-bit ID and an internal ADC converts the analog temperature voltage to a 10-bit digital sequence. The digital data stream is fed into a RF switch to modulate the antenna according to the digital bits. The designed antenna resonates at 900 MHz within the commercial RFID frequency band (900 MHz to 930 MHz). The complete tag design is shown in Fig. 7.

Additionally, if multiple sensors are coupled with the microcontroller, the digital bit sequences from the sensor can be cascaded after the ID and the complete data bits can be transmitted serially realizing multiple sensor based sensorID.

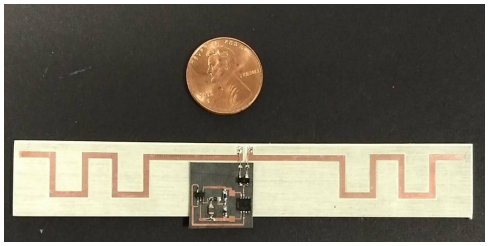


Fig. 7: The sensorID design with an antenna and digital circuit.

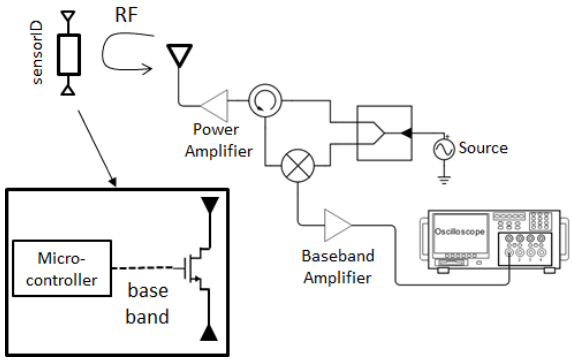


Fig. 8: The reader and tag circuit to obtain the sensor and ID data wirelessly from the sensorID.

A simple reader is designed to interrogate the sensorID and obtain the sensor data along with the ID. The demonstrated tag in this paper is a UHF type as it works at 900 MHz RF carrier frequency. However, the tag in its current form cannot be read by commercially available RFID readers. As demonstrated in [30], a demodulator is required at the tag end for decoding the reader's query signal. With the modifications at hardware level and EPC Gen-2 protocol embedded in the microcontroller, it is possible to use the commercial reader to read the proposed UHF RFID tag [30]. In this work, a simple program is embedded in the microcontroller to show the proof of concept of the sensor integrated RFID tag. The designed reader works in similar RF front end principle of commercial RFID reader.

The circuit detail for the tag is shown in Fig. 8 inset. The baseband signal is generated by the microcontroller at data rate of 1.8 kbps, which is used to modulate the high frequency RF MOSFET switch BF1105R. A single bit period of the base band signal takes around two clock cycles at 32 kHz. Based on the bit sequence, the switch changes the impedance of the tag antenna, which perturbs the RF field produced by the reader antenna. The reader interprets the digital bit sequence from the small perturbation in RF field. The RF front end of the designed reader is shown in Fig. 8. A single frequency 900 MHz signal is power amplified and transmitted using a high gain antenna. The return signal is isolated using a circulator and the signal is mixed with the reference source signal. After mixing, the baseband signal is amplified and the sensorID modulated signal is obtained. A local CPU is used to obtain the data which is further processed to create a transaction file as mentioned in (3) to be added in the blockchain.

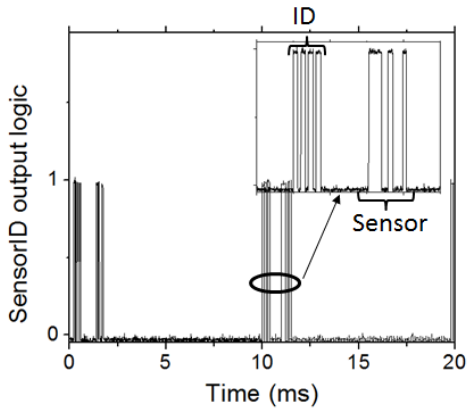


Fig. 9: Output signal generated by the microcontroller.

VI. Experimental Results

After design and fabrication of the sensorID, measurements were performed. The digital sequence generated by the microcontroller is shown in Fig. 9. The internal clock of the microcontroller is set at 32 KHz for low power consumption. Overall, the complete sensorID including the microcontroller consumes 342 μA from a 1.8 V DC source. The tag is powered by a small form factor commercially available CR2032 Lithium ion battery, operating at 3 V with typical 235 mAh capacity. As shown in Fig. 9, first the ID is transmitted followed by the sensor data. The sensor data stream and the ID are separated by 1 ms. Under continuous use, the proposed RFID tag can last for 230 hours of operation. The lifetime of the tag can be significantly increased by increasing the idle time in between two consecutive sensor and ID data sequence group. The idle time is 8 ms as shown in Fig. 9. The microcontroller is mounted on Curiosity Development Board to be programmed in C language using MPLAB- X IDE and MPLAB-XC8 C compiler from microchip technologies.

The block chain structure is developed using an open source integrated development environment (IDE) Spyder. Python 3.7 is used for programming the different blocks using the IDE. The IP address of the nodes are encrypted using the Serpent cipher algorithm as described in [30]. The hashlib library in python is imported into the program for generating hashes from plain text input using SHA-256 (secure hash algorithm) cryptographic hash function for hashing the source IP address, the RFID address, and the header hash [31]. The computation time of a single transaction depends upon the hash computation, the network latency, and parallelization of several computation stages. The computation time is compared in Fig. 11 for brute force based cyber address lookup and PoO algorithm, both based on the time obtained from single hash computation time from Fig. 10. The brute force computation time increases exponentially with number of ID bits of the sensorID. Hence, the cost for random guessing of a specific RFID address from cyber address would be very high. All the computation was performed using Intel(R) Core(TM) i5-7300U CPU with a processor speed of 2.60GHz and 8 GB RAM. A sample public ledger is shown in Table II for multiple

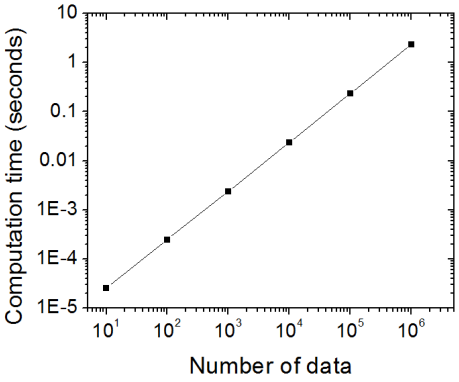


Fig. 10: Computation time of the hash.

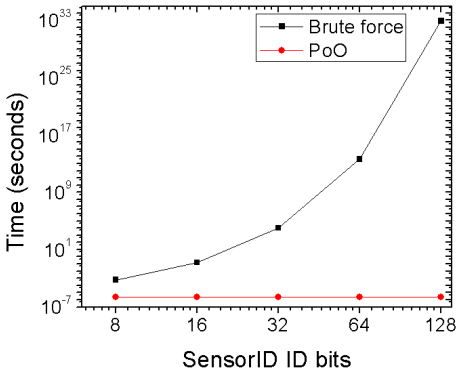


Fig. 11: Computation time comparison for brute force finding and PoO.

sensorIDs with multiple transactions.

VII. Security Analysis

Security is an important feature, which needs to be addressed for the proposed architecture. The primary type of vulnerabilities are: 1) Tampering, 2) Spamming, 3) Privacy stealing, 4) Physical layer attack, and 5) Preferential treatment. Tampering means unauthorized addition of information blocks in the blockchain. The blockchain data structure is integrated cryptographically and a 51% attack is required for tampering of existing blockchain data. Additionally, terminal to terminal communication data is cryptographically protected and hence the transaction verification stage is tamper-proof. However, tampering of acknowledged transactions is possible, which can be prevented using secure communication channel implementation among the terminals. All traffic to and from the terminals can be encrypted over SSL/TLS protocol, as proposed in [32] for confidential IoT based application services.

Tampering in terms of undesired block validation can occur in the following attack scenario as shown in Fig. 12. As the cyber address is publicly available, a malicious terminal can broadcast a fake transaction. Now, as the transaction does not contain the sensorID's physical address, the real terminals will not respond. However, there can be multiple malicious nodes that can respond back with an acknowledgment. Once all the acknowledgments are received, the network randomly selects

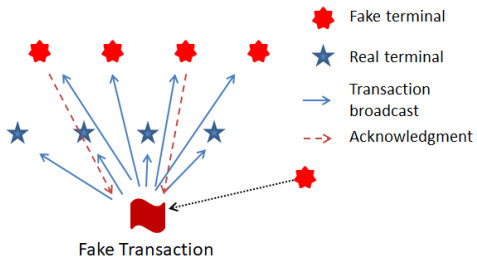


Fig. 12: A scenario of existing blockchain data tampering.

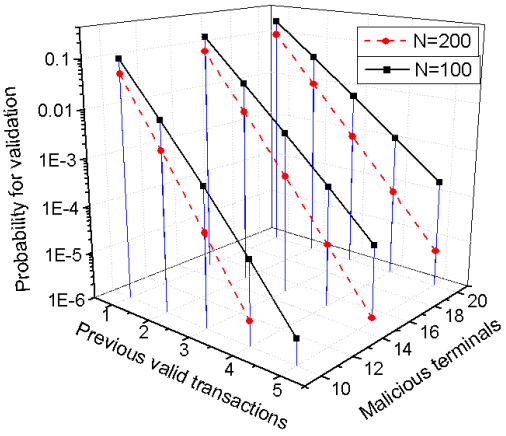


Fig. 13: Probability of block validation for different numbers of malicious terminals and total N terminals.

other nodes for verification of those acknowledgments. Now if malicious nodes are selected randomly at the acknowledgment verification stage, then the fake transaction would be validated into a block.

The probability of block validation of a fake transaction is shown in Fig. 13 for different scenarios. With higher number of prior valid blocks, the probability of a fake block inclusion drops down exponentially for $CL_{th} = n$. Additionally, the faking also drops with reduction in percentage of malicious terminals present in the network, where N is the total number of terminals. In case of the described tampering attack, the real nodes can signal an alert signal, upon which the manager in the network would set a high value for N_{opt} and the CL is compared after all the consensus stages. The network would evaluate the acknowledgments multiple times and thus the probability of fake validation would be reduced.

Multiple consensus stages can be used to prevent targeted spam during the CL_{T_j} computation. In case of targeted spam attack, a spam occurs during a valid transaction. This kind of attack happens when a malicious terminal is randomly selected during the acknowledgment verification stage. In this case, the malicious terminal spams with a penalty signal and CL_{T_j} becomes higher than the desired value. This type of spam attack is minimal provided the penetration of malicious terminal is low ($<50\%$). For a specific sensorID with n=6 and p=6 as in (7), let's consider a case where a single spam happens at the first stage of consensus stage. Then the CL_{T_j} will converge to desired $(n - p = 0)$ as shown in Fig.

TABLE II: An example of the ledger showing transactions of a sensorID.

Header hash	Encrypted terminal IP	Cyber address	Company	Location	Time stamp	Sensor type	Sensor value	Hash of terminal IP	CL
c04443ece3ae6 a386d90be4d71 73f5dd1fc4d8c ccedcf554daa2 d805be21bf84	e714ab97 440731b6 9ba8fe49 6feb7702	237320d509717 dc3f0d6bdcd5e 8dc8f88f8fd94 b06c728c1aaf9 4118ed34af38	ABC	40.8344, -74.1377	2018-11-27 12:17:24.943	TEMP	11110001	a05017f9346b0 d51a431136c7a 3539c8f0c3755 ea55724ef7433 3b9994a47dc9	0
d177390526a33 45b6071695280 c1c78320e9f85 a3d69810297b2 6ac57692e21b	aeecc645 a866a0db 089d2493 104e8b6e	237320d509717 dc3f0d6bdcd5e 8dc8f88f8fd94 b06c728c1aaf9 4118ed34af38	ABC	53.4926, -2.2991	2018-12-01 12:58:57.137	TEMP	11111001	50dc2ffb98845 a0a3d8690e6f6 cfb5a0963f3f1 8df72d5a6a04d e08f75b4d5f9	0
44ca24797dc95 ea2287c018d35 29d9fddd08bd5 bbfc716b0efba dd226d0063b4	f56d1fb7 32184a90 39f16101 30c8ceba	237320d509717 dc3f0d6bdcd5e 8dc8f88f8fd94 b06c728c1aaf9 4118ed34af38	ABC	40.8344, -74.1377	2018-12-03 13:22:59.622	TEMP	11110001	d5631004c1f00 9ff14cf885159 4cb73239d47d3 bcd8fbdc016ae 36c7d6177048	0

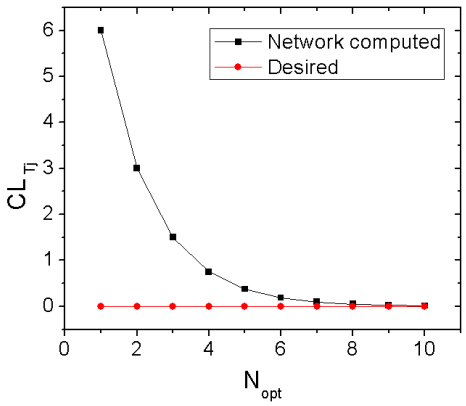


Fig. 14: CL_{T_j} dependance on different numbers of consensus stages.

14 for high value of N_{opt}. Apart from increasing the value of N_{opt}, if multiple terminals are invited to verify a single acknowledgment, that will also minimize the effect of spam attacks.

Privacy stealing is another problem in recent IoT architecture, where a malicious terminal steals information and impersonates a real terminal. In [33], different level of privacy information is categorized and respective security goals are provided. If a malicious node can infiltrate the local storage of a terminal, then it will have access to the previously stored physical addresses. As a prevention, the local data storage should be encrypted and isolated from the web based IoT application layer such as CoAP, HTTP, MQTT [32].

Randomized spamming can be another problem in the decentralized architecture, where unwanted broadcast information is stored digitally. For example, if a fake manufacturing terminal registers a fake sensorID in the network, it will not alter the information of other legitimate sensorID information but will occupy storage memory. This problem can be solved by a certificate based authentication where a trusted third party will issue certificates to the legit manufacturer for registering a sensorID. Physical layer information such as sensorID's RFID address, scanning node IP address are important information, which should be protected. Hence, extra security features at the hardware level should be implemented to prevent attacks.

Preferential treatment to some transactions over others can happen when a biased group of terminals are present in the network. However, as majority of the transaction information are communicated cryptographically with other nodes' consensus, preferential treatment is least likely to happen in this scenario.

VIII. Conclusion

An IoT based FSC monitoring architecture has been proposed in this work. Sensing modality was integrated with identification with a small footprint for tracking and quality monitoring of the food packages. When the food packages are scanned at different retailers, logistics or storage stage within the supply chain, the real time sensor data is updated in a blockchain providing a tamper-proof digital history. Any consumer or retailer can check the public ledger to obtain information regarding the specific food packages. The information helps in updating the shelf life, identifying key bottlenecks in the FSC, implementing targeted recalls and moreover increasing visibility. A single sensor integration was demonstrated in this work. However, more sensors for moisture, light or specific volatiles can be integrated with the RFID depending on the packaged food and sensing parameters of interest. The proposed architecture takes consensus from participating terminals in the network before updating the blockchain data. The broader participation of all the nodes helps to keep the network decentralized. The security analysis showed that the validation of a fake block drops with a higher number of node participation in the network and multiple consensus stages. However, the security features can be further improved by strengthening the hardware security of the sensorIDs and readers.

Acknowledgment

The authors would like to thank Mr. Brian Wright from ECEshop and all Electromagnetic Group members of MSU for helpful suggestions. This project was supported by the Axia Institute.

REFERENCES

[1] D. I. Ellis, V. L. Brewster, W. B. Dunn, J. W. Allwood, A. P. Golovanov, and R. Goodacre, "Fingerprinting food: current technologies for the detection of food adulteration and contamination," *Chemical Society Reviews*, vol. 41, no. 17, pp. 5706–5727, 2012.

[2] S. Herschdoerfer, *Quality control in the food industry*. Elsevier, 2012, vol. 2.

[3] J. Landt, "The history of RFID," *IEEE potentials*, vol. 24, no. 4, pp. 8–11, 2005.

[4] R. Saltini and R. Akkerman, "Testing improvements in the chocolate traceability system: Impact on product recalls and production efficiency," *Food Control*, vol. 23, no. 1, pp. 221–226, 2012.

[5] W.-D. Huang, S. Deb, Y.-S. Seo, S. Rao, M. Chiao, and J. Chiao, "A passive radio-frequency pH-sensing tag for wireless food-quality monitoring," *IEEE Sensors Journal*, vol. 12, no. 3, pp. 487–495, 2012.

[6] E. Smits, J. Schram, M. Nagelkerke, R. Kusters, G. v. Heck, V. Van Acht, M. Van Koetse, J. v. d. Brand, G. Van Den Gelinck, and H. Schoo, "Development of printed RFID sensor tags for smart food packaging," in *Proceedings of the 14th International Meeting on Chemical Sensors, Nuremberg, Germany*, 2012, pp. 20–23.

[7] R. A. Potyrailo, N. Nagraj, Z. Tang, F. J. Mondello, C. Surman, and W. Morris, "Battery-free radio frequency identification (RFID) sensors for food quality and safety," *Journal of agricultural and food chemistry*, vol. 60, no. 35, pp. 8535–8543, 2012.

[8] C. Amador, J.-P. Emond, and M. C. do Nascimento Nunes, "Application of RFID technologies in the temperature mapping of the pineapple supply chain," *Sensing and Instrumentation for Food Quality and Safety*, vol. 3, no. 1, pp. 26–33, 2009.

[9] J. Virtanen, L. Ukkonen, T. Björninen, and L. Sydänheimo, "Printed humidity sensor for UHF RFID systems," in *Sensors Applications Symposium (SAS)*. IEEE, 2010, pp. 269–272.

[10] K.-H. Eom, K.-H. Hyun, S. Lin, and J.-W. Kim, "The meat freshness monitoring system using the smart RFID tag," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 591812, 2014.

[11] K. H. Eom, M. C. Kim, S. Lee, and C. W. Lee, "The vegetable freshness monitoring system using RFID with oxygen and carbon dioxide sensor," *International Journal of Distributed Sensor Networks*, vol. 8, no. 6, p. 472986, 2012.

[12] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?" *Journal of Excipients and Food Chemicals*, vol. 7, no. 3, 2016.

[13] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[14] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," *Information Systems Frontiers*, vol. 17, no. 2, pp. 289–319, 2015.

[15] S. Piramuthu and W. Zhou, *RFID and sensor network automation in the food industry: ensuring quality and safety through supply chain visibility*. John Wiley & Sons, 2016.

[16] C. Costa, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti, "A review on agri-food supply chain traceability by means of RFID technology," *Food and bioprocess technology*, vol. 6, no. 2, pp. 353–366, 2013.

[17] O. Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, 2018.

[18] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2016, pp. 1–6.

[19] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *13th International Conference on Service Systems and Service Management (ICSSSM)*. IEEE, 2016, pp. 1–6.

[20] ——, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *International Conference on Service Systems and Service Management (ICSSSM)*. IEEE, 2017, pp. 1–6.

[21] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 2014.

[22] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference*. Springer, 1992, pp. 139–147.

[23] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "Karma: A secure economic framework for peer-to-peer resource sharing," in *Workshop on Economics of Peer-to-peer Systems*, vol. 35, no. 6, 2003.

[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[25] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014.

[26] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*. Springer, 2017, pp. 357–388.

[27] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2017, pp. 297–315.

[28] J. F. Salmerón, F. Molina-Lopez, A. Rivadeneyra, A. V. Quintero, L. F. Capitán-Vallvey, N. F. de Rooij, J. B. Ozáez, D. Briand, and A. J. Palma, "Design and development of sensing RFID Tags on flexible foil compatible with EPC Gen 2," *IEEE Sensors Journal*, vol. 14, no. 12, pp. 4361–4371, 2014.

[29] K. Mizuno and M. Shimizu, "Transportation quality monitor using sensor active rfid," in *International Symposium on Applications and the Internet Workshops*. IEEE, 2007, pp. 19–19.

[30] M. S. Khan, M. S. Islam, and H. Deng, "Design of a reconfigurable RFID sensing tag as a generic sensing platform toward the future Internet of Things," *IEEE Internet of things journal*, vol. 1, no. 4, pp. 300–310, 2014.

[31] S. Gueron, S. Johnson, and J. Walker, "Sha-512/256," in *Eighth International Conference on Information Technology: New Generations (ITNG)*. IEEE, 2011, pp. 354–358.

[32] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[33] X. Lu, Q. Li, Z. Qu, and P. Hui, "Privacy information security classification study in internet of things," in *International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*. IEEE, 2014, pp. 162–165.

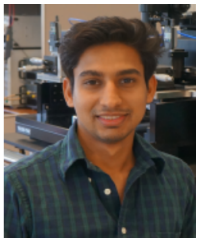
Saikat Mondal received the B.Tech. and M. Eng. in electronics and electrical engineering from IIT Kharagpur, Kharagpur, India, and City University of New York, NY, USA in 2013 and 2016 respectively.

He has been with the Telecom Regulatory Authority of India, Delhi, India as a Research Associate from 2013 to 2014. He is currently a PhD student in Michigan State University, East Lansing, MI, USA. His current research interests include RF circuit design, RFID, sensing, blockchain, and 3-D through-silicon-via inductor modeling. Mr. Mondal received the Best Student Paper Award at the IEEE International Conference on Electronic Packaging Technology Conference in 2015.

Kanishka P. Wijewardena was born in Sri Lanka in 1998. He is currently studying for his B.S. degree in Computer Engineering, Class of 2021, at Michigan State University, East Lansing, MI, USA. Since 2017, he has been a Professorial Assistant in the Electromagnetics Research Group of the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI, USA. His research interests include, embedded devices, energy efficient devices, radio frequency identification and sensors.

Saranraj Karuppuswami (S15) received the B.E. degree in electrical and computer engineering from Anna University, Guindy, India, in 2011, and the M.Sc. degree in electrical engineering from the National University of Singapore, Singapore, in 2013. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Michigan State University, East Lansing, MI, USA. From 2013 to 2015, he was with the Energy Research Institute, Nanyang Technological University, Singapore, as a Research Associate. His current research interests include RF sensors, metamaterials, and sensors for supply chain.

Nitya Kriti received the B.Tech. in electronics and communication engineering from Sikkim Manipal Institute of Technology, Rangpo, India. Her research interests includes blockchain technology and DNA fingerprinting.



Deepak Kumar received the B.Tech. and M. S. in electronics and electrical engineering from Lingayas University, Haryana, India and University of Colorado Denver, USA. He is currently pursuing his PhD in Electrical and Computer Engineering from Michigan State University, East Lansing, MI, USA. His current research interest includes Wireless Communication, Imaging, RF Sensors, Non Destructive Evaluation and Structural Health Monitoring.

Premjeet Chahal (M'03) received the B.S. and M.S. degrees in electrical engineering from Iowa State University, Ames, IA, USA, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 1999.

He was a Senior Researcher with Raytheon, Dallas, TX, USA, from 1999 to 2006, and with Abbott Laboratories, Abbott Park, IL, USA, from 2006 to 2008, where he developed many new technologies for sensing, devices, packaging, and components. He joined Michigan State University, East Lansing, MI, USA, in 2009, as a Faculty Member, and has been an Associate Professor since 2015. He holds nine U.S. patents. His current research interests include blockchain, terahertz technology, millimeter-wave electronics, RF-based sensors, RF MEMS, RF-optical devices, and microwave and millimeter-wave systems packaging.

Dr. Chahal was a recipient of the 2012 DARPA Young Faculty Award and the 2016 Withrow Teaching Excellence Award.