Will Blockchain technology become a reality in sensor networks?

MARCHANG, Jims <http://orcid.org/0000-0002-3700-6671>, IBBOTSON, Gregg and WHEWAY, Paul

Will Blockchain Technology Become a Reality in Sensor Networks?

Jims Marchang
Department of Computing
Sheffield Hallam University
Sheffield, UK
jims.marchang@shu.ac.uk

Gregg Ibbotson
Department of Computing
Sheffield Hallam University
Sheffield, UK
acesgi@exchange.shu.ac.uk

Paul Wheway
Department of Computing
Sheffield Hallam University
Sheffield, UK
cmspw@exchange.shu.ac.uk

***Abstract*—The need for sensors to deliver, communicate, collect, alert, and share information in various applications has made wireless sensor networks very popular. However, due to its limited resources in terms of computation power, battery life and memory storage of the sensor nodes, it is challenging to add security features to provide the confidentiality, integrity, and availability. In order to communicate reliably with trust and authenticity, providing data and system security especially for those sensors dealing with sensitive data related to healthcare, military activity, environmental sensing for weather prediction or seismic data etc. is vital. Blockchain technology ensures security and avoids the need of any trusted third party for security. However, applying Blockchain in a resource-constrained wireless sensor network is a challenging task because Blockchain is power, computation, and memory hungry in nature and demands heavy bandwidth due to control overheads. In this paper, a new routing and a private communication Blockchain framework is designed and tested with sensors generating constant and continuous data (like voice and video). However, it is realized that even if computation and bandwidth requirements are taken for granted, storage and battery life will cripple the sustainability of Blockchain application in sensor networks especially for high data generating sensors. The proposed Load Balancing Multi-Hop (LBMH) routing shares and enhances the battery life of the Cluster Heads and reduce control overhead during Block updates, but due to limited storage and energy of the sensor nodes, Blockchain in sensor networks may never be a reality unless storage and battery life of sensor devices are not limited on the one hand and computation power and bandwidth availability are high, on the other.**

***Index Terms*—Sensor Networks, Blockchain Technology, Cluster Head**

I. Introduction

Wireless sensor networks have a wide range of applications including industrial, healthcare, military, environmental sensing and monitoring, urbanization and infrastructure [1]. In most of these applications, they deal with sensitive information, so security should be required, to provide privacy, data integrity and availability [2] [3]. The network comprises of a group of lightweight battery powered devices and a wireless infrastructure to record and monitors the surrounding environment (building, city, wild areas and so on). The inherent problem of the network includes limited shared bandwidth, low computation power, low storage, and limited battery life. When nodes are deployed in inaccessible terrains or disaster relief areas localization of the sensor nodes is a huge challenge [4]. Due to its limited resources, providing computationally intensive security features is a huge challenge. However, providing security to the node and ensuring data communication secrecy is vital to maintaining the confidentiality, integrity, and availability (CIA) so required. In such networks, security vulnerabilities of different layers of the network from physical to the application layer are highlighted by [5] [6]. One such technology that ensures implementation of the CIA triad as a package in security is Blockchain technology. Blockchain provides a global digital ledger to be used for every form of transaction and record in a systematic order. It is public, but it's tamper-proof, node failure tolerant, and secure without the need or help of any trusted third party. This makes it an interesting technique to apply in any kind of distributed network and is used for cryptocurrencies (Bitcoin, Etherium, Ripple etc) [7] with great success, but grows as a threat to the traditional financial banking system. In this paper a wireless sensor network framework is designed aiming to support a Blockchain by considering the limited computational power, battery life and storage of the sensor nodes in one hand and conducts architecture optimization to reduce control overhead needed for routing and block updates and balances energy among cluster heads.

II. Background Study

The Blockchain, is built by providing asymmetric key encryption, hash values, Merkle Trees and Peer-to-Peer networks and its application domain is vast as highlighted in [8]. In a sensor network with limited resources, it will be more appropriate to design a lightweight key encryption technique rather than using standard asymmetric key encryption techniques. The technology is also used in designing robotic swamp systems to provide security, decision making, behavioral differentiation and business models [9]. In a Bitcoin Blockchain, a block takes around 10 minutes to complete its processing, so to confirm a transaction it takes a long time. So, directly applying the Blockchain technology in a sensor network is not feasible due to a limited resource build-in the sensor nodes, latency effect and the network limitations nature like throughput and bandwidth, when dealing with real-time sensitive and urgent sensor information. Sensor nodes can be responsible for collecting different types of data including video, images,

voice, movement, temperature, seismic data for example. If the data collection is video or images which need considerable processing and transmission time, adding a distributed global ledger will totally outweigh the feasibility and advantages of security and indestructible scope provided by Blockchain due to limited sensor resources in terms of computation power, storage, and battery life. Since data communication of image sensor networks takes most of the energy, data compression technique allow a significant reduction in the transmission time and correspondingly the overall transmission energy [10]. Balancing an energy consumption of communication and computation could be achieved by data compression and its true when data to be communicated is image or video, but in many cases data communication may take the least energy consumption compared to computation, if data to be communicated is small in size eg. temperature data, seismic data, humidity data and so on. In fact, enabling security features and incorporating salient features of security in terms of providing data integrity, confidentiality, and availability, the energy usage for computation will overwhelm that is used for data communication, especially when the data is neither image nor video like data.

A. Security Challenges and Related Work in Sensor Network

As briefed in the introduction in order to consider that a system is secured, the following three points are vital and mandatory:

1) Confidentiality: *Unauthorized users should not be allowed or should not be able to access any sensitive information from a system.*
2) Integrity: *The guarantee that information is not tampered with or altered, modified or deleted by an unauthorized user.*
3) Availability: *Authorized user should be able to access the data when needed or required. The means of making the data available can be through a physical presence in front of the system or via a network.*

In the current sensor model, the Sink collects all the data, so the confidentiality, integrity, and availability are maintained and controlled via the Sink. Authentication of the sensor nodes after deployment and data privacy are incorporated in order to avoid access of the data by unauthorized users. The key for maintaining the confidentiality of sensed data is managing the private key or shared key in such a way that others don't have a way to access the private key or the shared key because compromising the private key or shared key will lead to leaking of information. One of the latest key management systems designed is CONIKS [11], it does not need users from encryption key management. In this mechanism, initially the user request for a public key from the server by using a user-name and here, when it wants to communicate with another user then it checks if the public key it uses is the same as the public key held by the receiver. It also ensures that the key has not been changed. In a sensor network, communication from the Sink to the data server or cloud server could also use certificates to guarantee security over the data transmission over the internet, but it has to make sure that the certificate providers should be a trusted third party. In order to maintain the trust of the certificate provider and conduct Secure Socket Layer (SSL) auditing in real time (validity of the certificate can be checked), a Google Certificate Transparency framework is developed using a Merkle hash tree [12]. In a Blockchain model, the integrity of the data is maintained by using hashing techniques and proof-of-work method. In terms of data availability, since the data storage in Blockchain is distributed in nature, access to data is easy and readily available. The interesting fact, about Blockchain, is that since it works on distributed nature, attack on some portion of the network will not impact the entire network. However, the majority attack or 51% attack is a situation, where a single user or n number of users take control of the majority of the mining power, so the attacker takes control in generating a new block, receiving rewards, reverse transactions etc.

A zero-knowledge proof or zero-knowledge protocol is a method in which a user claims to know certain information without revealing more than the claim made about knowing the information [13]. The privacy of the data can be increased through this method as designed in Zerocoin [14], Zerocash [15] or Zcash [16], unlike bitcoin where the data and the distributed ledger is not private [17]. If original Blockchain technology idea is closely observed, it is clear that all the data is available to all the participating users or devices, so confidentiality is not a primary feature of this technology, however, anonymity of the user identification is maintained. It's computation expensive and complex, so adopting such method in Sensor networks will be very challenging.

Due to the nature of the limited resource constraints of the sensor networks, incorporating security features to provide data confidentiality, data availability, data integrity, authentication, avoiding relay attack, access control, denial of service attack and non-repudiation attack is a huge challenge [18] [19]. If a Blockchain can be applied, then there is no need of a trusted third party and the aspects of privacy, integrity, and confidentiality will be covered and provides high-level security and avoid replay attack and non-repudiation all at the same time. Other security aspects like detecting malicious nodes, intrusion detection, and access control can also be ensured to provide better overall security to the sensor networks. The security levels can be grouped into three categories i.e. Data level requirement (anonymity and freshness), access level requirement (authentication, authorization, and accessibility) and network level requirements (robustness, self-organization, time synchronization) as highlighted in [20]. The authors of [20] also elaborate that attacks in a wireless sensor network can happen across the layers starting from the physical layer to the application layer. Attacking the physical layer can give access to unauthorized nodes, whilst jamming and data collision techniques can destroy the usable channel and caused congestion, data loss, increased interference and waste energy at the Data link layer. The attack can also occur in a Network layer in the form of replay attack, sink-hole, selective route forwarding,

hello flooding and spoofing in order to generate an error or false message, misleading route compromise, refusing data forward, network congestion and data tampering respectively. Other forms of attacks can include energy draining by sending un-ending connection request at the transport layer to exhaust the node's resources and it can even lead to denial of service. A node can be inserted along the path of communication to generate false data to attack the ongoing communication and degrades the energy usage and increase the data collision at the application level. Other authors also highlight the security challenges in the Internet of Things (IoT) and identify the security vulnerabilities and threads in [21] [22] [23]. This paper aimed to design a Blockchain framework to address security solutions as a single package since Blockchain doesn't need a trusted third party to perform secure communication between any two transacting nodes but ensures data confidentiality, integrity, and availability. In a decentralize sensor network, in order to build trust and authenticate, a Blockchain based mechanism is designed in [24], but this paper is a first attempt in wireless sensor networks to study the applicability of Blockchain in terms of resource constraints.

B. Blockchain applicability in Sensor Networks

Blockchain technology is an amazing concept, but will it be applicable in sensor network where the computation, battery life, storage, and bandwidth are limited. Moreover, adopting Blockchain technology in a distributed network has lots of advantages including data incorruptible, data temper-proof, non-repudiation, resilient to failure, provides transparency with pseudonymity, validity checking, avoidance of depending on specific systems to mention some. However, adopting Blockchain has many challenges including the followings:

1) Energy consumption: *Since a block is created for each transaction and it is replicated to each node in the network after adopting security features like hashing e.g. MD5, SHA-256, SHA-512 etc..*
2) Computation Power: *In order to create a block, appending a block, receive or send a block and incorporating security features adds up to the complexity of the computation power*
3) Storage Memory: *Since the block created or received from other nodes are all stored, each node has a high demand of memory for storing the data*
4) Validation and verification: *User and transaction validation can be an additional overhead, but its compulsory for digital-based financial transactions. Who will be responsible for sensor networks?*
5) Control Overhead: *Creating a new block leads to broadcasting to a P2P network communication for necessary block updates, however in a sensor network with limited resources, it will be a challenging task.*
6) Bandwidth: *Creating of any new blocks by any node leads to additional communication overhead and since bandwidth is shared and is limited, efficient routing and block updates techniques have to be designed not to stain the limited bandwidth while dealing with overheads*
7) Dynamic Nature of the Network: *The network keeps changing depending on the number of nodes (joining or leaving or dying), change in cluster head, change in route etc.*
8) Identity Privacy: *Even though anonymity is maintained, its actual pseudonymity and others can figure out the activity if the activity is not encrypted*
9) Overheads for Data Secrecy: *Applying high-end encryption for data communication will further stress the limited sensors and its network resources, however its important if collected data is to be kept hidden from the intruders. So, designing smart lightweight secure encryption techniques are vital to support data secrecy*.

Incorporating all the Blockchain features in a sensor network may not be realistic due to limited battery life, computation power and storage unless an efficient framework and techniques are adopted. The challenges and issues faced by the Internet of Things network are also addressed in [25]. The time complexity of MD5 and SHA-256 is $\ominus(N)$ and in terms of computation time, MD5 takes lesser time compared to the SHA-256 [26]. The output of the MD5 is 32 digit Hex irrespective of the input file size and likewise for SHA-256, the output is 64 digit Hex. So, in terms of storage, applying SHA-256 will increase the storage by 100% and if SHA-512 is used then storage will be increased by 400% compared to MD5. As per the findings of the authors of [26], it can be deduced that it takes an average of 1.85e-07 seconds and 5.07e-07 seconds per byte size input data execution in MD5 and SHA-256 respectively when an Intel(R) Core(TM) i5-2430M CPU @ 2,40GHz (4CPUs), 2.4 GHz architecture with 8.00 GB RAM is used. It means that SHA-256 takes approximately 2.7 times the time needed to execute the same input data compared to MD5. In reality, the sensor nodes are not equipped with a powerful processor and are supported by limited battery life too but have to execute complex computation intensive hashing and encryption if Blockchain security is to be incorporated. So, it will be very unrealistic to apply Blockchain at the sensor node level because it is not equipped with sufficient resources especially in terms of computation power, storage, and battery life. However, if Blockchain is applied then the advantages is immense as highlighted earlier.

III. Proposed Hierarchical Sensor Network Model

In this paper, a novel approach of selecting and assigning tasks for the cluster heads (C_h) depending on the type of activity or its role (routing to the sink or collecting data from sensors), sensor node density and rate of energy usage is proposed. In this model, the nodes are classified into two categories namely: potential cluster heads i.e. S_m (more powerful in terms of computation and battery life) and normal sensor nodes i.e. S_n which senses data and deliver data to the Sink via the potential cluster heads or cluster heads. Therefore, So, in this proposed model, any sensor nodes cannot become a cluster head, rather a cluster head is selected only from S_p which has more energy and computation power. In real life

applications, it becomes unrealistic to make the cluster heads conduct routing, heavy computation and data forwarding all at the same time for all the cluster members and be treated as normal sensor nodes of the same energy and computational level. Applying a power hungry and computational intensive Blockchain (BC) technology to all the participating nodes of the sensor networks to maintain data integrity and privacy will not be realistic, because sensor nodes conduct only light information gathering, processing, and communication. In a normal sensor network without considering security features, the main energy usage by a normal sensor node is due to communication and computation.

In a normal sensor network scenario when a collected data is relayed to the neighbor node or cluster head without much data processing then data communication power may require more energy than computation power [27]. However, if security features like data integrity, confidentiality and availability are incorporated then heavy processing of data will lead to a very high computational power and energy consumption in computation will outweigh the energy used in communication. So, resource-aware load sharing is vital to distribute the energy consumption levels of the participating active sensor nodes (SN_a), especially the designated cluster heads (C_h). Thus, the sensor nodes are divided into more powerful (S_m) and normal nodes (S_n), total sensor nodes deployed = $S_m \cup S_n$. Among the more powerful sensor nodes i.e. S_m, cluster heads C_hs are selected, so S_m = $C_h \cup C_p$, where C_p are the sensor nodes which can become cluster heads but are not acting as a cluster head at the moment. The sensor nodes could be in an active or passive mode or non-existent due to no battery life, so sensor nodes (S_n) which could become cluster members = $SN_a \cup SN_n$, where SN_n are the non-active sensor nodes.

The paper address the following three aspects to make the cluster heads more durable and secure.

- Dynamic cluster head selection.
- Resource aware routing to balance energy usage in the network
- Using Blockchain to provide data privacy and security

Using Blockchain is not only computationally intensive but also memory and communication intensive, so applying Blockchain in a sensor network is not only challenging but also very difficult, unless ways of reducing control and communication overheads are designed, find ways to reduce memory utilization and most importantly find ways to reduce computation power.

A. Cluster Head Selection

In this model, cluster heads are dynamically and distributedly selected. The factors used in selecting the cluster heads are based on active node density (SN_a), energy depletion factor (E_{df}) and a random value (R_v). All the deployed sensor nodes need not be active at all times, because identical sensors can share the activity load and some may go into suspend or sleep mode while others are active. So, considering only the number of active nodes at a given time is more appropriate in evaluating the node density because it is the active nodes

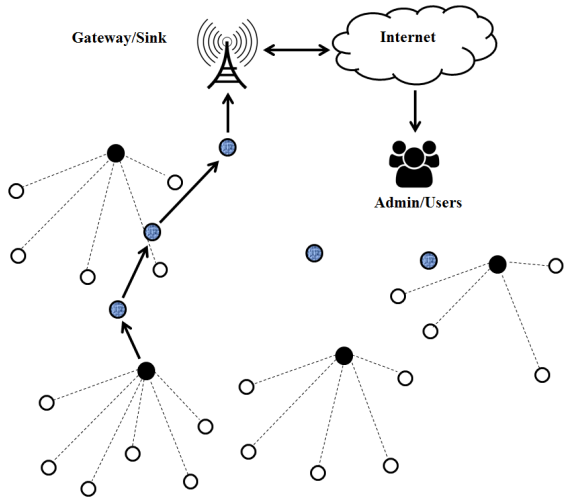

Fig. 1. Routing from a Cluster Head to the Sink.

which involved during channel contention. In terms of energy usage or residual energy, it is more appropriate to assign the role of cluster head role to the one which uses lower rate of energy or have a higher energy residual based on its recent usage rather then simply looking into the static remaining energy level, because the one using the higher energy rate will end up depleting its energy level faster compared to the one using energy with lower rate in the recent past, in this work, the energy-depleting factor (E_{df}) is derived from $Remaining_e/EU_{rate}$ where $Remaining_e$ and EU_{rate} stands for total remaining energy of the node and the rate of using the energy in the recent past respectively. The active node density distribution of the cluster members provides the level of load distribution on the cluster head over time. Thus, a factor that narrates the energy level of the present and the prospect of the durability of the node's energy is given by E_{useful} in 1.

$$E_{useful} = \frac{Remaining_e}{EU_{rate} \times SN_a} \tag{1}$$

When active node density and energy usage are similar then the deciding factor for cluster head selection is governed by a random value generated by each potential cluster heads C_p. Initially, the energy levels will be the same or similar, so the deciding factor for selecting cluster heads is active node density (SN_a) and a random value (R_v). If the derived E_{useful} is similar then the random value will decide the outcome of cluster head selection. In order to collect the information about the potential cluster members, all the S_m nodes broadcast a "hello" packet to measure the density of the cluster members that it can cover within a transmission range and upon receiving the "reply" messages from all the active neighbor sensor nodes i.e. SN_a, each potential cluster head registers the number of all the active sensors. After collecting the sensor density information of potential cluster members within the vicinity of each potential cluster heads, each potential cluster head S_m nodes conducts the following steps:

1) Broadcast the E_{useful} and the pseudo-random value R_v i.e. (E_{useful} and R_v)
2) Upon receiving (E_{useful} and R_v) by each S_m nodes, it checks the possibility of becoming a cluster head by checking the following:
    a) It checks if E_{useful} of self is $> E_{useful}$ of the rest of S_m which are received and are well within its transmission range. Then, this node becomes the cluster head.
    b) However, if its E_{useful} value is same with any of the other potential cluster heads then, the value of the pseudo-random value is check to see if its R_v value is $> R_v$ of the rest of the values generated by the rest of S_m which are received and are well within its transmission range. It is highly unlikely that two or more potential cluster head generates the same pseudo-random value at the same time.
3) If 2(a) or 2(b) is satisfied when a cluster head among the competing nodes will be determined, however, if E_{useful} and R_v are same (which is very highly unlikely), then the nodes which have the same R_v are allowed to regenerate a pseudo-random and re-broadcast to determine who has a greater R_v to avoid conflicts.
4) Repeat step 3, if cluster head within a transmission range cannot be determined.
5) Thus, cluster heads (C_h) is selected from among S_m. The cluster head selection is initiated by the existing cluster head based on the amount of energy spent (use of 10% energy since it took charged of the cluster head role) rather than time duration, because battery depletion rate is directly related to the activity of the number of sensor nodes and the rate of data generated. Considering time duration to trigger cluster head selection process could mean overwork for some cluster head while other cluster head may be less busy depending on the activity and the time of activation of the sensor nodes.

B. Routing from Source to Sink

Cluster heads are already overloaded by the incoming data from the cluster members, so using the cluster heads to route data from the sensor sources to the sink will enhance the depletion of the battery life of the cluster heads. So, in this framework, routing to the sink is conducted via the cluster head from the sensor nodes as shown in figure 1. However, the routing is designed in such a way that the path between the sensor source node and the Sink is not built by the cluster heads, rather the i^{th} cluster head i.e. ${C_h}^i$ build a path using the other potential cluster heads C_p, rather than using the cluster heads to balance the load, computing power, and energy usage. The routing from a Source node to the Sink is done in two stages in order to offload the burden of computation to the sensor nodes as follows:

1) Source to the Cluster head: The routing from a Source sensor node to its cluster head is conducted by a secure broadcast technique to the Cluster head. The job of the Cluster head is to collect information from the cluster members, but in order to collect the information from the cluster members securely, it provides its public key during the cluster member discovery session, so that any information sent by the cluster members are encrypted and are secure.

2) Cluster head to the Sink: The Cluster head is responsible of discovering a route to the Sink for every Cluster members. Adopting this method helps all the cluster members, because each cluster members are now not responsible for discovering a route to the Sink, rather only one node i.e. the Cluster head is responsible for the route discovery for all its member only once. So, the route discovery overhead is reduced immensely as the number of cluster member increases. A novel flow based load balancing AODV routing from a Cluster head to the Sink is designed as follows:

1) All nodes do not forward route request routing packets. So, the routing route request packets does not flood the network.
2) Only the potential cluster heads C_p forwards the route request initiated by the i^{th} cluster head.
3) All the cluster members of the i^{th} cluster head forwards their data to the cluster head and the cluster head route the data to the sink following the route via the potential cluster heads C_p.
4) Each potential cluster heads C_p records the number of flows generating from *n* unique sources. In order to balance the load, power computation and energy usage, potential cluster heads C_p forward the route request packet along with the number of flows (F_n) it relays. When an j^{th} potential cluster head receives a route request from an i^{th} potential cluster head, it checks to update the (F_n) to number of flows along that route as follows:
    a) If F_n of j^{th} potential $C_p > i^{th}$ potential C_p then F_n = flows of j^{th} potential C_p.
    b) Otherwise, F_n = flows of i^{th} potential C_p. So, the number of maximum number of flows along that route is reported to the Sink.
5) The Sink node checks the following before the route reply is initiated:
    a) It compares the F_n values receives from all the ${C_p}^1$, ${C_p}^2$, ${C_p}^3$, ..., ${C_p}^i$, ..., ${C_p}^n$ through route request packets.
    b) Min of $\{$ F_n values$\}$ from among all the C_p is selected and route reply is initiated.

By adopting this routing method three factors pertaining to the load, computing power and energy usage of the cluster heads will be reduced and durability of both the cluster heads and potential cluster heads are distributed and balanced. This provides a better scope to incorporate a memory, power, and computation hungry technology like Blockchain technologies. However, it will be very challenging to incorporate an incorruptible but transparently distributed ledger to ensure data temper-proof, non-repudiation and resilient to failure etc.

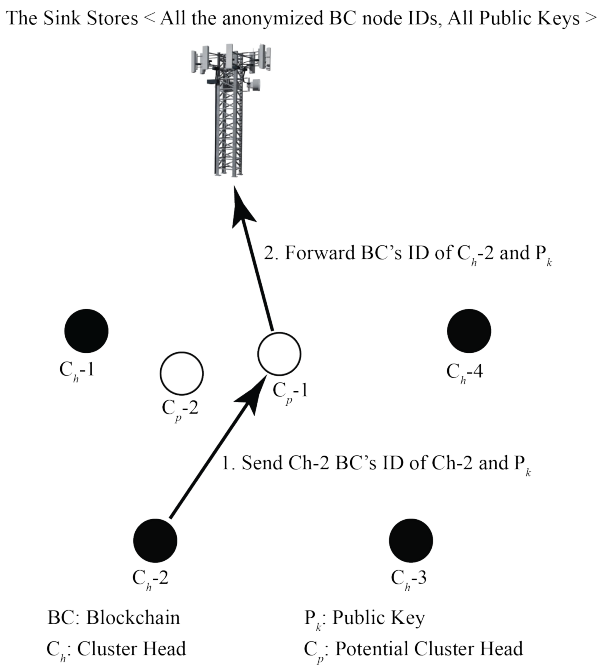

Fig. 2. Cluster Heads updating its BC's ID and its Public Key to the Sink.

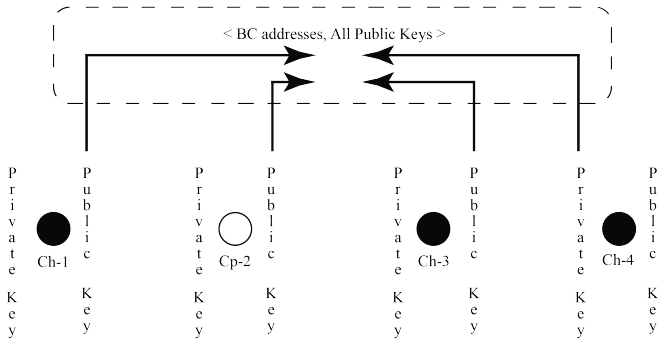

Fig. 3. Communication using Public Key in the Blockchain.

Network Parameters	Protocol/Value Used
Grid Size	1000 m^2 x 1000 m^2
Routing Protocol	EEM-LEACH Vs Proposed LBMH
Queue Type	DropTail
Queue Size	100
Bandwidth	2Mbps
Default Power (Pt)	24.49dBm
Default RXThresh	-64.37dBm
Default CSThresh	-78.07dBm
MaxRetry	7
Simulation Time	1000
Traffic Type	CBR
Frame size	100 Bytes

TABLE I
SENSOR NETWORK SIMULATION SETUP.

IV. PROPOSED PRIVATE BLOCKCHAIN IN LBMH- SENSOR NETWORK ROUTING

Cryptographic complexity of Blockchain limits its applicability in Sensor Networks due to the limited resources available in the sensor nodes. However, to harvest the benefits of Blockchain, an attempt is made to design a private Blockchain in order to avoid data tampering, damage or falsification of information and to prevent from potential threats, attacks, and misuse of information. In this framework, miners will not be involved, but the Sink will be responsible for authenticating the participating sensors nodes and the Sink stores the node's ID along with the anonymized BC node IDs. It also stores all the public keys of all the participating sensor nodes, so that it becomes easier for the C_hs to retrieve the public keys i.e. P_ks. During the route discovery from the source's C_h to the Sink node, the Sink stores the reverse route information to the source. So, the Sink doesn't need to re-discover the route to the C_h again as long as the routes are valid. This measure will offload the control overhead of performing heavy peer-to-peer communication when block updates have to take place because, in this framework, block updates will take place via the Sink otherwise the overheads of conducting block update will overload the limited sensor network resources. All the cluster head updates its BC's ID and P_k to the Sink as shown in figure 2. Since the Sink node has high computation power, high bandwidth, high energy, and high memory storage, it is used to facilitate, store and relay public keys of the cluster heads in the proposed Blockchain model as shown in figure 3. Each block stores nonce (8 bytes), previous header's hash (32 bytes), timestamp (8 bytes), block type (1 byte), data count of each type (8 bytes), and the hash of the data (32 bytes), in this model the actual data is not stored in the blocks, otherwise the volume of data generated will be impossible to store especially when the data is audio, video or picture etc. So, other sensor nodes or cluster nodes cannot know the actual data collected by other sensors but is used only to maintain consistency. All the data collected from the sensor nodes is communicated to the Sink (Gateway) by encrypting using the Sink's public key, so only the Sink can decrypt the information. In terms of securing data communication between P2P, an RSA public key cryptography is used in the framework and for hashing SHA-256 is used.

In the following sections will analyze the energy, storage and control overhead usage for the proposed private Blockchain and also study if the proposed routing and cluster head selection enhance the durability and connectivity of the network. The proposed private Blockchain based load balancing multi-hop routing is compared with EEM-LEACH [28] which discovers a multi-hop path considering minimum communication cost from each sensor nodes to the Sink.

V. RESULTS AND ANALYSIS

In this study, the focus is given on battery utilization and storage requirement when a Blockchain using SHA-256 hashing and an RSA public key cryptography is adopted. It is clear that adopting Blockchain will not only protect the

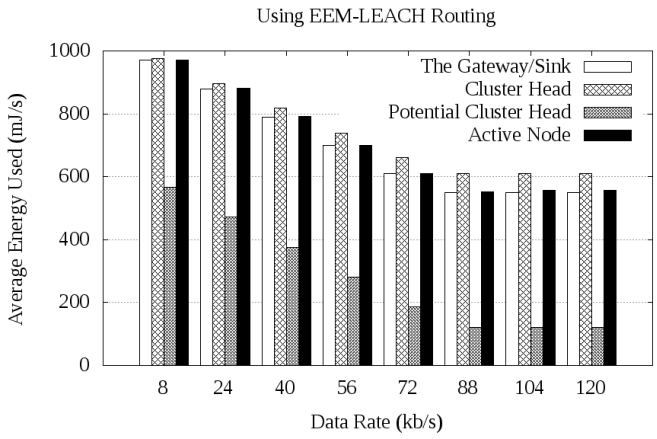

Fig. 4. Energy usage during data Transmission in EEM-LEACH Routing.

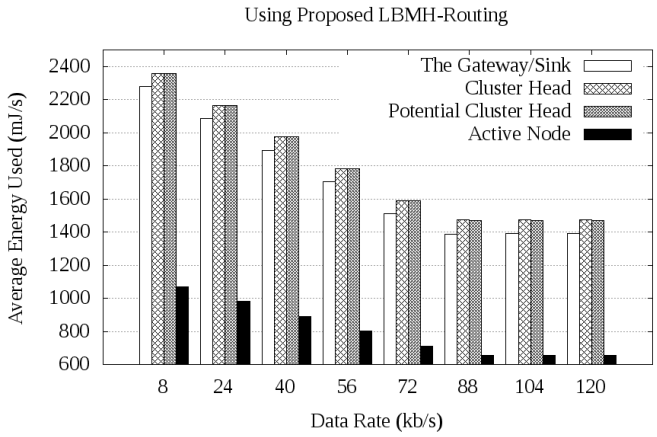

Fig. 5. Energy usage during Data Transmission and Blockchain update in Proposed LBMH-Routing.

sensed data by the sensors but the Sink (the Gateway) is also protected from the man-in-middle attack because the neighboring cluster heads will help the Sink in ensuring data consistency through Blockchain hashing, secrecy, and privacy through RSA algorithm. The network parameters used in the test are given in table I. In this simulation model, it is assumed that 100 mJ/s of energy is used during encryption, decryption and hashing computation by the Sink, Cluster Head, and the Potential Cluster Heads.

A. Battery Life

In EEM-LEACH Routing as shown in 4, the energy usage of the Gateway/Sink, Cluster Heads, Potential Cluster Heads, and the sensor nodes decreases as the data rates of the participating nodes increases because more data could be transmitted for a fix data packet size per second. However, the energy utilization of the active nodes remains constant after 88kb/s because 100 Byte packet gets saturated after that data rate. It is observed that in the EEM-LEACH routing protocol, the amount of energy used by the Cluster Heads and the Sensor nodes are similar, however, the potential surrounding cluster heads use lesser energy, so the energy depletion rate of the cluster head is high in this model. When the data rate is low and more time is required to send a 100 Byte packet, each node uses close to 1000 mJ/s except the neighbor nodes, however, the energy usage goes down as low as around 600 mJ/s for both Cluster Heads and the Sensor nodes. When the neighbor nodes do not participate in the transaction of sending or receiving data, it also uses energy for sensing and checking node status and surrounding activity.

On the other hand in the proposed routing model using a private Blockchain Technology, the amount of energy usage with the cluster head and the potential cluster heads are similar, because of the fact that the routing of multi-hop nodes are not conducted via the Cluster heads unlike EEM-LEACH, but they are routed via the potential cluster heads. It is an advantage in terms of energy sharing and balancing to prolonged the battery life of the participating nodes. Another advantage is that the usage of the sensor node's energy is reduced immensely compared to the cluster heads and the potential cluster heads because it is the cluster heads that endures and carried out all the complex computations including encryption, decryption, and routing etc. However, the amount of energy used is extremely high compared to the ones like EEM-LEACH which does not use Blockchain Technology. The amount of energy usage is as high as nearly 2400 mJ/s when the data rate is as low as 8 kb/s and it's as low as around 700 mJ/s for sensor nodes while the cluster heads and potential cluster heads consumed energy as low as approximately 1500 mJ/s. It shows that the amount of energy consumption is around 150% more for the Gateway/Sink, cluster heads and potential cluster heads when Blockchain technology is adopted. It also shows that Block updates in a Blockchain consume as much energy as the energy used in normal data transmission. This energy consumption is calculated when the sensor network is activated using only two active sensor nodes generating 100 Bytes packet at a constant rate. It means that as the number of active sensor nodes increases, the amount of energy usage for Block updates, and other cryptographic computation is going to increase exponentially. More active nodes imply more Block updates, and it means higher bandwidth requirement, and it also means that the overall performance of the network will degrade due to limited bandwidth. So, in terms of battery life support, applying Blockchain will cripple the limited constrained bandwidth and the limited power supply.

B. Storage Requirement

In terms of storage requirement, since the normal sensor nodes or the cluster heads don't store data except buffering during queuing not much storage space is required in any normal sensor nodes. In this study, the size of the queue is 100, so at the most 100 packets can be queued at a time, however, when Blockchain is adopted, it is mandatory to have permanent storage for maintaining the Blocks of the Blockchain. In this model, the size of each Block is 89 Bytes, so irrespective of the data size generated or sent by the sensors,

the Block size is 89 Bytes. In this test, a packet size of 100 Bytes is taken into account, and the simulation was run for 1000 seconds. When the data rate was 120 kb/s, the throughput was 107 packets per second per sensor node, which accounts to 107 Blocks per second, and equates to 107000 for 1000 seconds. So, the storage required equals to 89 Bytes x 107000 = 9.523 Megabyte. When there are 100 sensors and the number of data generated is the same, then 952.3 Megabyte data is formed as a Blockchain when 100 sensors gather data for just 1000 seconds (16.6667 minutes). It means that in an average when 100 sensor nodes are active and each sensor generates 107 packets per second and each packet size is 100 Bytes, then 952.3 Megabyte of Blockchain data is generated within approximately 17 minutes. It will make Blockchain unsustainable for any form of wireless sensor networks, despite load balancing and energy distribution because of storage hungry.

VI. Conclusion and Future Direction

In resource-constrained sensor networks, incorporating a resource hungry technology like Blockchain is a huge challenge. In order to make it a reality, multiple considerations has to be taken into account to meet the resource requirement in terms of computation power, communication overhead, battery life, and limited bandwidth etc. In this framework, the Sink is updated with the routes of the cluster heads to reduce control overheads during block update activities. Routing via the potential cluster heads for routing rather than using the cluster heads balances and distribute the energy usage. During a new block formation and block updates, cluster head does it via the Sink securely and when a new cluster head is selected, the Blockchain is updated from its neighbor cluster head.

It is realized that introducing Blockchain in a sensor networks is far from reality especially for real time data like voice or video, because storage and battery life will not be able to support with ease even if computation and bandwidth constraint are ignored. In future, detail network performance will be further studied with different data types and the framework will be tested using real devices.

References

[1] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, 2014. "Wireless sensor networks: A survey on recent developments and potential synergies," J. Supercomput. , vol. 68, no. 1, pp. 148.

[2] F. Mattern and C. Floerkemeier, 2010. "From the Internet of computers to the Internet of Things," in From Active Data Management to Event-Based Systems and More. Berlin, Germany: Springer, pp. 242259.

[3] Y. Mo et al. , 2012. "Cyber-physical security of a smart grid infrastructure," Proc. IEEE , vol. 100, no. 1, pp. 195209.

[4] Suo, H., Wan, J., Huang, L. and Zou, C., 2012. "Issues and challenges of wireless sensor networks localization in emerging applications". In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 3, pp. 447-451). IEEE.

[5] Sastry, A.S., Sulthana, S. and Vagdevi, S., 2013. "Security threats in wireless sensor networks in each layer". International Journal of Advanced Networking and Applications, 4(4), p.1657.

[6] Pathan, A.S.K., Lee, H.W. and Hong, C.S., 2006. "Security in wireless sensor networks: issues and challenges". In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.

[7] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[8] Chris Jaikaran, 2018. Blockchain: Background and Policy Issues. CRS Report, Congressional Research Services, R45116.

[9] Ferrer, E.C., 2016. The blockchain: a new framework for robotic swarm systems. MIT Media Lab, arXiv preprint arXiv:1608.00695.

[10] Ferrigno, Luigi & Marano, S & Paciello, Vincenzo & Pietrosanto, Antonio, 2005. "Balancing computational and transmission power consumption in wireless image sensor networks". VECIMS 2005 - IEEE International Conference onVirtual Environments, Human-Computer Interfaces, and Measurement Systems. 2005. 6 pp.. 10.1109/VECIMS.2005.1567564.

[11] CONIKS. Accessed: 05.12.2018. [Online]. Available: https://coniks.cs.princeton.edu

[12] Googles Certificate Transparency . Accessed: 05.12.2018. [Online]. Available: https://www.certificate-transparency.org

[13] M. Schukat and P. Flood, Zero-knowledge proofs in M2M communication, in Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Commun. Technol., Limerick, Ireland, Jun. 2014, pp. 269273.

[14] Zerocoin. Accessed: 05.12.2018. [Online]. Available: http://zerocoin.org

[15] Zerocash. Accessed: 05.12.2018. [Online]. Available: http://zerocash-project.org

[16] Zcash. Accessed: 05.12.2018. [Online]. Available: https://z.cash

[17] bitcoin. Accessed: 05.12.2018. [Online]. Available: https://bitcoin.org

[18] M. E. Whitman and H. J. Mattord, 2012. "Principles of Information Security", 4th ed. Boston, MA, USA: Cengage Learn.

[19] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, 2016. A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE, vol. 104, no. 9, pp. 17271765.

[20] I. Tomi and J. A. McCann, 2017. "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1910-1923.

[21] J. S. Kumar and D. R. Patel, 2014. "A survey on Internet of Things: Security and privacy issues," Int. J. Comput. Appl. , vol. 90, no. 11, pp. 2026.

[22] S. Sicari, A. Rizzardia, L. A. Griecob, and A. Coen-Porisini, 2015. "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146164.

[23] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, 2017. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142.

[24] Moinet, A., Darties, B. and Baril, J.L., 2017. Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.

[25] Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L. and Janicke, H., 2018. Blockchain Technologies for the Internet of Things: Research Issues and Challenges.

[26] Rachmawati, D., Tarigan, J.T. and Ginting, A.B.C., 2018, March. A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012116).

[27] G. J. Pottie, W. J. Kaiser, 2000. "Wireless integrated network sensors". Communications of the ACM, Vol. 43, n. 5, pp. 51-58.

[28] Antoo, A. and Mohammed, A.R., 2014. EEM-LEACH: Energy efficient multi-hop LEACH routing protocol for clustered WSNs. In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 812-818). IEEE.