

IoT Privacy preservation using blockchain *

Chintan Patel¹[0000–0002–3824–6781]

Pandit deendayal petroleum university, Gujarat-382007, India
chintan.p592@gmail.com

Abstract. Internet of things security will be a big challenge for the enterprises working behind the build-up of the internet of things, and its application. With IoT, another buzzword is blockchain-based cryptocurrency bitcoin. Blockchain technology has proven itself as one of the most secured existing technology. In this paper, we have discussed the significant challenges that will come up in identity management due to the heterogeneity of devices. We have proposed a solution for privacy preservation using secure identity management and possible communication methodology by using public key-based cryptography used in the blockchain. We have taken the ecosystem of smart home management and smart health management. At last, we have concluded with the discussion of futuristic applications of blockchain in other applications of the internet of things.

Keywords: Blockchain · Internet of things · Public key cryptography · hash function · smart home · smart health.

1 An introduction

History of internet communication has shown significant growth in the last decade. Internet communication started with four nodes that had reached almost 50 billion devices. As per statistica analysis, the total number of connected devices will be more than 75.44 Billion by 2025. As mentioned in the report from technical firm Gartner[10], the total amount of the connected device has already reached 8.4 billion and had shown significant growth of more than 31% since 2016.

* Pandit deendayal petroleum university

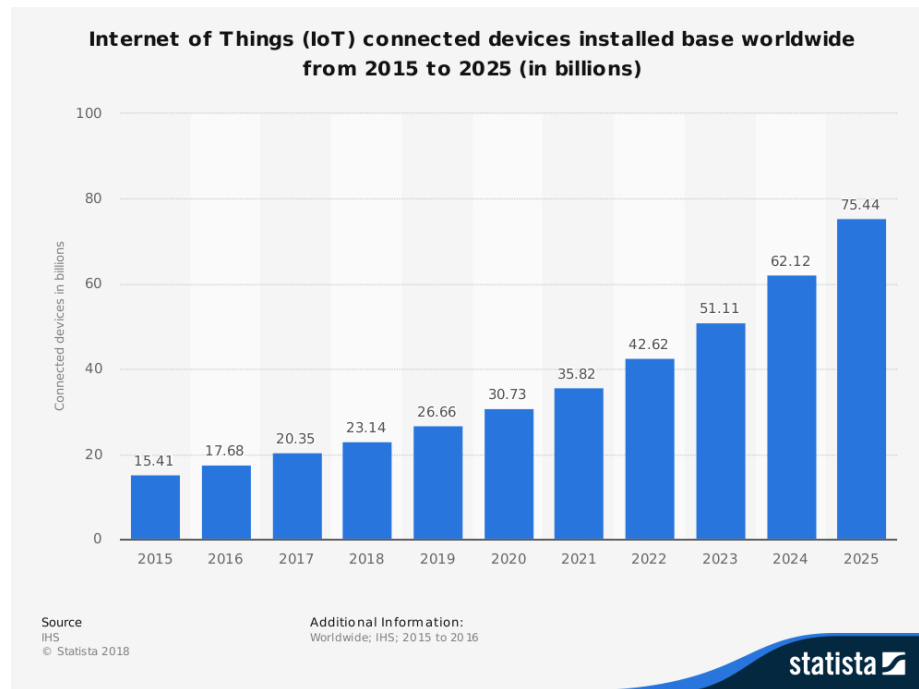


Fig. 1. Connected device statistics by statista[24]

In 2009, Kevin Ashton from MIT RFID lab had published a paper titled "That Internet of Things Thing" in the RFID journal[6], this paper has opened the door for the next revolution in the world of technology. CISCO, IBM, MICROSOFT, INTEL, and many other world giant enterprises have started work in the design and development of the Internet of things nuts and bolts. Nuts and bolts of the Internet of things include communication protocols required by smart and tiny devices, enhancement in capabilities of IoT devices, and manufacturing of working models for various IoT applications. Report by GSMA [7] has put on notice that growth on connected home devices was 67% in 2017 compared to 2016, and it is predicted that by 2022, every smart home will have an average 50 smart connected devices. Innovation on the Internet of things has started to show the impact of day to day life. Starting from the smart coffee maker in the home to smart air condition in the office. Smart wearable devices have created lots of impact in the healthcare services[3]. A recent report by IHS[14], A global data research firm, also predicts that the total number of connected devices will be 125 billion by 2030. As per shown in [14], IoT has four major pillars:

- **Connection** : Connecting billions of devices.
- **Collection** : Collecting trillion bytes of data.
- **Computations** : Computing collected data

- **Creations** : creating new solutions and standardization

The major generalized challenge in the internet of things that every industry has to focus on is "Standardization of IoT architecture and protocol." Due to the lack of universal standardization for identity allocation, every industry provides different in a different format. So currently, due to a limited number of devices, we don't face a problem in connecting these devices. In the future, a significant challenge will be the interoperability between these devices. To discuss the working model of IoT devices, we will discuss the famous seven-layered architecture proposed by CISCO[1], as shown in figure 2.

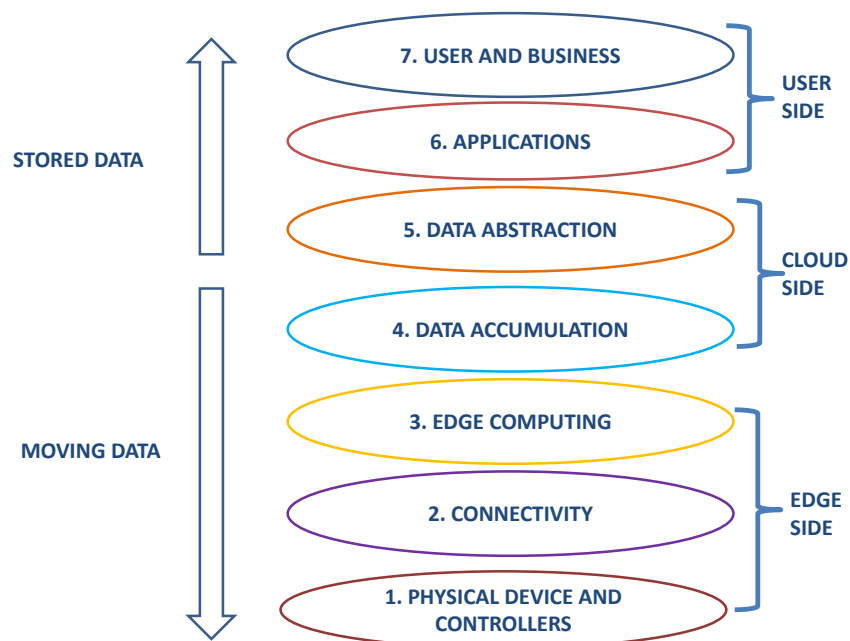


Fig. 2. CISCO 7 layered reference model[1]

1. **Physical devices and controllers:** This layer is also called a layer 1 of the internet of things in which ground level of devices will be deployed. Appliances can be smart sensors, sensor-based products, actuators, micro-processors, and micro-controllers. The primary work of this layer is to collect the data from the environment.
2. **Connectivity:** This layer is layer 2, which provides connectivity between layer one devices with layer 3, fog devices. This layer implements various short-range wireless protocols and long-range wireless protocols.

4 C. Patel et al.

3. **Edge computing:** Layer 3 of CISCO reference model shows fog computing[2], Fog computing is the technology introduced by CISCO with the aim of distributed data processing. It believes that let layer three devices of communication do some local data processing so that unnecessary data will be deleted and data mining will become easy.
4. **Data accumulation:** Layer 4 is the last layer in which data will be in movement. Data accumulation layers show the storing of IoT data into the proper server based on indexing.
5. **Data Abstraction:** Layer 5 is also called as knowledge generation in which collected data will be mined. They will be passing through various machine learning and artificial algorithms so that it can provide knowledge(decisive data).
6. **Application:** Layer 6 contains various applications developed at the server-side and accessed by users. An app like smart home, smart health, and so on. This layer works as an intermediary between mined data and users.
7. **Users and Business:** Layer 7 implements various mobile applications and web applications for individual users as well as business enterprises. It collects the data from the application server and makes decisions.

Major security challenges on the internet of things include:

- Device identity management
- Secure authentication
- Privacy and trust management

Recent attacks on the internet of things show that the biggest challenge for the internet of things is identity theft of the user and devices[2]. The identity of the device can relieve some of the important information about the device and location. Let us take an example of devices manufactured by XYZ organization than the identity of that device is given as /XYZ/year/model no. This information can help an attacker so that he/she can easily extract which type of devices is this, how much power it may consume, which type of data it may collect, what can be the purpose of the user to use this device. So the biggest and first important challenge is not to relive an identity of the devices in the internet of things. IoT device identity management will be part of the most focused agenda when we need to connect billions of devices developed by thousands of companies, either with security parameters or without security parameters. In this paper, we have tried to solve this heterogeneity and identity theft of IoT devices, which can lead to further development of the IoT ecosystem.

This paper is constructed as per the following outline. Section 2 discusses the blockchain technology. Section 3 focuses on blockchain user identity management and the necessary mathematical foundations required for the proposed scheme. Section 4 proposes an IoT device identity management scheme by using blockchain-based public key cryptography. Section 5 shows the use case of a proposed scheme for smart home application, and section 6 concludes this paper.

2 A blockchain introduction

In 1991, Stuart Haber introduced a chain which was secured by cryptography paper titled "How to time-stamp a digital document" but this came in notice while in 2008, An unknown person or group called as a Satoshi Nakamoto published one paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"[19], Nakamoto paper had introduced exciting and revolutionary product in currency world called as bitcoin. Bitcoin is the digital currency which makes use of immutable "blockchain" technology to perform a transaction. So if user A wants to transfer certain bitcoin to user B, then this transaction will make use of blockchain technology. The underlying motive behind introducing this new technology was:

- Peer to peer transaction
- Distributed database
- Trust and transparency creation
- Transaction security
- Non repudiation

The current financial transaction system depends on the banking system, which is the centralized system. All the transactions happen via the third party, and it has certain limitations like the double-spending problem, transaction delay, hacking of data and financial transactions, and high transaction fees. As per proposed blockchain technology by Nakamoto says that blockchain technology is peer to peer communication, so there is no third party that is involved in the conversation. A complete blockchain will be distributed in the form of cryptographically signed ledgers with all the participants in the system. The blockchain is the chain of blocks, and each block contains transactions performed by various users. In the initial days of the blockchain, the block size was 36MB[9], and it was capable enough to deliver 100 to 120 transactions per second. Still, due to support multiple users and tackle with denial of service attack, the block size was reduced to 1 MB and 4-6 transactions per second. As per the report on blockchain technology by the national institute of standard and technology[28], Blockchain technology has three types of nodes:

1. **Full node:** Which contains complete blockchain and ensures that newly added blocks are valid blocks. It forwards received blockchain to all neighbor nodes.
2. **Mining nodes:** Mining nodes are considered as a regulator of the blockchain system. They validate and verify each transaction. Mining nodes solve a cryptographic puzzle, utilizes their resources, and get a right to creating blocks.
3. **Lightweight nodes:** Lightweight nodes does not store blockchain. This node doesn't validate anything. These nodes just generate requests and forward this request to the full node for further processing.

6 C. Patel et al.

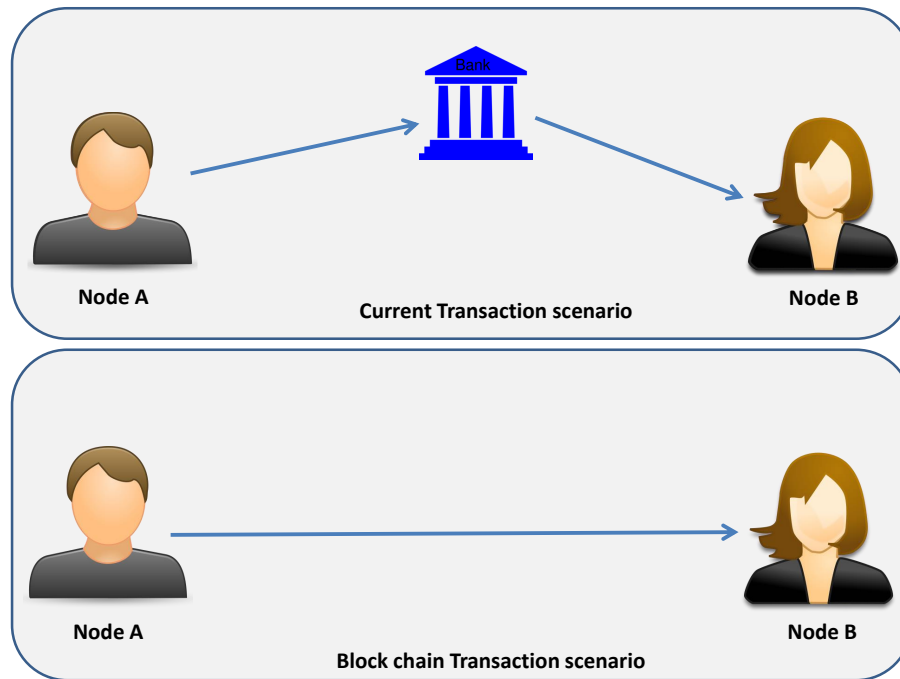


Fig. 3. Current financial system vs blockchain

blockchain technology was introduced with 3 types of blockchain:

1. **Public blockchain:** In this blockchain system, every user can see the complete ledger, and any user can verify the block and add a chunk of the transaction in the system. Any user can join blockchain at any time. Bitcoin and ethereum make use of public blockchain
2. **Private blockchain:** In this blockchain, only permitted users can write a block, but every user can view the blockchain. Access to permission granting is centralized to a particular organization. The multi-chain makes use of private blockchains.
3. **Consortium blockchain:** In this type of blockchain, A complete system is controlled by a group of nodes or groups of organizations. They don't allow any operation to any outside node. CORDA[8] uses this type of blockchain system.

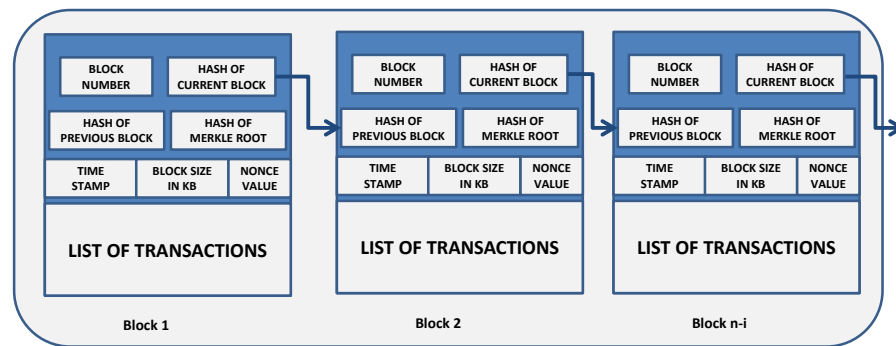


Fig. 4. blockchain

As per shown in figure 4, Every block in blockchain basically contains 8 items:

1. **Block No:** Block number or block height is the decimal number, which represents as an identity or counter for a number of blocks in the blockchain.
2. **Hash of current block:** Hash of the current block is computed and stored inside the block, which helps another node in the validation of block.
3. **Hash of the previous block:** Hash of the last block is also a part of the current block, so if any alteration occurs in the previous block, then all the subsequent blocks hash value will be impacted and will not allow validation of block.
4. **Hash of Merkle root:** Merkle tree is a data structure in which data is stored after subsequent hashing operation. Example: Let us assume we have 4 data messages, {Data0,Data1,Data2 and Data3} Than:
 $H0 = \text{Hash}(\text{Data0})$
 $H1 = \text{Hash}(\text{Data1})$
 $H2 = \text{Hash}(\text{Data2})$
 $H3 = \text{Hash}(\text{Data3})$
 $H01 = \text{Hash}(H0, H1)$
 $H23 = \text{Hash}(H2, H3)$
 $\text{Root} = \text{Hash}(H01; H23)$
Merkle root value makes sure that any alteration occurred in the transaction will impact the current block as well as all subsequent blocks. So root ensures the validity of the transaction.
5. **Time stamp:** Timestamp is the time of block generation.
6. **Block size:** Size of the block in including a list of transactions and block header.
7. **Nonce value:** Nonce value is the one time used value with the help of which miner has solved the cryptographic puzzle of ensuring x number of zeros in the initial value of the hash.

8. **List of transactions:** List of the transaction is the ledger of all validated and verified transactions.

Blockchain technology makes use of public-key cryptography to digitally sign each transaction and hash function to ensure that no one can alter or delete any single bit of value in the block. Example: Let us say user A wants to send five bitcoin to user B, then A will generate the request which contains sender public key, receiver public key, and the number of bitcoin he is interested to send.

This will generate message $M1 = \{K_{puA}, K_{puB}, 5\}$ and Message $M1$ will be hashed and $M2$ will be generated by $M2 = E_{K_{PrA}}(M1, H(M1))$ and $M2$ will be transmitted to miners so miners will validate this transaction and add it into currently running block. Over here K_{puA} and K_{puB} are the public key of A and B while K_{PrA} is the private key of user A. Every transaction in blockchain will be validated so that double-spending problem will not be possible.

The transaction will be verified by multiple miners, so even if any miner will change the value in the transaction, then the user will get a different copy for same transaction block, so users will keep the copy of miner who has created currently running block and keep trust on that miner. "Genesis block" is the first block of each blockchain, and this block is created with mutual understanding between all the users of the system. These users will also decide the consensus model, which helps them to work with mutual understanding.

Every mining node will get an incentive for the successful creation of the block. Still, to create a block, mining nodes need to solve a cryptographic puzzle, which is a time-consuming and resource-consuming process. As per shown in [18], Let us assume miners have to find a hash value where first six digits of hash value should be zero, and it makes use of SHA256 algorithm than hash is computed as follow:

$$\text{Hash} = \text{SHA256}(\text{"blockchain", Nonce value})$$

User will continuously update nonce value for that much time till it gets hash value like $\{f0x000000xxxxx.....g\}$ so for to solve 6 zero puzzle user needs at least 54 seconds to find this, which if single zero is increased means rather than 6 zero, if 7 zero puzzles are created than the same system needs more than 1 hour, so difficulty increases with increase in number of zeros and time and resource consumption also increases[28]. The current blockchain for bitcoin makes use of 18 zero puzzles so that no same miner can generate block individually within one day.

Many times multiple miners come together and try to solve this puzzle and later on share the incentive of block generation. Designing and development of green blockchain or energy-efficient blockchain will surely be hot topic for researcher because currently blockchain technology in bitcoin uses power for single transaction which is equal to 1.57 household in the USA and 5000 times more energy consumer than single credit card transaction so blockchain transaction reduces cost for users in terms of less transaction cost but will increase energy cost for the country[21].

3 A Consensus model

The consensus model is the way trust-based data inclusion happens in the blockchain. It assures that the next block is the valid one by using specific consensus algorithms. Consensus algorithms inspire a group of nodes to work together to solve a similar problem, and each node trust on each other. Some famous consensus algorithms are as follows:

1. Proof of work[19]:

- Proof of work consensus model was introduced in 1993 by Cynthia work and Moni Naor, and that was used by Markus Jakobsson in 1999[16]. Satoshi Nakamoto, in his paper on bitcoin[19] makes use of Proof of work consensus model.
- Proof of work became the most famous consensus model after rapid bitcoin growth. In this consensus model, multiple blockchain miners will play in a competitive environment for the creation of a new block. The one who will solve the cryptographic puzzle first will get the incentive.
- Bitcoin consensus model provides 12.5 bitcoin to block creators. Proof of work inspires the mining node to work collaboratively.
- Proof of Work ensures that every node must perform a task, and they do not have any shortcut to implement this model. We can consider this property as an advantage when we want fairness in a system, and we can consider the same property as a disadvantage when it comes to resource and time utilization.

2. Proof of stake[25]:

- In 2011, A public forum named bitcoin talk lightened about Proof of stake. Some of the cryptocurrencies like Peercoin[25], NavCoin, Blackcoin[?] makes use of Proof of stake.
- Proof of stake work on the principle of how much stake or wealth you currently hold, If you hold x% of currently generated currency than your chance of getting selected for block creation is x times out of each 100 times.
- Proof of stake removes unnecessary utilization of resources in puzzle solving. In Proof of work, miner nodes were receiving an incentive for block creation while in Proof of stake, the mining node will not receive any excuse, so the will charge for transaction validation and implementations.
- In Proof of work, if 51% resources are available with malicious node than it can create the block and it may be possible if big organization with data centers try to implement it, but in Proof of stake, malicious node need to get 51% stake to perform larger attack and to obtain 51% of currency is complicated task.
- "Chain based proof of stake" method is based on the random selection of blockchain.
- Proof of stake consensus model makes it more productive and most difficult for newly entered miners.

3. Proof of activity[15]:

10 C. Patel et al.

- proof of activity is based on a combination of operations in Proof of work and Proof of stake.
- Miners will solve the cryptographic puzzle and generate a block template that contains header information and the reward address of miners.
- Now, Proof of stake method will randomly select a group of block validators (Miners) based on stake how much stake (Cryptocurrency) they have. The one who will have more currency will have more chance of random selection, and they all will validate this block. After the validation block will be publicized.
- Decree is a cryptocurrency, which makes use of proof of activity-based consensus model.

4. Round robin based[12]:

- Rather than implementing complex mechanisms for block creation, the Round-robin based consensus model works based on the concept of private blockchain in which some nodes will work as moderators of the system and that every node will get chance of block creation in turn by turn.
- If any node is not available when it turns comes, then that randomly next node will be selected for block creation.
- Round robin model is suitable in the permission-based environment, and it is not a suitable option for a permissionless environment; otherwise, it may suffer from a "false block creation attack."

5. Proof of capacity[4]:

- proof of capacity model is also called a space availability based model in which the node which has more space available in memory will get a chance of block-creation.
- proof of capacity will generate significant data set called as plots and node which can store a high number of plots in their memory will get an opportunity of block-creation.
- So big data center which can store zeta bytes of storage or thousands of Terra byte storage can make use of proof of capacity based consensus model.

6. Proof of authority[20]:

- Provides quick and continuous trust in the real-time implemented network.
- "Validators" are the authorized entity that has access to the chain. The validator can approve the transaction and create the block.
- Identity is the stake of the validator. Proof of authority is one of the best options for the permissions network.
- No need of mining and same stake, so better than a proof of work and proof of stake.

So up to 2015 end, most of the people were thinking that blockchain can be used in only financial transaction systems. Still, recently, certain research opens a gate to utilized secure, transparent, decentralized, and distributed systems for other applications. In these applications, we firmly believe that the internet of things will come up as a bigger adopter of blockchain technology.

4 blockchain and IoT

Blockchain technology has proven itself as one of the most secure technology in the financial world due to properties like decentralized database and decision making, public key-based identity verification, hash-based identity management, consensus-based data creation. Internet of things aims to connect billions of devices to achieve the common goal of connecting "Anythings" at "Any time" at "Anywhere." Major challenges internet of things based devices, services, and applications will get in the future are as follows:

- IoT device identity management
- IoT eco-system management
- IoT device and data security
- Handling heterogeneity of devices developed by global industries in the environment of uncommon standardization.

So these are some major challenges that will be lightened in the future that we believe. In the future, the most important question will arise about handling or storing the identity of devices in the communication packet due to a lack of standardization in device identity allocations. Blockchain technology can play an important role in smart health-care for privacy preservation for a patient. Key management for privacy preservation in health care is proposed in [29]. The government can use blockchain technology in the agriculture sector for accurate crop production tracking, fertilizer vs. production ratio analysis, weather prediction, crop disease analysis, and many more. Another primary use-case of blockchain technology is inland record monitoring, in which many government agencies are working so that land transactions can be tracked in an immutable way. Blockchain technology can play a significant role in transparency establishment for defense deals and provide strength to inventory management. A private blockchain can play a vital role in industrial asset[18] management, asset tracking, product quality analysis, production payment system, and human resource management. Various use cases where document verification is so much crucial aspect, blockchain technology can replace the physical documents with its immutable records storing technology[27]. Blockchain technology will lead to the creation of trust-building and transparency of operations. It can help to detect which device has initiated which operation or have publicized which data so, later on, to verify data generation or validation of operational activity will be more comfortable. Global rm international data corporation(IDC) in their report titled "IDC FutureScape: Worldwide IoT 2018 predictions" [26] has predicted that By 2020, more than 10% blockchain ledger will include IoT sensors. In the 2017 report[17], IDC predicted that by 2019,20% of IoT services will be enabled with blockchain technology.

Fabio Antonelli[5] published the report on blockchain and IoT; in this report, he mentioned that immutable transaction recording could be widely accepted technology in the applications where asset monitoring, product tracking, financial and order tracking is required. Industries making use of IoT applications like smart logistics, smart supply chain, smart retail can adopt this technology

for their business monitoring. In the same report, he predicted that by 2021, the blockchain market size would grow by 2312.5 million dollars.

In 2016, Siva Gopal from tata consultancy service published white paper[11] titled "Blockchain for the internet of things." In this report, he pointed out that blockchain can be one of the most useful technology for the internet of things applications where transparent information sharing is required. RFID data, sensor data, Bar-code information, and much other information can be shared on the public ledger. The author has directed four benefits of accepting blockchain in IoT, and it includes: Soup to 2015 end, most of the people were thinking that blockchain can be used in only financial transaction systems, but recently certain research opens a gate for to utilized secure, transparent, decentralized and distributed system for other applications. In these applications, we firmly believe that the internet of things will come up as a bigger adopter of blockchain technology.

Blockchain technology has proven itself as one of the most secure technology in the financial world due to properties like decentralized database and decision making, public key-based identity verification, hash-based identity management, consensus-based data creation. Internet of things aims to connect billions of devices to achieve the common goal of connecting "Anythings" at "Any time" at "Anywhere." Major challenges internet of things based devices, services, and applications will get in the future are as follows:

- **Trust building:** Improve the trust between devices and intermediate communication.
- **Cost reduction:** Peer to peer communication reduces the overhead of connection establishment and destination-specific communications.
- **Accelerate data exchange:** Peer to peer contracts will reduce the time required for device information exchange.
- **Security for IoT:** Decentralized technology can help in building a secure environment.

Authentication is one of the most important security challenges that lie in the IoT. Major internet of things devices is resource-constrained, so security algorithms for IoT devices must be able to run on 256 KB ROM and 128 KB RAM. For any IoT devices, we can allocate a maximum of 20% resources for security purposes, and the remaining 80% must be used for core functionalities of devices.

Various cryptographic capabilities available in blockchain can be used for IoT by combining lightweight security techniques like physically unclonable function or precision coding. Blockchain makes use of the SHA hash function to maintain the integrity of the transaction, auditability, transparency, and user identity. It makes use of elliptic curve digital signature algorithms for authentication of the transaction. So we can use this technique for IoT device identity management and data integrity using a combination of the public and private blockchain.

5 A mathematical foundations

5.1 One way hash function:

One way hash function can be defined as $H : X \rightarrow Y$ where X is any size plain text input, and Y is fixed-size hash text value. One way hash function has the following properties:

- If X is given, then it is easy to compute Y .
- If Y is given, then it is impossible to compute X .
- For any different input value of X and X' , if the hash value is Y and Y' , then it is not possible to find any pair of $Y = Y'$.

Blockchain technology implemented in bitcoin makes use of the Secure Hash Algorithm(SHA-256). For any value of X , SHA256 will give a 256-bit value of Y .

5.2 Elliptic curve digital signature algorithms:

An elliptic curve is a curve with the polynomial expression:

$$Y^3 = (X^2 + aX + b) \bmod n$$

In this polynomial equation, $P(X, Y)$ is the pair of coordinate locations for any point on the curve. P is the point defined prime field F on which curve is defined, and n is the large prime number as well as is the order of point P . Value of a and b must satisfy the following equation:

$$4a^3 + 27b^2 \neq 0$$

Now let us consider point P on the elliptic curve and elliptic curve equation is publicly available if Sender A wants to generate key pair than it chooses random integer d from the range of 0 to $n-1$ where n is greater than 2160 for curve P-160. Now A will compute the following operation:

$$Q(X,Y) = d * P(X,Y)$$

Where $Q(X, Y)$ is a public key, and d is the private key for the user A . so the pair of (public key, private key) = $(Q(X, Y), d)$. Now to sign the transaction TX , user A will generate a set of domain parameter(D), which contains seven tuples, $D = (q, FR, a, b, Gn, h)$ where q is the size of the field on which curve is defined. If we use a prime field, then q is similar to p and if we use binary field than $q = 2^m$. FR is a field representative, a and b are constants of an elliptic curve. Gn is the point on the curve, which is generated by finite point $Gn = (Gx, Gy)$, n is the order of point G , and cofactor h is the order of curve divided by n . Now let us compute signature generation for transaction TX :

- $Q(X,Y) = d * P(X,Y)$
- Generate random number k of length of d

14 C. Patel et al.

- $(X_a, Y_a) = k * P(X, Y)$
- $r = X_a \bmod n$
- $s = (H(TX) + r*d) * k^{-1} \pmod n$

so pair (r, s) is the digital signature for TX. Now let us compute signature verification by receiver.

- $w = s^{-1} \bmod n$
- $u_1 = H(TX) * w \bmod n$
- $u_2 = r * w \bmod n$
- $(X_b, Y_b) = u_1 * P(X, Y) + u_2 * Q(X, Y)$

so if $r = X_b \bmod n$ then we can say that signature is validated.

5.3 blockchain user identity management:

The most beneficial aspect of blockchain technology is that it does not reveal the identity of any users. In blockchain-based financial transactions, user identity is calculated in the following way:

Let us say that there are n users involved in peer to peer network, $\{U_1, U_2, \dots, U_n\}$, then $K_{PUB_{U_i}}$ and $K_{PRIV_{U_i}}$ is the public and private key pair of user i . In cryptocurrency, whenever a user registers with a cryptocurrency wallet, then the wallet will generate the private and public key pair. So identity, as well as address of user i in the system, will be:

$$\text{identity}(i) = H(K_{PUB_{U_i}})$$

Hash function of the public key of the user will be considered as an identity and address of the user. So everyone who has blockchain can see the $\text{identity}(i)$ as well as can computer also. Still, they can not get any other information about the user like name, place, bank account number, bank identity, and so on. Due to the immutable properties of blockchain technology, no one can alter the hash value of any user identity. So the major advantage is the immutable record and unreadable identity.

6 A Proposed IoT device identity management

IoT device identity is the most important parameter in terms of security due to the following reasons:

- As shown in the survey[23], less than 10% IoT devices are secured, and most of the device identities are open.
- IoT devices identity reveals information about the product used by the customer, and it may damage the privacy of a person.
- Sending IoT devices in plain text or encrypted text, both are dangerous aspects of communications.

- Most of the authentication schemes proposed by researchers or used by enterprises communicate the identity of devices either in plain text or encrypted text.

In the proposed identity management scheme, none of the devices will communicate identity during any phase of communication.

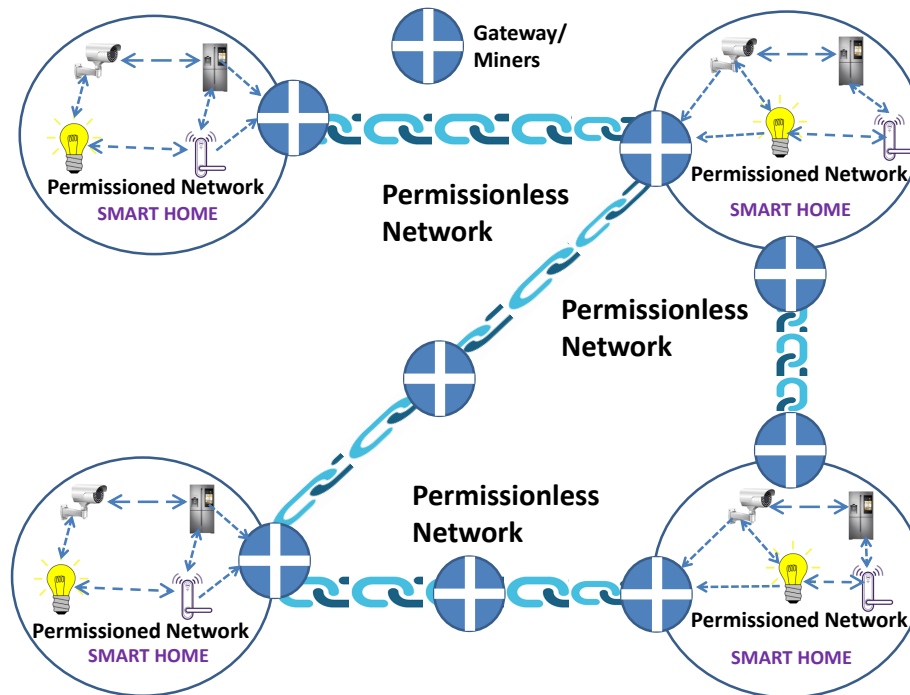


Fig. 5. Smart home blockchain

As seen in figure 5, Smart home communication using blockchain pass through two types of blockchain. Permissioned blockchain and permissionless less blockchain. Permissioned blockchain is the blockchain that is controlled by some authority and only permitted devices can be part of it while permissionless blockchain is open blockchain and any device can join it. In smart home communication, there will be a combination of this; both, communication between devices inside the home will be through permissioned network, and external communication will be through the permissionless network. We need to make use of two types of consensus model for our communication,

- Proof of authority consensus model for permissioned network
- Proof of work consensus model for the permissionless network.

Proof of authority model will provide rights to validators inside the home, which can work as a miner, validator, verifier, and local data store. Proof of work consensus model is discussed in [19]; Public miners will work as block creator, validator, and verifier. Smart home blockchain communication will be completely different in permissioned and permissionless network. Over here, we will focus on the permissioned network, and it's communication.

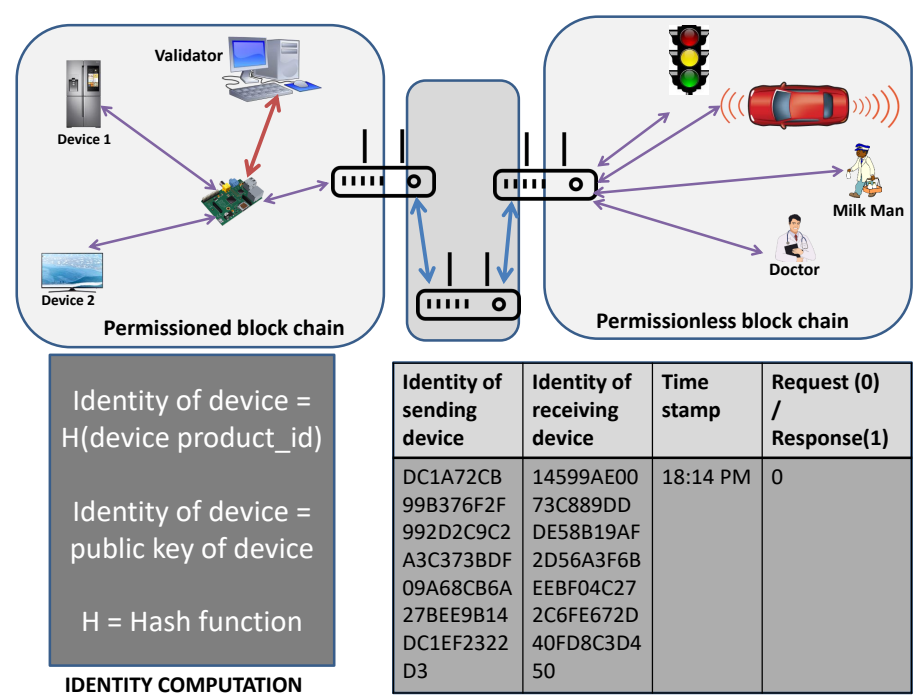
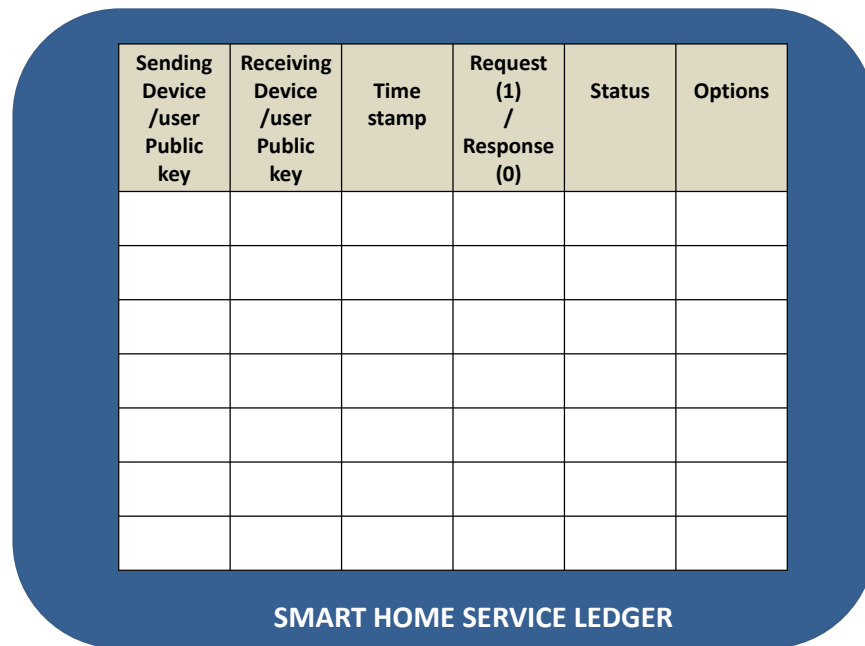


Fig. 6. Identity and Published message in smart home

Every device inside the smart home or any IoT network will have some unique identity, and through that identity, it makes use of communication. Message queuing telemetry transport(MQTT) makes 23 bytes or 184 bits identity for each device, Most of the MQTT based communication protocols make use of 48 bit MAC address of the device for their communication or directly use the device location hierarchy like URL for the communication with sequence numbers. Both the type of communication reveals information about the device. Similarly, all other communication protocols for IoT don't have any specification about managing the identity of devices outside the network. More than 90% of developed devices communicate securely due to the uncertainty of identity management for devices.

As shown in figure 6, proposed identity management needs only one hash computation facility or hash digest size storage at each device that works as a service generator or service seekers. Every device which is part of the smart home network will compute the identity of the device, Identity of device = Hash(device product id), or Identity of device = Hash(/city/area/street/home/product id). The hash function used for communication will be SHA-1 and will generate the 160-bit digest. Based on the communication protocol, the identity of the device can be computed, compressed, and communicated. Packet(or smart home transaction) will look like as shown in figure 6, It will contain identity of the sending device, identity of receiving device, timestamp (contains synchronized time of request or response generation) and 1 bit is either its request or response, for request value will be set to 0 and for response value will be set to 1.

Later on, this transaction will be forwarded to validator or also called as home miners, and Home miners will validate identity or both sender and receiver, it will verify whether they are part of this communication blockchain or not. After validation and verification, it will digitally sign this transaction. To sign this transaction, the home miner will make use of elliptic curve-based digital signature protocols. Elliptic curve digital signature for transaction TX ($EC_{DS_{TX}}$) is encrypted using the public key of receiving the device and store this message in the block, as shown in the following format.



Sending Device /user Public key	Receiving Device /user Public key	Time stamp	Request (1) / Response (0)	Status	Options

SMART HOME SERVICE LEDGER

Fig. 7. Ledger in in smart home blockchain

So will contain transaction, as shown in figure 7, status, and options, are two other parameters that block contains. The status may have two possible values,

- 0 indicates an active transaction.
- 1 indicates complete transactions.

Whenever the receiver also generates the response transactions, miners from the permissionless network may add transactions and verify the current status; if the current status will active, and it's the message from the valid receiver, then it will convert the transaction to finished. It depends on either

1. Receiving device belongs to the same permissioned network. OR
2. Receiving device belongs to the permissionless network.

If receiving device belongs to same home permissioned network than same miner or validator will forward this transaction and will add response transaction while if it belongs to permissionless network than receiver device will generate response message and will forward that message to home miners on internet, due to hash value of both device, no one can understand the identity of device.

7 More IoT application using blockchain

Parallel computations, enhanced efficiency, risk reduction, and automation capabilities to implement business logic are the key futures which attracted researchers to focus on blockchain technology. The absence of a trusted third party and smart contracts are bases for the major attraction from both research and enterprise community. Some of the IoT applications of blockchain listed in the article wrote by Nelson from TIBCO Software Inc[22] are as follows:

- Smart manufacturing
- Insurance claims
- Apartment rental
- Airline compensations
- Government land record tracking, contract management, tender process.
- Smart energy distribution.
- Healthcare and pharmacy

Blockchain technology can also be used in authentication validation, sensor-based authentication[5]. IBM has joined hands with Samsung and started a project called ADEPT(Autonomous decentralized peer-to-peer telemetry). Smartmatic introduced the project "blockchain-based voting system." IBM blue mix started to allow hosting of blockchain-based applications[11]. Similarly, there are many use cases that are initiated with the motive of a combination of blockchain and IoT. With the help of blockchain, other financial activities like portfolio management, equity distribution, bond tracking, letter of undertakings, mutual funds, pensions, derivatives, and bonds can be easily tracked. The government can make use of blockchain technology to track social initiatives and to enhance transparency inside government funding. Large technology firm IBM has allotted more than 200 million dollars to initiate research on blockchain-powered IoT. IBM handshake with Kinno to develop "supply chain tracking capabilities," which will track, report, and monitor packing.[13]. So blockchain can open many more doors for IoT enabled, cloud-based, distributed related applications.

8 Conclusion and future work

In this paper, We have focused on the internet of things and blockchain technology. Blockchain technology is highlighted due to its security features. Recently many cryptocurrency wallets are attacked but no attack till now founded in blockchain technology. A distributed ledger, peer to peer authentication, no third party communication, and trusted consensus models have attracted many researchers to find out the way through which other technology also gets benefits of blockchain technology. In this paper, we have focused on the identity management problem of the internet of things. We have not discussed complete ledger and communication of IoT application using the blockchain, so as future work on this paper, we will come up with complete IoT application inducted with blockchain technology. Identity management discussed in this paper in a

smart home will open many other ways for the researcher to apply it to smart health, smart logistics, smart retail, smart manufacturing, and so on. Some of the challenges that may come up when we try to implement blockchain in IoT type resource-constrained devices, the major challenge in the blockchain is to reduce computation and resource requirement to store blockchain so as a future scope, researcher community needs to focus on this two aspects also parallel with application-oriented development.

References

1. The internet of things reference model (2014), <http://cdn.iotwf.com/resources/71/IoT-Reference-Model-White-Paper-June-4-2014.pdf>
2. Beware! data and identity theft in the iot (March 2016), <https://www.globalsign.com/en/blog/identity-theft-in-the-iot/>
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials* **17**(4), 2347–2376 (Fourthquarter 2015). <https://doi.org/10.1109/COMST.2015.2444095>
4. Andrew, P.: What is proof of capacity? an eco-friendly mining solution (January 2018), <https://coincentral.com/what-is-proof-of-capacity/>
5. Antonelli, F.: Blockchain and Internet of Things : Why a Perfect Match About me ... (2017), www.iothingsmilan.com/wp-content/uploads/2017/05/Antonelli.pdf
6. Ashton, K.: That “internet of things” thing **22**, 97–114 (01 2009)
7. Bouverot, A.: The impact of the internet of things, the connected home (November 2017), <https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf>
8. Brown, R., C.J.G.I., Hearn, M.C.: An introduction, whitepaper (August 2016), <https://www.r3cev.com/s/corda-introductory-whitepaper-final.pdf>
9. Caffyn, G.: What is the bitcoin block size debate and why does it matter? (August 2015), <https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/>
10. Gartner: Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016 (2017), <https://www.gartner.com/newsroom/id/3598917>
11. Gopal, S.: Blockchain for the Internet of Things. Tech. rep. (2016), <https://www.tcs.com/blockchain-for-iot>
12. Greenspan, D.G.: Multichain private blockchain “white paper (July 2015), <https://www.multichain.com/download/MultiChain-White-Paper.pdf>
13. Higgins, S.: Ibm invests 200 million in blockchain-powered iot (2016), <https://www.coindesk.com/ibm-blockchain-iot-office/>
14. Howell, J.: Number of connected iot devices will surge to 125 billion by 2030 (October 2017), <https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says>
15. Iddo Bentov, Charles Lee, A.M.M.R.: Proof of activity: Extending bitcoin’s proof of work via proof of stake (March 2013), <https://eprint.iacr.org/2014/452.pdf>
16. Jakobsson, M., Juels, A.: Proofs of Work and Bread Pudding Protocols(Extended Abstract), pp. 258–272. Springer US, Boston, MA (1999). <https://doi.org/10.1007/978-0-387-35568-9-18>, <https://doi.org/10.1007/978-0-387-35568-9-18>

17. Macgillivray, C.: IDC FutureScape : Worldwide Internet of Things 2017 Predictions (oct 2017), <https://www.idc.com/url.do?url=/getFile.dyn?containerId=US43193617...>
18. Miller, D.: Blockchain and the internet of things in the industrial sector. IT Professional **20**(3), 15–18 (May 2018). <https://doi.org/10.1109/MITP.2018.032501742>
19. Nakamoto, S.: Bitcoin : A Peer-to-Peer Electronic Cash System pp. 1–9 (2008), <https://bitcoin.org/bitcoin.pdf>
20. Naumoff, A.: Why blockchain needs “proof of authority” instead of “proof of stake” (April 2017), <https://cointelegraph.com/news/why-blockchain-needs-proof-of-authority-instead-of-proof-of-stake>
21. Opray, M.: Could block chain based electricity network change the energy market? (2017), <https://www.theguardian.com/sustainable-business/2017/jul/13/could-a-blockchain-based-electricity-network-change-the-energy-market>
22. Petracek, N.: Beyond bitcoin:what to do with blockchain? (2017), https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_497577.pdf
23. Seals, T.: Less than 10https://www.iotsecurityfoundation.org/survey-less-than-10-of-iot-devices-keep-data-secure/
24. statista: Iot statistics by statista (November 2016), <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
25. Sunny King, S.N.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake (August 2012), <https://peercoin.net/assets/paper/peercoin-paper.pdf>
26. Turner, V., Macgillivray, C.: IDC FutureScape : Worldwide IoT 2018 Predictions (2018), <https://www.idc.com/url.do?url=/getFile.dyn?containerId=US43193617...>
27. Universa: Blockchain in education (May 2018), <https://medium.com/universablockchain/blockchain-in-education-49ad413b9e12>
28. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain Technology Overview Blockchain Technology Overview. National institute of standards and technology pp. 1–57 (2018)
29. Zhao, H., Bai, P., Peng, Y., Xu, R.: Efficient key management scheme for health blockchain. CAAI Transactions on Intelligence Technology **3**(2), 114–118 (2018). <https://doi.org/10.1049/trit.2018.0014>