2nd International Conference on Advanced Computing and Communication Engineering (ICACCE-2018)
Paris, France 22-23 June 2018

Role and Applications of IoT in Online Transactions using Blockchain Technology

Akash Shandilya
Amity University
Uttar Pradesh
Noida, INDIA
akash.shandilya@live.co.uk

Himanshu Gupta
Amity University
Uttar Pradesh
Noida, INDIA
hgupta@amity.edu

Sunil Kumar Khatri
Amity University
Uttar Pradesh
Noida, INDIA
skkatri@amity.edu

***Abstract*—IoT is one of the leading technologies apart from blockchain that is being worked on to develop more consumer friendly devices which can help in the daily chores to perform more important and necessary actions, but as we know all the malware and security concerns which can hamper the growth of IoT based devices, we need blockchain technology to reinforce the devices as blockchain has proved it's worth as a security door which is unbreachable. The use of peer to peer communication between the IoT devices will make transactions more secure and user friendly while being fully precise. With these things in place we can see automation in household work or reduction in piracy via internet, the proper integrated use of IoT with our household devices or phones and digital devices will make our lives better and more convenient while being able to sustain more resources for the future. In current scenario, the biggest challenge is that how will Online Transactions get better and automated if we implement IoT using blockchain technology to improve the efficiency, transparency and security? In this paper we are trying to make our online transactions much more accessible and autonomous to interact whole being highly secure so as they can be integrated in the new gen smart homes systems and the home security systems, blockchain is the key to this need that we need to integrate with IoT to make our transactions more objective centered and have our payment system autonomous to make interactions with the daily services monitored by a IoT based smart device ecosystem more hassle free and fully secured. For this we will be going through the mining of blocks and their suggested applicability in the IoT ecosystem.**

Keywords: IoT, Blockchain, Ecosystem, Mining, Transactions, Autonomous, Convenient, Computation.

I. INTRODUCTION

Blockchain technology is gaining rapid popularity and is being used for Bitcoin and in many other sectors like finance, real estate, government sector, music industry due to it being able to operate in a decentralized fashion, without the need for a central authority. Its biggest advantage is that it is public; Everyone participating can see the blocks and the transactions stored in them. However, that doesn't mean everyone can see the actual content of a transaction; that information is protected by a private key.

The blockchain conceivably removes the middleman for these types of transactions. Personal computing ended up available to the overall population with the development of the Graphical User Interface (GUI), which appeared as a "work area". Essentially, the most common GUI devised for the blockchain are the so-called "wallet" applications, which individuals use to purchase things with Bitcoin, and store it alongside different cryptographic forms of money.

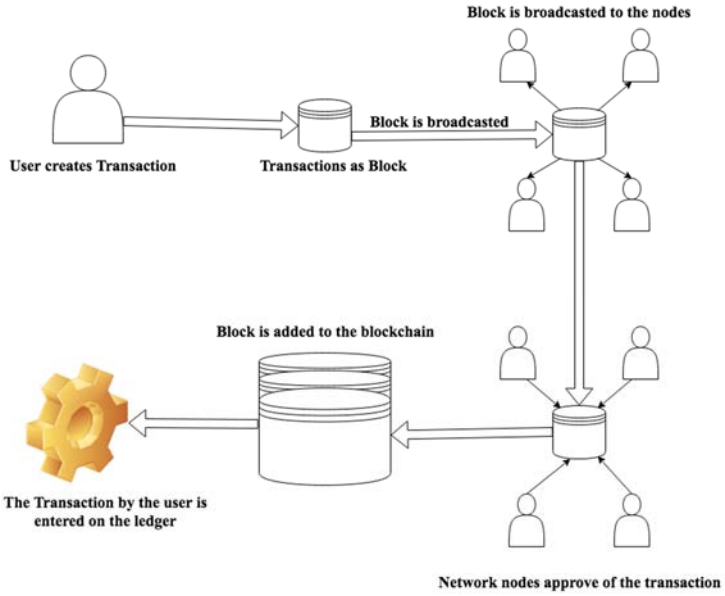

Fig. 1 : Working of Blockchain and Cryptocurrency Transfers[1]

The above diagram reflects the working process of Blockchain, how it is made and its functionality. The following steps will help better understanding the basics of Blockchain:

- Person A has to send money to person B who is on a different continent.
- A decides to send money and the first block is created in the process and to help guarantee honesty all through the blockchain,each piece's hash will be a cryptographic hash of the block's index, timestamp, data, and the hash of the previous block's hash.
- The block is then broadcasted to every party or node that is present in the network.
- The people or party be it autonomous or identified then approve of the transaction or the smart contracts are put to use.
- The block is then added to the chain with the data to provide a permanent, non-reversible and transparent record of the transaction.

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been doled out an IP address and can gather and exchange information over a system

978-1-5386-4485-0/18/$31.00 ©2018 IEEE

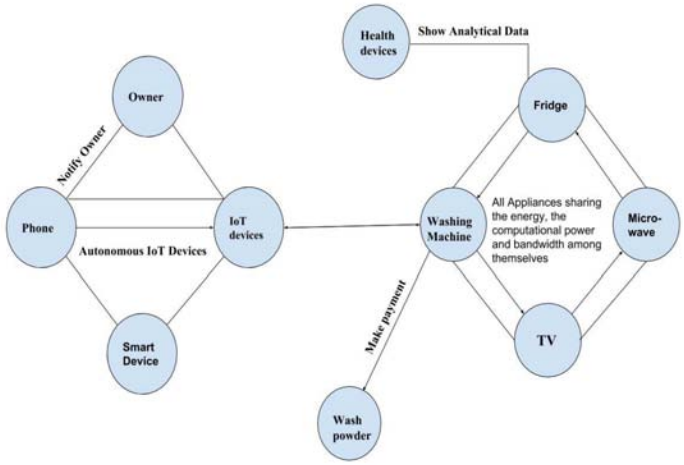

Fig 2 : Standard IoT devices interacting with each other and coordinating to provide services automatically.

The above diagram demonstrates the working of the autonomous IoT model with all the devices managing the network.

The Fridge, Microwave, Washing Machine and TV are balancing the energy, the computing power and the bandwidth among themselves. The Fridge is synced with the health devices for data related to calorie intake and the burned calories for diagnosis.

The Washing Machine will detect the depleted amount of washing powder and will make order for the same with prepayment. The phone will be connected to the smart watch and will be available for the user to add trusted devices or authenticate the untrusted ones for single time use.

On every purchase or task completed the smartwatch and the smartphone will notify the Owner. But the IoT model doesn't come without the risks of security. The Centralized system in which the security of the IoT model works is not the best of the security systems available.

The utilization of blockchain in IoT can bolster IoT applications. It can be configured to work securely and dependably in view of its condition. Individual blockchain is configured to do clients' verifications that is authentic among devices, making and recording securely the activity subtle elements, and making brilliant contract in view of IoT situation.

Blockchain will provide enhanced device security through implementation of a specific authentication scheme by applying a Quantum Random Number to eliminate possibility of hacks occurring. Beyond the human pay, which can be utilized after the creation of blocks allows one to provide the currency their devices can use. The platform acts to support micro-transactions with state-of-the-art hardware wallets immune to virus.[5]

The paper is divided into sections for better understanding of the applicability of Blockchain in IoT for online Transactions:

1. Methodology provides detailed insights of the hypothetical working of the model and the creation of blocks.
2. Results will be evident after the systematic display of the methodology.
3. Final Conclusions will be made with respect to the present trends.

II. METHODOLOGY

For creation of the first block on the blockchain we will have to create a Rig or a ASIC(Application Specific Integrated Circuit) that has enough computation power to guess the hash value which is less than the target hash value on the previous blockchain ledger.

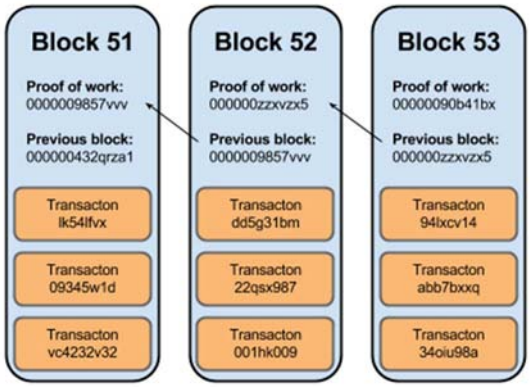

Fig. 3 : Blocks in the Blockchain with the hash values.

The creation of the blocks can be explained in the steps below:

1. Use of a ASIC or a computational rig that can handle the computation power for mining a block.
2. Select the best available software to use for the mining(in case of Computational Rig).
3. Allow the system to guess the Target hash value using the computation algorithm.[13]

Blockchain has the important fundamental conditions all the nodes participating in the network to concur on in the progression of checking that the square is legitimate for connecting a new block(Computational algorithm). Every partaking node (full node) ought to have the capacity to recognise a similar outcome with a similar strategy, and all confirmation forms must decide a similar esteem.[11]

The IoT blockchain network is a permissioned private blockchain that is enlisted in the wake of being verified and can work on a blockchain arrange. In this manner, one might say that its identity is not the same as an open blockchain which access to the system.[2]

Components of the IoT blockchain Network

a) **Blockchain Node:** Records all transaction blocks as a full node. Stores setting data identified with user device, device control, charging, and administration performed by the user.

b) **Administrator:** A man who registers clients, passages, and gadgets in the blockchain and gives access between them. The settings are securely stored in the full node of the blockchain and are transmitted to the accompanying clients, portals, and devices through the system. Every user and device keeps up the most recent settings identified with them. It can likewise be coordinated methodically with the current IoT working environment.

c) **User:** A man or gadget with a program running as a straightforward node that does not store pieces.

d) **Gateway:** As it is, a unit used to control numerous fake gadgets or sensors. It can dissect points of interest of the IoT contract and after that transmit to sham gadgets or sensors. Every gadget or sensor is associated with an individual address.
e) **Device:** As it is, a device that is associated with an entryway or a straightforward hub which does not store squares.

The block can then be used to validate devices in situations as a smart home in which devices are closely interconnected utilizing a private blockchain, designed to work more securely and dependably as per each other's conditions.
A private blockchain is arranged to perform user validation as well as mutual confirmation between devices, generating and safely recording activity elements and situation based IoT contracts. 'A private blockchain network is a blockchain with access privileges. Therefore, to get to a private blockchain from an open blockchain, a bridge node is required. This node must have the majority of the setup data of the private blockchain, to permit it an indistinguishable level of access from its private comparable while enabling it to post to people in public chain.[12]

User-Device Mapping in IoT Blockchain

The user on the IoT blockchain must have the access to get to the device as per clear access rights tenets to control the device. The user ought to likewise have the capacity to control the particular equipment as per the setting or to just read the status of the hardware, and it ought to be conceivable to make general clients difficult to reach to certain gear.
This enables the administrator to set access authorizations by the addresses of the user, devices, or gateways. This entrance right setting is put away in the greater part of the full hubs of the blockchain arrange, and is additionally shared among all nodes, gateways, and devices.
Access and control of clients and gadgets, and transaction authority, are recorded safely in the blockchain. The IoT contract can be done after the authority checked contrasted with this record when the exchange happens.

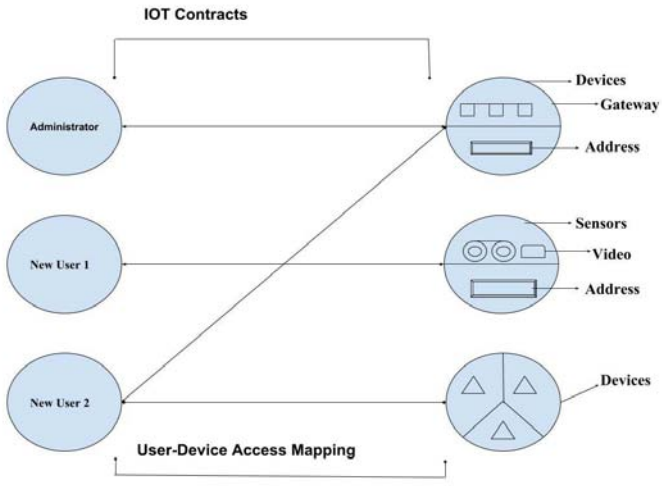

Fig. 4 : Mapping between device and user on private blockchain

Expert Mapping of the Network

- User device/Gateway mapping
- User mapping
- Device/Gateway device mapping

Mapping Rights of the Network

Access rights: Indicates the privilege to get to the device. Will have the capacity to indicate a base access rating.
Right to Read: It is a privilege to peruse the present state, and detailed authority can be indicated as a different string.
Right to control/write: It is the privilege to control the device or to change the state.
Transaction rights: Specifies configurable rights identified with manual and automatic transaction.
Other rights (indicating definite rights by device): Other point by point rights can be determined as a different code or string, and can be deciphered by the gadget to decide if they are pertinent or not.[4]
Security for IoT Blockchain

Security could be enhanced by utilizing a different secure channel by isolating the system amongst nodes and devices or between blockchain nodes and users.This technique can be implemented through hardware or blockchain programming, which can be mounted on a device. This technique has favorable position that it isn't important to change a current blockchain node or device configuration. Low-performance devices that experience issues performing complex encryption can specifically utilize IDEA (International Data Encryption Algorithm) or ARIA (Generic 23-Block Cryptographic Algorithm with Involutional SPN Structure Optimized for Lightweight Environments and Hardware Implementation) or with the AES128 to AES256 standard symmetric key encryption calculation, depending on the device
Consequently, at least one nodes ought to work as watchdogs to identify anomalous transactions and produce events. In every node, the capacity of checking the status of the server might be embedded to notify the administrator, who can act before the blockchain ends up hard to work.[3]

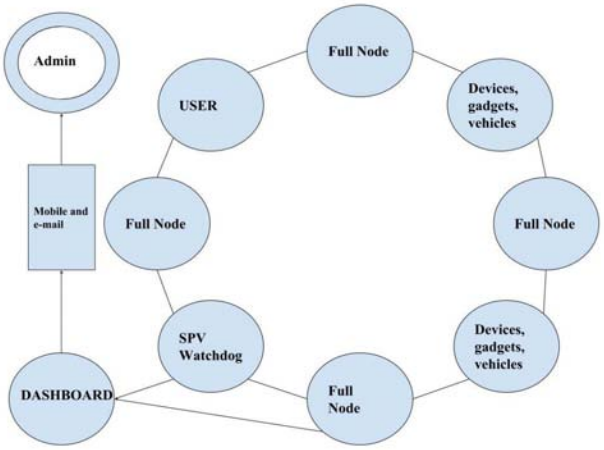

Fig. 5 : Threat prevention in the IoT private blockchain

Security Requirements For The Network

- Confidentiality**:** Confidentiality sees that only the authorized user is able to see the message.
- Integrity**:** Integrity makes sure that the sent message is unchanged when it reaches the destination.
- Availability**:** availability means that every service and data will be available when they are needed[9].

Design Of The IoT-Blockchain Network

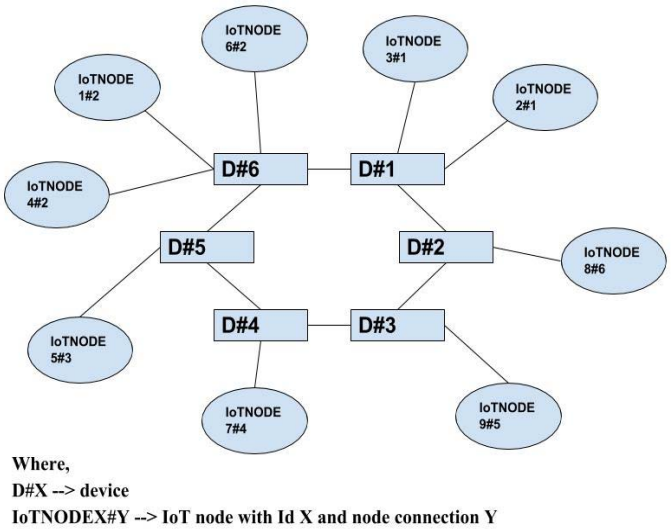

Fig. 6 : Representation of the connection of IoT Gateway Nodes with the devices.

The Devices will be connected with the Gateway Node creating a Personal Area Network.

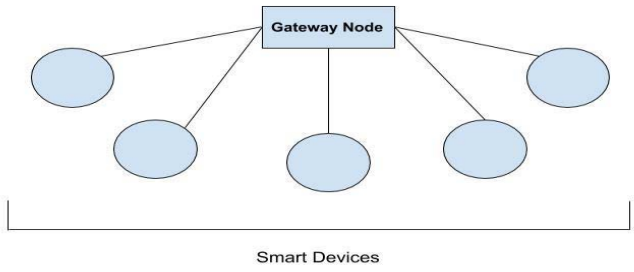

Fig. 7 : Gateway Node interacting with the smart devices.

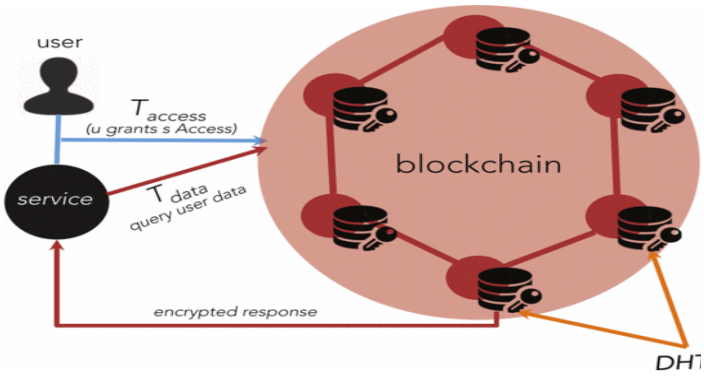

Fig. 8 : The Link of trust maintains and secures the data

Through the Gateway Node the Validation of the devices will be done as the Validators are connected with the Gateway Nodes which will form the Link of Trust providing the network to access to the new nodes from the blockchain. The three elements containing our framework are mobile phone clients, intrigued by downloading and utilizing applications; benefits, the suppliers of such applications who require handling individual information for operational and business-related reasons (e.g., directed advertisements, customized administration); and hubs Note that while clients in the framework remain anonymous, we could store profiles on the blockchain and validate their identity.[7]

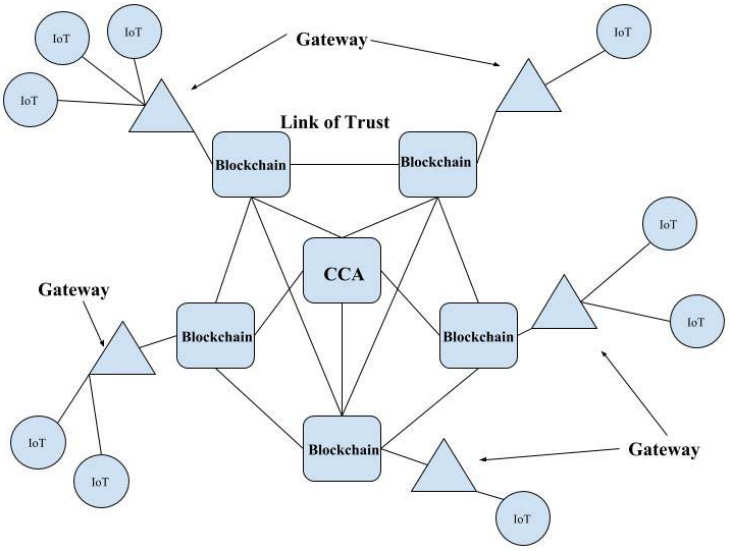

Fig. 9 : Architecture of the IoT Blockchain Network

- A simple network with blockchain validators and a CCA with different IoT Nodes connected to central validator network.
- All the blockchain validators are connected to each other and a CCA.
- The IoT end nodes are within the PAN(Personal Area Network).

The IoT devices will retrieve selective information from the analytical data and will send the corresponding information to the concerned devices, fulfilling its purpose. The Gateway devices will work as the mediator between the IoT devices and the blockchain, helping in the integration of the two in the process which is extremely necessary for the model to be safe and systematic the way it should be. The Blockchain will ensure that the right person gets the right information and the integrity of the model stays safe.[15]

III. RESULT ANALYSIS

The IoT-Blockchain architecture is a better way of interacting with the online market for transactions is much better than the existing traditional online shopping models of daily necessity as:

1. The proposed model works with less consumption of energy, which is essential as the economic feasibility of the model restrains it to working more efficiently.
2. The model will be able to handle other forms of digital wallet payments.
3. The model will make the selection of devices and their integration with the other devices like of the refrigerator with the health app on the phone so as to check the daily calorie intake.
4. In India, where the cryptomarket is gaining pace, the introduction of such a model will benefit the working class through its automated system.[6]

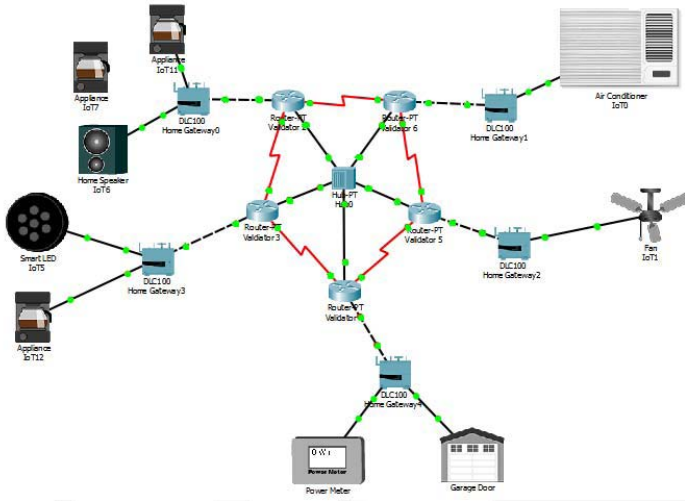

Fig.10: Introspection of the architecture on Cisco Packet Tracer.

Introspection of the architecture on the Cisco Packet Tracer reveals that the IoT devices which are validated by the CCA (Central Certifying Authority) successfully pinged with each other

Security Requirement Evaluation :

Table 1 : Implemented safeguards for security requirements

REQUIREMENT	SAFEGUARDS IMPLEMENTED
Confidentiality	Use of symmetric key encryption
Integrity	Hashing Employed
user control	Logging transaction in the Local BC
Authorization	shared key for every device

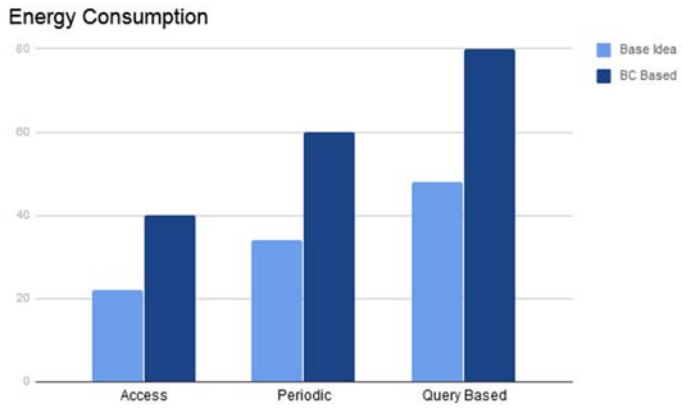

Fig. 11 : Energy consumption(µj) evaluation of different data traffic flow.

In Chart 1, we can clearly observe the difference in energy consumption in the different types of Data Flow patterns with Access Data Flow patterns having the least out of the three.

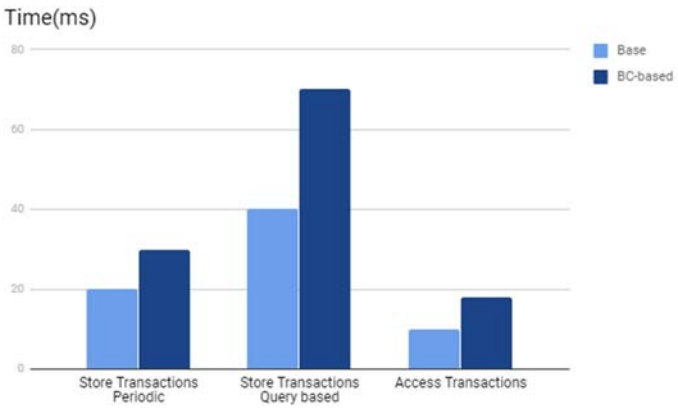

Fig. 12 : Time taken by different traffic flows to register a transaction.

In Chart 2, the least time to register a transaction on the blockchain was achieved by the Access Transactions.
From the two resultant charts we can formulate that the Access Data flow patterns are more economic feasible and less time consuming.

Table 2 : Comparison of Bitcoin BC with Local BC.

s.n	Features	BC in Bitcoin	Local BC
1	BC Visibility	Public	Private ✓
2	Mining Requirement	POW	None ✓
3	Forking	Not allowed	Allowed ✓
4	Double Spending	Prohibited	N/A
5	Transaction Parameters	input, output, coins	block-numbers, hash of data, time, output
6	Data Flow patterns	Periodic, Query-based	Access
7	Miner Selection	Self-selection	Owner ✓
8	Malicious Miner	Allowed to join	Not Possible ✓
9	Effect of 51% Attack	Double Spending	Not Possible ✓
10	Miner Checks	No one	No one
11	BC Control	No one	Owner ✓

Table 2 compares the Bitcoin BC with the Local BC, here we can clearly see the edge towards the Local BC as there is no mining required to set up a Local BC, Forking is allowed; that means we can select whether the Transaction is valid or not. Rest all the parameters in favor of the Local BC are highlighted which indicate the advantages of Local BC.

IV. CONCLUSION

Individual information, and sensitive information, should not be confided in the hands of third-parties, where they are susceptible to attacks and misuse. Rather, clients should claim and control their information without giving in any personal info to give customized administrations. Users are not required to share any information to people they don't want to know. Moreover, the blockchain perceives the clients as the proprietors of their own information. Developing secured and more efficient solutions for the Internet of Things requires collaboration, coordination and availability for each device in the network, and all through the network overall.[14] Almost all electronic devices will soon be able to connect to internet. Even the kettle can be connected to the internet now and we can heat water for my tea not leaving my room. Another big trend is that digital currencies are forecasted to become the main choice of customers. That is no surprise seeing how many advantages cryptocurrencies have over credit cards and other payment methods.By combining digital payments and Internet of Things in the form blockchain, the result will exploit growing trends. Customers demand reliable and convenient blockchains to utilize IoT devices. So, it is vital for this blockchain to be as safe and convenient as only possible.

V. FUTURE SCOPE

In the scope of blockchain and IoT it's interesting to look at the combination of blockchain and the Internet of Things as it's used in insurance and will increasingly be, moving beyond the pure telematics model to the connection of real-time IoT data in various perspectives for various intelligent automated applications:

- Vending Machines that can monitor its inventory and buy and restock it whenever required or is needed with automatic payment from users or vendors account.[10]
- A system of smart home applications that can bid with one another for priority so that the washing machine, dishwasher, air conditioner, robot-vacuum cleaner, etc. all run at an appropriate time minimizing the electricity costs.
- Vehicles that can diagnose issues and schedule its maintenance and diagnostic checks and paying for them.[8]

Customers demand reliable and convenient blockchains to utilize IoT devices. So, it is vital for this blockchain to be as safe and convenient as only possible.

VI. REFERENCES

1. http://www ft.com/intl/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64 html#axzz3qe4rV5dH.
2. Crosby Michael, Nachiappan, Verma Sanjeev, Pattanayak Pradhan, Kalyanaraman Vignesh, "Blockchain Technology: beyond Bitcoin", Berkeley Engineering. Pg. 9-10.
3. Salah, Khan Khaled & Khan Ahmad, Minhaj, "IoT Security: Review, Blockchain Solutions, and Open Challenges." Future Generation Computer Systems.10. 1016/j future.2017.11.022. 2017. Pg 3-10
4. KONSTANTINOS CHRISTIDIS, (Graduate Student Member, IEEE), AND DEVETSIKIOTIS MICHAEL, (Fellow, IEEE)Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA. 2016. Pg. 7-9.
5. Dorri, Ali & Kanhere, Salil & Jurdak, Raja "Towards an Optimized BlockChain for IoT. 10.1145/3054977.305500 3. 2017. Pg. 4-7
6. Reijers Wessel and Coeckelbergh Mark, "The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies", Grant 13/RC/2016.
7. Anirudh Bhardwaj, A beginner's guide to Bitcoin and Cryptocurrencies. Oodles Technologies, 2016.
8. Aditya Gaur, Bryan Scotney, Gerard Parr, and Sally McClean. 2015. Smart city architecture and its applications based on IoT. Procedia Computer Science 52, 1089–1094. 2015.
9. Boldt, Bill, "Without Security, is the Internet of Things justaToy?"Pubnub,https://www.pubnub.com/blog/2015-01-30-without-security-internet-things-just-toy/, (January 2015).
10. Huckle Steve, Bhattacharya Rituparna, White Martin, Beloff Natalia, "Internet Of Things, Blockchain and Shared Economy Applications.", Texas Tech University/14 Aug 2014/SSRN-2312787.
11. Groshoff David, "Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles", American Jewish University/15 Nov 2013.
12. https://www researchgate.net/publication/314363377_Towards_an_Optimized_BlockChain_for_IoT.
13. https://internetinitiative.ieee.org/newsletter//blockchain-a-technical-review.
14. Ahmed Banafa, "IoT and Blockchain Convergence: Benefits and Challenges".
15. Saptarshi Gan, Sandeep Shukla, "a key-based authentication architecture for IoT devices using blockchain & An IoT simulator in NS3".