BLENDING IOT AND BLOCKCHAIN: OPPORTUNITIES, CHALLENGES AND USE CASES

V. Shete[1], A. Dhumane[2], D. Upasani[3], S. Bendale[4] and and S. Athawale[5]
[1,2,3]MIT School of Engineering, MIT ADT University, Pune
[4]NBN Sinhgad School of Engineering, Pune
[4]AISSMS College of Engineering, Pune
virendra.shete@mituniversity.edu.in, amol.dhumane@mituniversity.edu.in
dhananjay.upasani@mituniversity.edu.in, shailesh.bendale@sinhgad.edu, svathawale@aissmscoe.com

ABSTRACT

In traditional IoT systems, sensors sense the data, further this data is advanced towards the cloud. The data analysis is done on the cloud platform for taking appropriate decisions. During data streaming and data storage, security of the data is a big concern. Several malicious activities are going on continuously with or without intention. It is necessary that the data should be tamperproof in all scenarios for correct action taking. On the other hand, blockchain provides a platform to evadereliable third parties, it also safeguards against single point of failure and helps to enhance the security of the data with the help of associated consensus algorithms. As both IoT and blockchain are emerging giant technologies, so there will be huge number of applications on the basis of blending these two technologies. IoT will provide pervasiveness and Blockchain will provide integrity of data in those applications. This has motivated academicians and researchers to blend these technologies to take maximum benefit from them. The opportunities, issues and various applications by blending these two technologies are discussed in this paper.

Keywords*: blockchain, Internet of Things (IoT), Blending, Peer-to-peer networks, consensus mechanism*

Introduction

Risk and security challenges with using the Internet today

Internet is miraculous and it isaltering the world with rapid pace. Knowingly and unknowingly, Internet has touched majority of aspects of our life by various means, but the thing to note is still there is huge scope to this technology as today also we have 50% of the global population that is not connected to it. The internet plays crucial a role in our everyday's activity includingour working, learning process, communications, entertainment and many more. It has significantly impacted majority of the industries and created new industries like social media. It is becoming a root cause of many disruptive technologies.

According to some researchers, we are still in the initial phase of the internet technology and we have yet to evidence the most disruptive days of this technology. We are concentrating on the positive side of this technology including low barriers during setting up and doing a global online business, low-cost communications anywhere in the world and new ways to access healthcare information and services. It's a correct time to put a beam of light on the stubborn problems associated with this vast network of networks. If we don't pay attention to it, it means that we are kidding ourselves. There is a great need to think about those problems beyond the current issues of software viruses, trolling on social media, online scams, false news, and illegitimate hacking. Since its origin, internet is struggling with serious fundamental problem of trust.

In day to day life we come across many questions such as is the personswith whom we are doing online business are really who are these people? Are these are same people with which we are dealing? Or those people are giving their fake identity? Of course, we could all think of hundreds of other examples of trust on the internet. Trust is a foundation of healthy ecosystems. Now, it is often said that we have done miracles with current technology. Along with passwords and usernames, now a day we need to takeadditional effort to confirm an identity of every individual e.g.Now a day's users of some applications are asked to type another security code that is sent independently on that person's mobile phone after entering a userid and password in his computer system. For blocking the security attacks and bad network traffic, we installed various intrusion detection systems, software and hardware

firewalls, along with it, we use CAPTCHA's to fill those online text boxes for proving that we are not any computer program (bots), we also have the mechanisms of biometrics such as iris and fingerprint for accessing and storing secure information. For maintaining trust and security, we came a long way with these mechanisms and tools, but still there is always a danger of getting hacked. We are not 100% sure about the security. We can't predict that at which time momentour databases and systems will be compromised, will become unavailable and our identities as well as money will be stolen, and our self-confidence to invent even further using the internet is muffled and, at worst, obstructed.If we want effective digital currencies, ironclad online voting systems, sureness in machine to machine communications, self-driving vehicles that securely communicate with oneanother, better and unifiedapproaches to validateindividuality, and many more, we're will need anextrasafe, reliableas well as highly trustworthy internet in the coming time.

We are living in the era of information where huge amount of data is getting generated at every moment with several devices connected to the internet. It includes healthcare monitoring facilities, environment monitoring devices, personal safety related devices or home appliances. It is very difficult for us to live without internet connectivity. This trend is getting increased exponentially and very soon every person in the globe will be having at least one or more than that devices connected to the internet. With the rapid growth of IoT technology internet is touching every part of our life and by the emergence of blockchain technology, we are feeling confident about introducing the trust in the online communication process. The combination of these two technologies may help us to build some promising applications in future. This paper has focused on various issues and importance of merging these technologies together.

The remainder of the paper is organized as follows. Section I of this paper discusses about IoT and Blockchain technologies. Section II first presents need of blending IoT and blockchain. Section III describes about the key benefits of using blockchain technology in IoT. Challenges of Integrating Blockchain Technology with IoT arediscussed in Section IV. Section V focuses on various use cases of Blockchain Technology with IoT, Section VI concludes the paper.

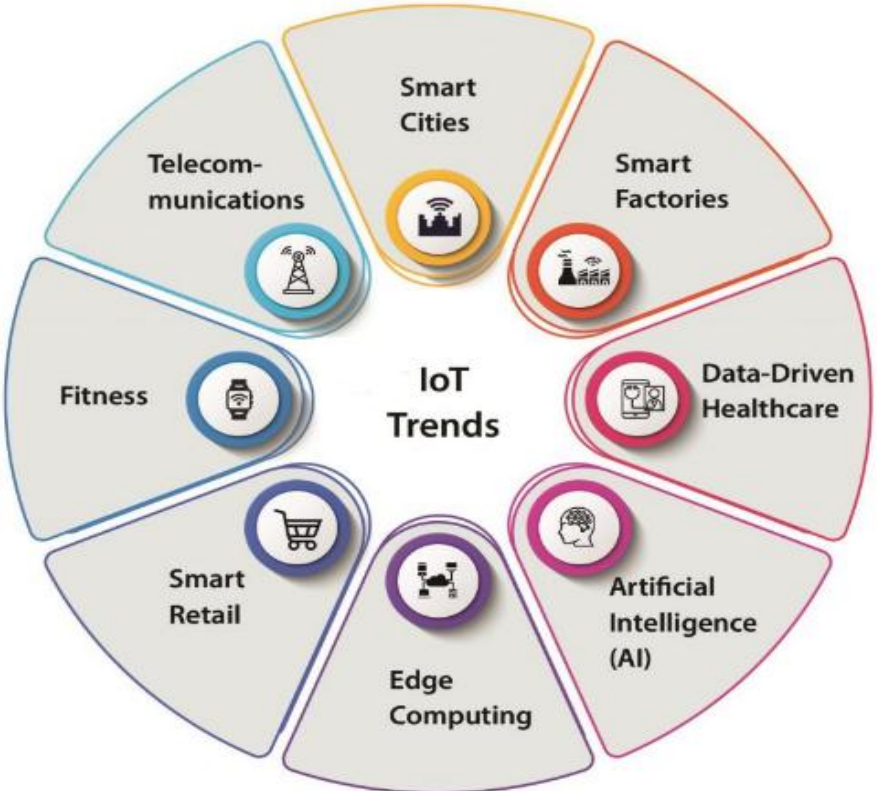

Fig 1: IoT Trends

I. IoT and Blockchain technologies

IoT Technology

By the arrival of smart things, smart homes and smart cities, IoT has raised as a ground of massive impact, prospects and expansion with the expectation of more than 60 billion connected devices by 2022.

As stated by International Telecommunication Union, the Internet of Things (IoT) refers to the network of abundant smart things (containing sensors and actuators) that are connected to the Internet. These devices gather the information from the surrounding using the sensors, communicate that information to other connected devices for routing it to the base station for doing its analysis and generating knowledge for taking appropriate decisions. These decisions result into creating a smart environment for human comfort.

Internet of Things (IoT) will play a crucial role in restructuring the industry in to smart industry with the capability of decision making based on the gathered information.However, basic properties of IoT including poor interoperability, intermittent connectivity, heterogeneous devices, different networking standards, decentralization, privacy and security vulnerabilities etc. lead it towards a number of challenges [1,3].

Regardless of the several advantages offered by IoT serious secrecy concerns may arise due to its ubiquitous and distributed nature. The huge number of things connected in the network may share sensitive information and data that may disclose behaviours and inclinations of their proprietors. To prevent such situation, proper precautions need to be taken for maintaining the guaranteed privacy in the design of IoT system while dealing with the sensitive information.

Blockchain Technology

Blockchain representsa distributed and tamper proof transactional database. It has provided a safe method for storing and processing data across huge network participants [8]. Blockchain is a continuously rising list of transactions stored in the form of blocks, these blocks are connected to each other by using cryptographic mechanisms. Transaction is a data unit of blockchain. Several transactions are bundled together to form a block. Every block contains cryptographic hash of previous block, transaction data and the timestamp. It is fundamentally a distributed ledger spread across the entire distributed system. The decisions in the blockchain environment are normally done by the consensus of other computational nodes distributed across the network. “Consensus is the process of decision making in the group where group members take a decision for the best interest of the community/system”. Using Consensus algorithm, all node come to Consensus and maintain a same copy of blockchain across the network which result into building a trust in the network as well as with the help of Consensus algorithm the data tampering in the block chain becomes difficult. With the help of decentralized consensus and without the intervention of the trusted third party (like banks), blockchains made possible for a transaction to take place and get validated in a distributed system.Blockchain works on peer-to-peer architecture. This architecture may help to prevent the single point of failure problem of IoT network which will result into building overall trust, availability and reliability of the IoT network[4]. Every participating entity verifies the behaviour of other participants, it also verifies and approves the new transactions before recording it into Blockchain ledger. This guarantees stable Blockchain operations decrease the chances of single point failure with tamper resistance mechanisms [6].Here, it is interesting to note that the blockchain ledger is presentwith every participant without any type of regulations of network authorities.

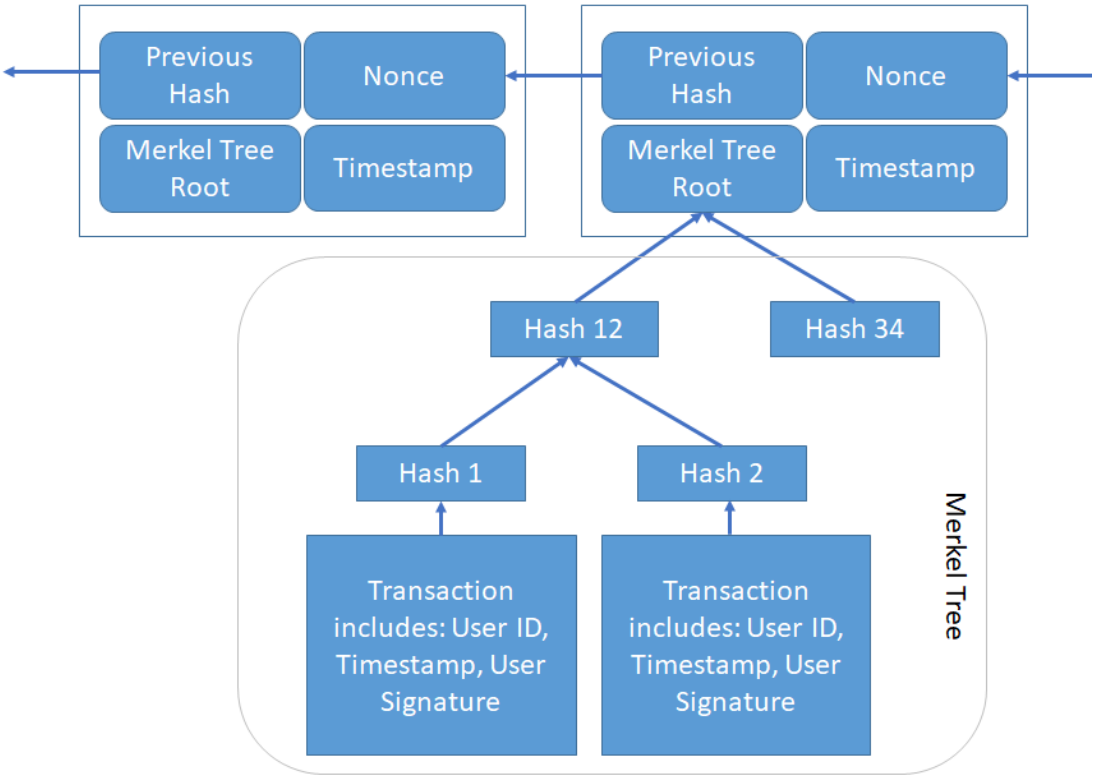

Fig 2: The structure of a Block Blockchain [2]

In peer to peer network of Blockchain technology, two types of nodes are maintained: light nodes and full nodes. Using the consensus mechanisms, full nodes validate the transactions and blocks. They have an ability of data mining. These nodes maintain trust into the network. Light nodes are used to make transactions. Light nodes store the Blockchain header while the complete distributed ledger is stored on full nodes.In general, the header of any block includes: 1) previous block's hash for authentication purpose, 2) a Merkle tree root for stuffing transactions in a group 3) a Nonce (number once)whichgenerates a hash value under the target level using consensus mechanism and 4) a Timestamp indicating the time of block creation.

With repetitive hashing, Merkle trees are produced till only one hash remains. Every leaf node contains transaction's hash, and that ofnon leaf node encompasses a hash of earlier hashes.

The possible obstacles to blockchain adoption

The major challenge is that most of the people are still unaware about the Blockchain. Knowledge and understanding are the two important pillars for emergence of any new technology.

The second problem is related to technical aspect. As the idea of blockchain is very new, sometimewill be required for getting it mature. Presently, blockchain is facing several issues liketransaction speed, data management and verification. It is very clear that blockchain will hold a huge amount of data in the coming future.Butin spite of anability of high security, it is considered that still there will be some privacy and security related challenges. The integration of blockchain with other technologies is also grabbing attention of researchers, a lot of innovation is needed to make that happen.

It is utmost necessary, for us to set guidelines and standards, processes, methods as well as practicesas a prerequisite for global acceptance of blockchain technology. We don't yet have them for the Blockchain, but initial standardization work is now underway, particularly by the ISO or International Organization for Standardization.

Along with technical limitations energy requirement for transactions is also one of the major hurdle. Blockchain transactions are irreversible in nature. This has also posed a major challenge today.

The final challenge includes, regulatory acceptance, resistance to change and cultural adoption There are a plenty of causes to trust the Blockchain will face difficult time while being adopted, but there are also a huge number of reasons specifying that it might just be bigger than the Internet.

II. Need of Blending IoT and Blockchain

With the active growth of wireless networks as well as the inclinations of digitization and miniaturization makes it possible to integrate intelligence and smartness into the home appliances and public infrastructure in our surrounding. The traditional security model based on the centralised approach is struggling for scaling up the ongoing and growing demands of continuously expanding Internet of Things networks. And as huge number of tiny and unobtrusive devices are deployed in the network, it become very difficult to pull them from circulation if they go rogue or are captured in a botnet. IoT network is a lot prone to security vulnerabilities including various malicious attacks such as Distributed Denial of Service (DDoS) and Ransomware.

Along with the combination of various crypto processes and blockchain, it is possible to offer a fascinating option with respect the IoT security. Especially the authentication of IoT devices, which is important for decentralized structures, can be made considerably easier with blockchain. As blockchain is developed for distributed control and avoiding single point of failure due to centralised control mechanism, the security scheme on it must be more scalable compared toalready existing mechanisms. Due to blockchain's ability of robust safeguards against data tampering, it will help to prevent a malicious device from troublemaking and spreading misleading information in the deployed IoT application setups.

By letting the stream of data encoded in blockchain technology into the infrastructure of GSM operators, it is possible to identify each chunk of data, along with its source and its producer. It helps to ensure a fully secure, transparent and universal communication standard which can be applicable to governments, cities, organizations as well as households and the single end user.

IoT devices are considered as wonders of engineering. These devices are still work with limited powered as compared to the other hardware which is supplying power to blockchains. Computational tasks of blockchain are complex and time-consuming it makes many of the IoT devices impossible to participate directly in a blockchain due to their limited processing power.

IoT enables devices across the Internet to gather huge amount of information, store it on cloud or distributed platforms, analyse it by considering the timestamp associated with the information and use it to for decision making. It makes very clear that the information is a core part of IoT ecosystem. That makes it essential to protect the information from evil intentions and attacks on the resource constraint environment with limited capability nodes.

Blockchain has decelerated in its implementation and evolution. Still its applications are comprehensive and broad. It has an ability to help the technologies like IoT and Artificial Intelligence.

The evolution of IoT is still going along, but it too has reduced its speed as researchers understood that becoming proficient at the network of smart 'things' is extremely hard than theirimagination due to severalissues of security and timelines of implementations. Due to that Blockchain and IoT find themselves at similar places when it comes to adoption that their amalgamation may help one another to resolve some of the important concerns that have dogged them at individual level.

It is now crystal clear that an immutable ledger with the safety and security concerns is having the ability to help the smart things system for performing as a network without much human interventionto become an un-hackable blockchain with a token system.

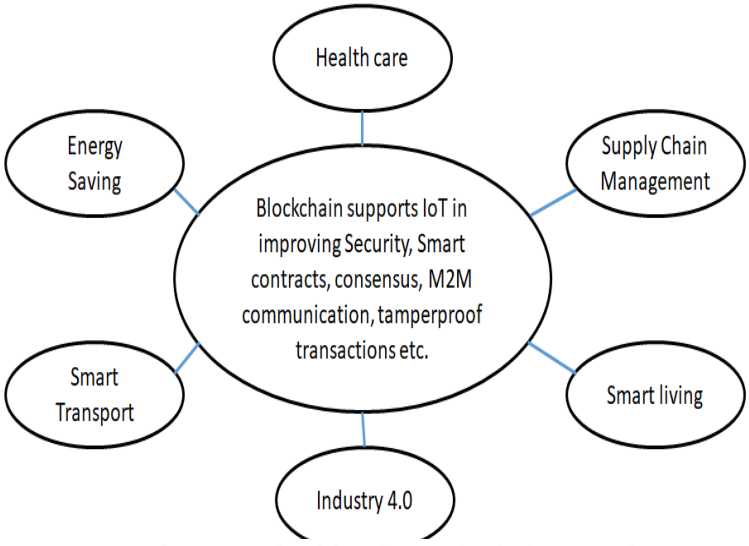

Fig 3: Applications by blending Blockchain and IoT

As time is going, huge number of data transactions are taking place amongseveral networks owned by severalestablishments. With the help of blockchain it is becomes easily possible to track physical goodsand data associated with it that is passed between several points in the supply chain. Apart from this, using blockchain, trust building, risk reducing with higher security, reducing costs, and acceleration of transaction is also possible.

The blending of blockchain and IoT will be most exciting combination across various industries and has countless applications. With blockchain we are in the position to add pretty much for changing the currentdigital infrastructure which has powered many evolutions and impactedon many areas such as security, analytics etc. in an environment that thus far was centralized. There are numerous diverse techniques and applications in which these technologies can work very strongly which are already discovered and verified, but as an amalgamation, still their final and resilient use case is yet to be discovered.

III. Benefits of Blending

blockchain will increase the trust level between the communicating parties in the IoT networks, it will also reduce the risk of data tampering, it will help to reduce the cost of transactions by removing the third parties (e.g. banks, paypaletc), It will help to accelerate the transactions and reduce the settlement time from days to few hours or minutes. Advantages by blending these two technologies are given below:

Privacy and Transparency: Transparency and privacy need to go hand in hand by mixing both these technologies. In IoT network, using their own ledger, it is possible for participants to see blocks and its associated transactions. The transaction content is kept secureusing the private key of participant [16].

Decentralization: Blockchain became a promising technique with its decentralised nature while solving bottleneck problemsas well as single-point failure issues by eradicating the necessity of a trusted third party in the communication process of an IoT network [7].

Instead of using centralised transaction verification system, the responsibility of verification of transaction is put on the shoulder of participants. The majority of participants verify and approve the transaction and add them in the distributed ledger. As majority of the participants involved in this process massive amount of trust is included in this process [17]. This helps blockchain to provide a secure and decentralised platform for IoT devices. This approach is more fault tolerant against any type of cyber-attack and malicious activities.

Speed of transactions. With the blockchain with shared ledger technology untrusted participants can also able to exchange data directly by eradicating the manual processes. This increases transactions speed.

Enhanced security: Security is incorporated in the Blockchain technology by the ability of verifying and allowing transactions originated by a trusted party with encryption during data

transmission and storage. Upon the verification of the encrypted transactions, these transactions are further linked to the previous set of transactions. Information in terms of blocks is stored over a multiple nodes of the network instead of storing it on a single server machine, it preventsmalicious users from tampering data of transactions. To safeguard the transactions in IoT infrastructure, Blockchain systems will use asymmetrical key cryptography that is not possible for an individual to formulate mathematically. This protects the data from prospect attacks, it lessens data leakage problems and strengthens the overall security.

Transparency: Blockchain technology offersclarity and transparency about who is accessing and transacting. It also records all the interactions. The transactions histories are available to all network users. These shared transaction documents can be altered only by means of a consensus.The data alteration process is bit complex as to change a single transaction record, it is necessary to modify all subsequent records, otherwise the chain of block becomes invalid. This makes Blockchains data storage more robust, accurate, as well as transparent than the traditional network. Even though Blockchains motive is to maintain transparency. But certain applications like healthcare sector related application on IoT domain may get affected due to that transparency. So it is necessary to maintain the proper trade-off between the transparency and privacy in such cases.

Reduced costs: By automating the transaction validation without including any third party, the entire environmentis made proactive with reduced transaction cost [12].

Immutability: Immutableledger created using blockchain across the nodes of IoT will help to improve security andprivacy [14,18]. Transaction blocks are protected by cryptography and using a suitable hashing technique. Hashing mechanisms builds a sequential chain by linking these blocks together. With this, it becomes very hard to alter or delete these transactions.

Anonymity: To process the transaction and keeping the identity private of bothbuyer and seller, theyuses uniqueand anonymous address numbers. This feature can play very vital role in some of the applications on IoT platform including health care system and electoral votingsystems [14, 19].

IV. Challenges of Integrating Blockchain Technology with IoT

Limited processing power and lifetime of IoT nodes

The major hurdle in integration process is Blockchains demand of very high processing power requirement. In Blockchain environment for high end laptops also it is difficult to do mining task due to their limited processing power. Blockchain require specialised infrastructure with very high processing power to solve the complex problems. Compared to that, IoT may contain resource constrained devices. The constraints can be in terms of processing power or in case of their lifetime. This posesbiggest challenges for integrating blockchain and IoT due tocertain IoT device's shortlife due to limited power supply.According to [11] the Bitcoin network uses considerable energy than the power requirements of several nations, including Colombia and Austria. Due to this, researchers suggested about optimizing blockchains central algorithms for increasing the number of confirmed Blocks in one second [9] by eliminating the Proof of Work consensus mechanism for reducing consumption of power and increasing the processing speed [15]. On the contrary, Proof of Work prevents malicious attacks and helps Blocks to become tamper-proof. Therefore, theobjective is to improveblockchain processes to properlyline upefficiency and security [10].

Limited Throughput of Blockchain

IoT devices does continuous communication in the deployed network [20]. So it is necessary to create and attach the blocks in the chain structured ledger of blockchain by synchronizing with the IoT devices communications. But due to consensus mechanisms, security algorithms and cryptographic functions, throughput of blockchain is limited. So, it becomes necessary to improve the throughput of blockchain for fulfilling the demand of frequent transactions of IoT.

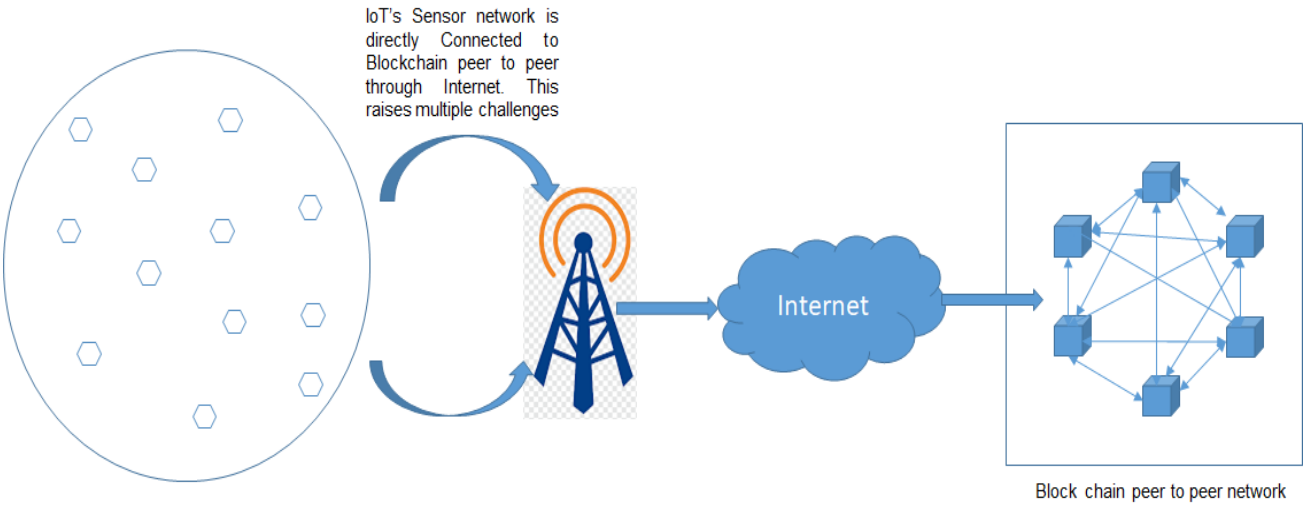

Fig 4: Blending of Blockchain and IoT network

Limited storage space of IoT nodes

IoT devices generates huge data in day to day life. According to the philosophy of blockchain, all the transactions are stored in the form of chain of block on every node in decentralized manner for improving the trust. This increases the storage demand at every IoT node. Authors [19] considered that a Blockchain node will need roughly data storage of 730 GB per year for 1000 participants exchanging a single 2 MB image per day in a Blockchain application. This clearly states the challenge related to high storage requirements in the resource constraint IoT environment.

Scalability restrictions

Due to some bottlenecks, the blockchain platform result into less scalability, limited throughput and higher computational costs. Bigger sizes of blocks result into need of higher transaction processing times for writing them into chain of previously confirmed blocks. In complex IoT scenarios data is tremendous that generates a need of processing of high volumes of data. It makes the process of block formation complicated. Due to these limitations, many applications developers don't see Blockchain technology as a promising alternative solution to the large IoT systems.

Security issues

It may happen that, if greater 50% of the machines executing Blockchain start controlling computing resources then there is a possibility that they can change consensus mechanisms and may discontinue the approval of new transactions with malicious intentions. By creating several identities, the malicious nodes can either overflow the network with transactions or make wrong statements in Sybil attacks. This can result into data instability. Selfish mining where a clusters of miners work together to raise their incomes is also a cause of concern [13]. It is difficult to maintain the secrecy of transaction history on public blockchain. By analysing transaction pattern, attackers can find out the users, so it is necessary to have an additional strategy to maintain the anonymity.

High consumption of Bandwidth

As every transaction need to be transmitted across the blockchain peer to peer network for verification and validation, so there is a huge need of bandwidth in the Blockchain peer to peer networks. But there can be scarcity of bandwidth into the sensor based IoT networks. This may pose a challenge while integrating these two technologies.

V. Usecases

1. Logistics and Supply chain

Multiple stakeholdersare involved in supply chain network including raw material suppliers, brokers etc. This is a complex scenario which is carried out over number of months' time and containthe record ofseveralexpenditures and invoices. Delivery

delays become the crucial challenge due to participation of several stakeholders.

This makes businesses to work on creating the trucks IoT-enabled for tracking theirdriveduring the shipment course. With such overall transparency the current supply chain and logisticssystem can be improved with the help of Blockchain and IoT by focusing on reliability, accountability and traceability.

Various IoT sensors such as temperature sensors, GPS, vehicle information, motion sensors can be used for this purpose. The information collected by the sensors is then stored in the blocks of blockchain which can be further accessed real time by different stakeholders for getting the exact status of current situation. This will improve the overall accountability and transparency in the supply chain management and logistics process.

2. Automotive Industry

Digitization trying to convertautomotive industries into smart automotive industries with the help ofvarious sensors for manufacturing fully automated vehicles. It will enable multiple users to exchange secure, vital and verified information easily and quickly with the blockchain and decentralized IoT network.

This is anexciting IoT blockchain use case, where IoT and blockchain technologies can disrupt: smart parking, automated traffic control, autonomous cars and automated payments like parking payment, fuel charges and toll. These payments are given through crypto-wallet of blockchain cryptocurrency without involving third party.

3. Smart Homes

Smart homes can be upgraded to next security level with the help of Blockchain. Now a day's masses of intelligenthardware's are connected using IoT. So it becomes difficult to stockand secure the day by day growing data in the cloud as multiple internet users can access it. Integrating Blockchain with IoT upliftssmart home with various characteristics such as augmenting transparency, security and smooth access of smart devices.

An Australian telecommunication and media company known as Telstra,offers smart home solutions. Thisenterprise has blended biometric safetywith blockchain to guaranteethat no one can tamper the sensitive data such as biometrics, voice recognition and facial recognition captured by devices installed in smart home.

The blended technology makes sure that, once the information is stored on the blockchain, it won't be altered, and will be accessible to the right person only.

4. Pharmacy Industry

With every passing day, in the pharmaceutical sector, the issue of fake medicines is increasing. The pharmacy industry is accountable for developing manufacturing and distributing new drugs.The overall tracking process of Drugs ischallengingand complex.The traceable and transparent behaviourof the blockchain technology can support toclosely observe these shipments of drugs from their origin to theirlast stop.Mediledger is ananother use case designed for tracking the legal change of prescription medicines' ownership. The data stored on the distributed ledger is timestamped and immutable and it is accessible to: wholesalers, manufacturers, end-customers and dispensers for maintaining Transparency and traceability. Mediledgerplatformstop fake drugs from invading the supply chain by offering simple payment mechanisms and controlled users access.

5. Agriculture

Day by day graph of population is increasing. For fulfilling the food demand of this growing population, it is necessary to grow more and more food. This process contains several hurdles. By coupling Blockchain with IoT the process of food production and its supply to the customers can be improved significantly.By mounting IoT sensors in the farm and directly sending its data to the blockchain can aidin enhancing the food supply chain to a greater extent. e.g. Pavo is a IoT blockchain use case which has offered a smart farming approach to farmers by installing IoT hardware in the fields. By using the collected data from this IoT hardware, it become easy for farmers to take farming related decisions. It also allows consumers, retailers and distributors to make informed decisions about purchasing a specific food item or crop. The Payomarketplace

system permits the farmers to sell their harvests early instead of waiting till the end of harvest.

VI. Conclusion

In this survey paper we tried to focus on the current security issues on the existing internet platform, the need of IoT and blockchain technology, their importance and their need in future applications from improving the trust in the communications. Both technologies have numerous advantages even though there are some limitations also. This paper discussed about the scope and challenges by blending these technologies. Current Blockchain and IoT papers were inspected with respect to various features for demonstrating their strength and limits. At the end, this paper discussed about some of the possible applications by amalgamation of these technologies.

References

1. Dhumane, A., Prasad, R., & Prasad, J. (2016). Routing issues in Internet of Things: A aurvey. In Proceedings of internationalmulti conference of engineers and computer scientists, vol. 1, (pp. 1–9).
2. M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian (2021), A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, Blockchain: Research and Applications,ISSN 2096-7209, (pp. 1-80).
3. A. Dhumane, S. Guja, S. Deo, and R. Prasad (2018). Context awareness in IoT routing, in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). IEEE, (pp. 1–5).
4. Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng (2019). Towards secure industrial iot: Blockchain system withcredit-based consensus mechanism. IEEE Transactions on Industrial Informatics, vol.15, (pp. 3680–3689).
5. Minhaj Ahmad Khan and Khaled Salah (2018). Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, vol.82, (pp. 395–411).
6. Avelino F Zorzo, Henry C Nunes, Roben C Lunardi, Regio A Michelin, and Salil S Kanhere (2018). Dependable iot using blockchain-basedtechnology. In 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), IEEE, (pp.1–9).
7. Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu (2018). Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, vol. 25, issue 6, (pp. 12–18).
8. Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu (2018). Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, vol. 25, issue 6, (pp.12–18).
9. Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito (2018). Blockchain and iot integration: A systematic survey. Sensors, vol.18(8), (pp. 2575-2585),
10. Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng (2019). Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, vol.15(6), (pp. 3680–3689).
11. Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian (2020) Solutions to scalability of blockchain: A survey. IEEE Access, vol. 8, (pp. 16440–16455).
12. UmeshBodkhe, SudeepTanwar, Karan Parekh, PimalKhanpara, SudhanshuTyagiNeeraj Kumar, and MamounAlazab(2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, vol 8, (pp. 79764–79800).
13. Jiawen Kang, ZehuiXiong, DusitNiyato, Dongdong Ye, Dong In Kim, and Jun Zhao (2019). Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, vol. 68(3), (pp. 2906–2920)

14. A. Torkaman and M. A. Seyyedi (2016). Analyzing IoT Reference Architecture Models, Int. J. Comput. Sci. Softw. Eng. ISSN, vol. 5, no. 8, (pp. 2409–4285).
15. MdAshraf Uddin, AndrewStranieri, Iqbal Gondal, andVenkiBalasubramanian (2019). An efficient selective miner consensus protocol in blockchainoriented iot smart monitoring. In ICIT, (pp. 1135–1142).
16. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba (2017), Blockchain technology innovations,2017 IEEE Technol. Eng. Manag. Conf., no. 2016, (pp. 137–141).
17. M. Samaniego and R. Deters (2016) Blockchain as a Service for IoT, 2016 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, (pp. 433–436).
18. A. Dhumane, D. Midhun chakkaravarthy(2020).Multi-Objective Whale Optimization Algorithm Using Fractional Calculus for Green Routing in Internet of Things,International Journal of Advanced Science and Technology, Vol. 29, No. 3s, (pp. 1905 – 1922).
19. H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills (2017). Integration of cloud computing with internet of things: challenges and open issues, in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), (pp. 670–675).
20. A. Dhumane, A. Bagul, P. Kulkarni (2015).A review on routing protocol for low power and lossy networks in IoT, International Journal of Advanced Engineering and Global Technology, I Vol-03, Issue-12, (pp. 57-65).