International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-03, June 2018

A Review on BIoT: Blockchain IoT

Prof. Sumaiyya Z. Khan[1], Prof. Snehal R. Kamble[2], Prof. Ambarish R. Bhuyar[3]

[1,2,3]Assistant Professor, Sipna College of Engineering and Technology, Amravati, Maharashtra, India.

[1]ksumaiyya53@gmail.com, [2]snehalkamble27@gmail.com, [3]ambarishbhuyar10@gmail.com

Abstract- Internet-of-Things (IoT) devices are increasingly being found in civilian and military contexts, ranging from smart cities and smart grids to Internet-of-Medical-Things, Internet-of-Vehicles, Internet-of-Military-Things, Internet-of-Battlefield-Things, etc.The IoT is experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Conventional security and privacy approaches tend to be inapplicable for IoT, mainly due to its decentralized topology and the resource-constraints of the majority of its devices. Blockchain (BC) that underpin the cryptocurrency Bitcoin have been recently used to provide security and privacy in peer-to-peer networks with similar topologies to IoT. In the Internet of Things (IoT) scenario, the blockchain and, in general, Peer-to-Peer approaches could play an important role in the development of decentralized and data-intensive applications running on billion of devices, preserving the privacy of the users. In this review paper we have described IoT, its security requirements, Blockchain, its working, and the current uses of the blockchain with IoT.

Keywords — Blockchain, Internet of Things, IoT, Privacy, Security.

I. INTRODUCTION

Technologies have changed the way we live, particularly in our data driven society. This is partly due to advances in semiconductor and communication technologies, which allow a multitude of devices to be connected over a network, providing us with ways to connect and communicate between machines and people (e.g. machine-to-machine). Such a trend is also commonly referred to as the Internet-of-Everything, comprising the Internet-of-Things (IoT), Internet-of-Medical-Things (IoMT), Internet-of-Battlefield-Things (IoBT), Internet-of-Vehicles (IoV), and so on. Given the pervasiveness of such devices in our society (e.g. in smart cities, smart grids and smart healthcare systems), security and privacy are two of several key concerns. For instance, it was reported in 2014 that more than 7,50,000 consumer devices were compromised to distribute phishing and spam emails. In data-sensitive applications such as IoMT and IoBT, ensuring the security of the data, systems and the devices, as well as the privacy of the data and data computations, is crucial. However, a threat to a system can be the result of a security measure that is not well thought out. For example, in a typical civilian or military hospital setting, the Information Technology (IT) team generally has control of the entire network, including endpoint devices and IoMT devices (basically, any devices with an IP address). It is not realistic to expect the IT team to be familiar with every individual connected device, although they have the system administrator capability to install patches, and access the device and their data remotely, and so on [1].

II. LITERATURE SURVEY

In "A blockchain future for Internet-of-Things security: a position paper"[1], Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo reviewed security techniques designed for IoT and related systems published since 2016. They argued that there is a pressing need for more extensive research in predictive IoT. They also observed the lack of publicly available IoT datasets and the absence of representative IoT datasets, both of which are important for IoT security research. They proposed the need for a standard to be established for IoT datasets that will facilitate the sharing of such datasets for research purposes. They also highlighted the potential of blockchain in sharing and distributing such datasets in a research network. They then presented a conceptual blockchain-based compromised firmware detection and self-healing approach that can be deployed in an IoT environment.

In "Internet of Things-IOT: Definition, characteristics, Architecture, Enabling Technologies, Application & Future Challenges"[2], Keyur K Patel, Sunil M Patel briefly discussed about what IOT is, how IOT enables different technologies, about its architecture, characteristics & applications, IOT functional view & what are the future challenges for IOT.

In "IoT security: Review, blockchain solutions, and open challenges"[3], Minhaj Ahmad Khan, Khaled Salah presented and surveyed major security issues for IoT. They reviewed and categorized popular security issues with

 DOI : 10.18231/2454-9150.2018.0427

regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management. They outlined security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions. Furthermore, they tabulated and mapped IoT security problems against existing solutions found in the literature. More importantly, they discussed, how blockchain, which is the underlying technology for bitcoin, can be a key enabler to solve many IoT security problems. The paper also identifies open research problems and challenges for IoT security.

In "A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices"[4], Poonam Ghuli, Urvashi Priyam Kumar and Rajashree Shettar, described a unique method for peer to peer identification of ownership of IoT devices in a cloud environment. The described methodology consists of device being added by it's manufacturer (also referred to as Genesis) & then being transferred to a user based on blockchain technology. This paper also introduces how similar blockchain mechanism can be used for the transfer of ownership of a device from one user to another, without the involvement of any third party and the benefits of using the same whereas serial K-means++ achieves 85-89% accuracy for same sampled dataset.

Siva Gopal, in White paper on "Blockchain for the Internet of Things"[5], Tata Consultancy Services said that Blockchain has begun to have a significant influence in the Internet of Things by enhancing security, empowering the incorporation of an increasing number of devices into the ecosystem. The enhancements in IoT device security facilitate faster adoption of this revolutionary innovation, and will open up a wide range of possibilities for enterprises in the days to come.

Satyajit Sinha, in his blog on "Securing IoT with Blockchain"[6], said that Blockchain can be used to improve IoT security. As more and more devices create massive quantities of data and companies aim to leverage IoT to create and employ that data, security and accountability will be major hurdles. The incorporation of blockchain databases into IoT solutions could be one way to ensure that data is secure and that devices are accurately registering and reporting information.

III. INTERNET OF THINGS

A. Definition of IoT

Internet of Things common definition is defining as: Internet of Things (IoT) is a network of physical objects. The internet is not only a network of computers, but it has evolved into a network of device of all type and sizes , vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected ,all communicating & sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safe & control & even personal real time online monitoring , online upgrade, process control & administration [2].

We define IoT into three categories as below: Internet of things is an internet of three things: (1). People to people, (2) People to machine /things, (3) Things /machine to things /machine, Interacting through internet.

B. Security requirements for IoT

a. Data privacy, confidentiality and integrity

As IoT data travels through multiple hops in a network, a proper encryption mechanism is required to ensure the confidentiality of data. Due to a diverse integration of services, devices and network, the data stored on a device is vulnerable to privacy violation by compromising nodes existing in an IoT network. The IoT devices susceptible to attacks may cause an attacker to impact the data integrity by modifying the stored data for malicious purposes.

b. Authentication, authorization and accounting

To secure communication in IoT, the authentication is required between two parties communicating with each other. For privileged access to services, the devices must be authenticated. The diversity of authentication mechanisms for IoT exists mainly due to the diverse heterogeneous underlying architectures and environments which support IoT devices. These environments pose a challenge for defining standard global protocol for authentication in IoT. Similarly, the authorization mechanisms ensure that the access to systems or information is provided to the authorized ones. A proper implementation of authorization and authentication results in a trustworthy environment which ensures a secure environment for communication. Moreover, the accounting for resource usage, along with auditing and reporting provide a reliable mechanism for securing network management[3].

c. Availability of services

The attacks on IoT devices may hinder the provision of services through the conventional denial-of service attacks. Various strategies including the sinkhole attacks, jamming adversaries or the replay attacks exploit IoT components at different layers to deteriorate the quality-of-service (QoS) being provided to IoT users.

d. Energy efficiency

The IoT devices are typically resource-constrained and are characterized with low power and less storage. The attacks on IoT architectures may result in an increase in energy consumption by flooding the network and exhausting IoT resources through redundant or forged service requests.

e. Single points of failure

A continuous growth of heterogeneous networks for the IoT based infrastructure may expose a large number of single-points of- failure which may in turn deteriorate the

 DOI : 10.18231/2454-9150.2018.0427

services envisioned through IoT. It necessitates the development of a tamper-proof environment for a large number of IoT devices as well as to provide alternative mechanisms for implementation of a fault-tolerant network [3].

IV. BLOCKCHAIN

A. What is Blockchain?

Blockchain is a distributed, publicly available ledger for all transactions (digital events) that were executed & processed between two clients. The decentralized nature is possible as each transaction is verified through a consensus of a majority of the clients participating in the entire system. Blockchain, is a read-only ledger, where once entered information can never be erased, this also ensures that each transaction present in a blockchain was verified and accepted as a valid transaction by a majority of clients involved at that period of time. The public availability, decentralized and read-only nature of blockchain makes it mathematically impossible to create a fraudulent transaction and get it added to a blockchain, making it a safe, secure and reliable method to store and execute transactions, without the involvement of any third party.

Bitcoin is one of the first and most popular application of blockchain technology, which has resulted in creation of a huge global market of anonymous transactions which is unregulated and outside of any government control. This in turn is quite controversial and often warrants for a large number of governmental and regulatory reforms to keep such unregulated financial markets in check. Where, Bitcoin has been considered as hugely controversial, the underlying blockchain technology has already been adopted and applied in a variety of areas. One such potential area is the world of IoT [4].

However, Blockchain technology is currently being successfully applied to both financial markets as well as quite a few non-financial applications. Since the adevent of blockchain many researchers have considered the distributed peer to peer model for blockchain as an invention comparable to steam engine or the internet, having the capability to completely alter the world of commerce and beyond.

B. How does Blockchain work?

For two willing parties to conduct any transaction over the internet a cryptographic proof is provided by each one. Instead of trusting a third party, Bitcoin uses cryptography and certificates to sign each request sent by any party. Each party has a set of "public key" and a "private key". A public key as the name explains, is publically available and can be viewed by anyone, whereas a private key is meant to be secured by the client and not shared with anyone. In order to perform a transaction the owner of bitcoin needs to provide a proof of ownership of the "private key". For this purposes digital signatures are used. Any transaction is signed using a hash between the private key and the transaction id. This hash if re-hashed with the public key, will give back the correct transaction id. This way any other client can verify the proof of ownership of the "private key" of any client as shown in Fig. No. 1.

Due to this peer to peer communication for any transaction to succeed, information about each transaction is transmitted to every node in the network and is recorded publically in an immutable ledger, which is known as blockchain. Each and every is transaction is verified for validity by a consensus of a majority of nodes before recording it into the blockchain ledger. Two major things need to be taken care of by the verifying nodes are as follows:

a. Verification of digital signature of sender: Sender owns the private key for that bitcoin.

b. Spender has sufficient balance in his/her account to spend the amount: As Blockchain maintains history, this makes it easier, as every single transaction is compared [4].

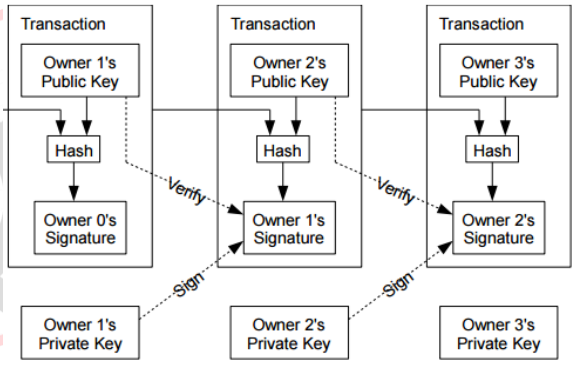

Fig. No.1: Transaction between two parties.

C. Blockchain Recommendations for IoT

Four important recommendations for IoT include:

a. Trust Building

IoT blockchain empowers devices to engage in transactions and communications as trusted parties. While device A may not know device B, and may not believe it varifiably, the permanent record of exchanges and information from devices stored on the blockchain confirm and enable the vital trust for organizations, individuals, and devices to cooperate.

b. Cost Reduction

It is important for IoT edge devices to reduce processing overhead and eliminate the 'middle man' (IoT gateways) from the procedure. Communication, data exchanges, and device information are conducted on a peer-to-peer basis, removing any additional traditional protocol, hardware, or communication overhead costs.

 DOI : 10.18231/2454-9150.2018.0427

c. **Accelerate Data Exchanges**

Improved data exchanges as the 'middle man' (IoT gateway or any intermediate □ltering device) is expelled from the process. Peer-to-peer device based contracts and ledgers (blockchain) decrease time required to complete device information exchange and processing time.

d. Scaled Security for IoT

Decentralized technologies hold great promise for a system that needs to handle storing and retrieving information of millions—if not billions—of connected devices. These future systems have to provide low latency, high throughput, querying, permissions, and decentralized control. Blockchain adoption in the IoT space can change the way IoT edge devices exchange data in a trustworthy environment, mechanizing and encoding transactions, while safeguarding data exchanges and ensuring security of all devices involved [5].

V. CURRENT IMPLEMENTATIONS OF BLOCKCHAIN IN IOT SECURITY

a. IBM and Samsung: IBM has unveiled a proof of concept known as ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry), which uses blockchain-type technology to form the backbone of a decentralized network of IoT devices. With ADEPT, Samsung has designed a washing machine that uses this IBM framework to order supplies from a vendor automatically.

b. Asset Tracking: A pharmaceutical seal from Chronicled combines NFC chips with blockchain to track and secure prescription drugs. The seal as shown in Fig. No. 2 contains secure information about the contents of a prescription bottle, registering the information on a blockchain, whilst also recording the registering party and location data. This tamper-proof technology solution adds a key layer of visibility to pharmaceuticals, allowing patients and physicians to ensure that medication is not counterfeit and provides visibility into the medication supply chain.

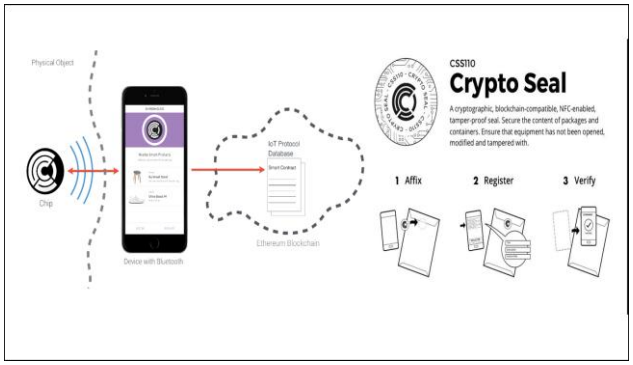

Fig. No. 2: Chronicled asset tracking blockchain concept showing single application Crypto Seal

c. Aircraft Maintenance: An aircraft typically has a long lifecycle with various owners and it is important to know which parts have been replaced and when. By combining IoT, instrumentation and device authentication, a record of ownership could be established for every part in an indisputable record. This would allow reliability and safety to be traced by both passengers and prospective buyers. Furthermore, damaging events such as hard landings, could be tracked by IoT devices and permanently recorded in the blockchain, thus providing critical information regarding the reliability of the aircraft for all stakeholders.

d. WISeKey International Holding Ltd: A Swiss cybersecurity and IoT solutions company, announced that it has partnered with VIMANA Global, to secure the VIMANA Blockchain Airspace Platform, the blockchain airspace platform for managing Autonomous Aerial Vehicle (AAV) flight, using WISeKey's Cybersecurity IoT technology as shown in Fig. No. 3. Through the partnership, the VIMANA Blockchain Airspace Platform will be secured by the WISeKey RooT of Trust (RoT) technology for IoT, that combines all the hardware, software, and Trust Model required to take the IoT security to a new level. The WISeKey IoT Blockchain is a vertical security framework, a one-stop-shop security software tool with a user-friendly interface and easy-to-integrate API that manages the life-cycle of devices and their digital certificates. Easy to implement, hard to attack, the WISeKey IoT Blockchain framework offers secure solutions even when the IoT device is in an unsecured environment, such as during production or in the field [6].

Fig. No. 3: VIMANA Blockchain Airspace Network.

VI. CONCLUSION

Blockchain in IoT represents the biggest technological disruption since the integration of computing and transaction processing systems. Due to major progress in device innovation and software, it is now possible to bring transaction processing and intelligence to devices everywhere. There are critical adaptability challenges connected with distributed systems, as well as security, coordination, intellectual property management, identity, and privacy. Many institutions and individuals are actively working on these issues and building an open source foundation for the proliferation of this technology.

In this review paper we first studied about what is IoT and what are its security requirements. Then we moved towards blockchain and discussed how the above mentioned requirements can be achieved through blockchain. Finally, we illustrated implementation of blockchain in IoT security.

 DOI : 10.18231/2454-9150.2018.0427

REFERENCES

[1] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo, "A blockchain future for Internet-of-Things security: a position paper", Digital Communications and Networks xxx (2018) 1–12.

[2] Keyur K Patel, Sunil M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International Journal of Engineering Science and Computing, May 2016**,** Volume 6 Issue No. 5.

[3] Minhaj Ahmad Khan, Khaled Salah," IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems 82 (2018) 395–411.

[4] Poonam Ghuli, Urvashi Priyam Kumar and Rajashree Shettar, "A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices", Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2449-2456.

[5] Siva Gopal, White paper on "Blockchain for the Internet of Things", Tata Consultancy Services.

[6] Satyajit Sinha, in blog "Securing IoT with Blockchain", May 11, 2018.

 DOI : 10.18231/2454-9150.2018.0427