Grenze International Journal of Engineering and Technology, Jan 2020

Comprehensive Survey on Blockchain: Applications, Issues and Challenges

Mrs. Pooja Mishra[1] , Mrs. Suvarna Patil[2] and Dr. Manisha Bhende[3]
[1-2]Assisstant Professor, DYPIEMR, Akurdi, Pune, India
pooja.mishra@dypiemr.ac.in, suvarna.patil@dypiemr.ac.in
[3]Associate Professor, DYPIEMR, Akurdi, Pune, India
[3]manisha.bhende@dypiemr.ac.in

***Abstract*—This paper gives a deep literature survey on blockchain protocols for Internet of Things (IoT) networks. Internet of Things is helping all the traditional devices to turn out to be smart. With the advances in the technology the vision is turning into reality, but still there are various challenges which need to be taken care of like in issues in the security area e.g., data reliability. In the recent years the concept of blockchain has come forth as a important technology which will change the way in which the information sharing is done. Building trust in circulated conditions without the requirement for specialists might be a mechanical development that can possibly adjust numerous businesses, the IoT among them. Disruptive technologies such as big data & cloud computing are furnished by IoT to overcome its constraints since its inception, & we assume that block chain is one of the subsequent ones. This paper investigates difficulties in blockchain IoT applications and surveys the most appropriate add order to evaluate but the block chain could possibly enhance the IoT.**

***Index Terms*— Internet of Things, Block Chain, Blockchain Application.**

I. INTRODUCTION

Internet of Things (IoT) is a ubiquitous internet work of intelligent physical objects, called “Things,” and people. IoT enables any "Thing" to connect and interact, making the physical world a huge data system. Various techniques are rapidly becoming an essential component of the IoT fabric, such as cloud computing and machine learning to data analysis and information modeling. In the field of IoT, tremendous progress is also causing development in the company of Information and Communication Technology (ICT). IoT enables new business methods to be developed, and one of its most important elements is information improvement that will influence ICT market growth. The extent to which IoT will be part of our daily lives can be understood by the reality that IoT technology will be at the heart of 95% of freshly launched goods by 2020 [1]. The Internet of Things (IoT) comprises of systems that produce, method and swap vast quantities of data critical to security and security, as well as information sensitive to privacy, and are thus attractive destinations for multiple cyber attacks[3]. Many new IoT-constituted networkable devices are low energy and lightweight. These systems have to devote most of their available electricity and computing to the execution of key application features, making it quite difficult to support safety and privacy affordably. In terms of power usage and overhead processing, traditional safety techniques tend to be costly for IoT. In addition,

Grenze ID: 01.GIJET.6.1.504

many of the state-of - the-art safety frameworks are extremely centralized and therefore not necessarily suitable for IoT owing to the complexity of scale, the many-to - one nature of traffic and the single point of failure. [4]. Existing techniques often either show loud information or incomplete information to safeguard user privacy, which could possibly hinder some IoT apps from providing personalized services[5]. IoT therefore requires a lightweight, scalable and distributed protection of safety and privacy. The Bitcoin's first system of cryptocurrency [6] has the potential to overcome the aforementioned challenges as a result of its distributed, secure and private nature.

With the ever-increasing existence of IoT objects and their Internet visibility, safety, i.e. access to resources by legitimate users, is of primary concern. On the one side, the ubiquitous nature of IoT promotes the development of innovative end-user apps, but on the other side, absence of safety measures can lead to critical problems such as people suffering physical harm as a result of hacking the intelligent alarm system, such as burglary. Security has another element connected with it, namely "the concern for privacy." Centralized businesses that manage sensitive user data may illegitimately use them, resulting in a privacy violation[2]. Aggravating the situation is the fact that a few years ago it was quite unlikely to think about a scenario with billions of linked appliances, which is why the safety elements were not always regarded during the product development stage. Indeed, according to Gartner's global research, IoT security expenditure in 2018 will reach $1.5 billion, and by 2022, half of all IoT security budgets will go to remediation, recall, and security errors rather than protection[1]. Therefore, the progressive company development associated with this sort of always linked settings means fresh technological difficulties and consequences for safety, privacy, and interoperability. A distributed trust technology that ensures scalability, privacy and reliability is a cornerstone of such IoT environments ' development. Due to its inherent safety, the Blockchain (BC) technology has matured considerably in latest years and is seen as a promising alternative in attaining the above-mentioned objectives.

As you see from the Fig. 1, The design of the blockchain comprises of a series of keys connected by their hash values. A public ledger in the blockchain network maintains digitally signed user transactions in a P2P network. This technology uses a public key cryptography to sign inter-party transactions. Transactions are subsequently stored on a distributed ledger. The ledger consists of cryptographically linked transaction blocks that form a blockchain. It is too much difficult to change or remove data blocks recorded on the blockchain ledger. When it comes to enhancing Iot using blockchain, there are so many problems and difficulties, but before that it enables us to know what IoT is.Fig. 1. Blockchain structure. A block in a blockchain architecture is an aggregated set of data, which each block can be identified using a hash function. Specifically, the block contains a header and relevant transaction data. In the header, several pieces of information are entered: the version of the block, the identifier of the previous block, and the date and the difficulty of carrying out the PoW. There are related survey papers [7], [8], [9]–[12] that covered different aspects of the blockchain technologyThe feasibility of multiple consensus protocols in the blockchain was briefly presented by Sankar et al.[9]. Surveys[8] provided an overview of IoT (BIoT) apps based on blockchain.

II. Application

Although the use of blockchain in IoT is comparatively recent, there are already a big range of suggestions that use this technology to enhance present IoT technology in various ways. Table 1 shows a summary of some of these suggestions.

TABLE I. IoT–Blockchain applications

Application	Classification	Platform
LO3 Energy [13]	Energy microgrid	Ethereum
ADEPT [14]	Smart contracts involving IoT devices	Ethereum
Slock.it [15]	Renting/Selling/Sharing smart objects	Ethereum
Aigang [16]	Insurance network for IoT assets	Ethereum
MyBit [17]	Investment in IoT devices	Ethereum
AeroToken [18]	Sharing airspace market for drone navigation	Ethereum
Chain of things [19]	Identity, security and interoperability	Ethereum
Chronicled [20]	Identity, data provenance and automation	Multiplatform
Modum [21]	Data integrity for the supply chain	Multiplatform
Riddle and Code [22]	Sharing and machine economy	Multiplatform
Blockchain of things [23]	Secure connectivity between IoT devices	Multiplatform

As shown in Table 1, Ethereum is the most common platform for IoT – blockchain apps. Ethereum offers more characteristics than Bitcoin, the incorporation of intelligent agreements extends the potential apps considerably. An energy microgrid using blockchain has been demonstrated in LO3 Energy[13]. The project constructs a marketplace for community energy that creates a decentralized P2P energy network that is coordinated with the wider power grid. It is the first ever energy-blockchain platform that enables devices at the grid edge to transact between microgrid participants securely and directly for energy sales. A hybrid device measures the energy generation of a building in use and sends information to the network. [14] seeks at pushing device freedom, and implementing blockchain technology to ensure edge device code execution. The blockchain framework proposed by Slock.it[15] seeks to address security, identity, coordination, and privacy in more than billions of IoT devices. They work on a variety of projects, such as a marketplace to provide electric vehicles with a charging infrastructure called Blockcharge. This alternative utilizes a smartplug, a mobile app to activate the charging plug and control, and a blockchain to pay for the services. Aigang[16] is an independent IoT asset insurance network. Aigang has implemented intelligent agreements that automatically perform risk assessment and process claims over the Ethereum test bed. They developed a tailored digital currency (AIX) in addition. They provide financing possibilities with one-of - a-kind rates of danger and feasible profits in unique products. Smart contracts connect smart devices with policies on the insurance plan. The devices can order renovation through these contracts and the payment of insurance can be automated. Claim coping with can be handled automatically with the inclusion of Oracle to report events.

MyBit[17] plans to build a service ecosystem in which IoT assets (from drones to cars) are owned and revenue shared with a crew of people. A new mannequin for financing and an opportunity for investment open to anyone. Ethereum smart contracts are used to automate procedures: when IoT systems produce revenue, investors automatically receive a share of revenue proportionate to their ownership stake. The platform is controlled, maintained and updated by a key clever agreement. The platform describes one type of asset and IoT devices are connected to resources as quickly as they are installed they send and demand information via an API. Oracles are used to link devices to the network.

AeroToken[18] aims to create an authorization system for real-time navigation and property access for commercial drone services at low altitude. By voluntarily sharing airspace over properties, they provide a solution for drone navigation. This helps solve the drone operation authorization problem, creating a new marketplace for sharing. The application was developed using smart contracts from Ethereum.The Chain of Things[19] is a blockchain-enabled IoT research laboratory that offers Maru, an integrated hardware solution for blockchain and IoT. Many number of products have been developed by choricled[20] which have cryptographic capabilities. This helps in building trust in IoT and thus provides chain ecosystem. This consists of blockchain synchronization server which is capable of synchronizing with more than one blockchain structures Registration and check of device identity is accomplished via smart contracts. The Modum[21] blockchain solution helps to ensure the integrity of data for physical products and is aimed at improving supply chain processes. During shipments, the Modum sensors record environment conditions. Modum was intended to operate with various platforms. A method has been arose to distribute medical products using Ethereum blockchain. Ethereum smart contracts are used to verify sensor data every time the goods change ownership, the contract confirms that the transaction meets the standards of the customer. The solution includes sensor tags that collect measurements during transit, a mobile application for connecting and activating sensors and changing ownership, and a dashboard for analyzing sensor data collected after receipt of shipment. Twin of Things is a remedy designed by Riddle and Code to ensure the possession and cradle of everyday objects[22]. The alternative incorporates blockchain and cryptography to give all linked physical items a hardware-based digital identity. Due to blockchain, communication and operations between computers are carried out autonomously and safely. The chip can interact with other devices when validated in the network. The solution was designed to be an agnostic blockchain, it can currently work with blockchains from Ethereum, Bitcoin and BigchainDB.A safe open communication platform for industrial IoT implementation is provided by the Blockchain of Things[23]. They propose a web service layer for fast inclusion of Bitcoin blockchain, with end-to-end encryption called Catenis.

III. Issues and challenge

When we're talking about BC, we think about Bitcoin right away. That's why we use Bitcoin as an instance of mention.

IoT today represents 5 billion connected devices, and by 2022 this amount will continue to expand and reach 29 billion [24]. Each device on the Internet generates and exchanges information. So, given this huge amount

of machines, it's simple to realize that we're talking about comprehensive and ongoing information manufacturing. It is a challenge in itself to address the basic safety problems for such a large data scheme. We address the difficulties facing IoT deployments in this chapter. IoT's distributed architecture is a key challenge. Typically, each node in an IoT network is a potential failure point that can be utilized to launch cyber assaults like Distributed Denial-of-Service (DDoS) [25]. A node system with multiple infected devices can crash rapidly, acting concurrently. Another issue is its centralized configuration (typically leverages to a core cloud service supplier for the IoT environment)[26]. A vulnerability that has to be resolved is such a key point of failure. The confidentiality and authentication of information is another continuous and likely one of the most critical threats[27]. IoT information can be abused and misused in the lack of data security. In addition, information safety becomes critical with the advent of fresh company models where systems can autonomously exchange resources such as information, computing energy or electricity.
Data integrity[26] is another challenge for IoT. Decision support systems are one of the major apps of IoT. The aggregated information from the sensor fleet can be used to make timely choices. Protecting the system from injection assaults, which attempt to inject false interventions and thus influence decision-making, is therefore crucial. For automated systems such as vehicle networks, manufacturing sectors, and intelligent grids that process real-time information, availability is critical[26]. Sensor downtime may lead in losses ranging from life-threatening circumstances to financial ones. With the advent of Machine Economy, whereby data-generating sensors are capable of trading data in information marketplaces and independent end-to-end system, building confidence between participating organizations is a major challenge[28]. It is desirable to have a publicly verifiable audit trail without a trusted third party, solving the non-repudiation issue.

Challenge	**Explanation**	**Potential blockchain solution**
Deficient Architecture	Each IoT architecture block acts as a bottleneck or failure point and disrupts the entire network; there is also a vulnerability to distributed denial-of-service attacks, hacking, information theft, and remote hijacking.	Secure messaging between devices: the validity of the identity of a device is verified, and transactions are cryptographically signed and checked to guarantee that it could only be sent by the originator of a message.
Cloud server downtime and unavailability of services	Due to cyber attacks, software bugs, energy, cooling, or other issues, cloud servers are sometimes down.	No single point of failure: documents are containing identical data on many computers and devices.
Susceptibility to Manipulation	Information is probable to be manipulated and misused.	Decentralized access and immutability: it can detect and prevent malicious behavior. Devices are interlaced: if blockchain updates of 1 device are infringed, it is rejected by the scheme.
Costs and capacity Constraints	Managing exponential development in IoT systems is a challenge: by 2020, a network capability will be required at least 1,000 times the 2016 level.	There is no need for centralized organization: devices can communicate safely, exchange value between, & implement activities automatically through smart agreements.

IV. CONCLUSIONS

Existing blockchain protocols designed for IoT network has been studied in this paper. All the state of art systems are evaluated on various parameters. Based on parameters like blockchain model, specific security goals, effectiveness, computational complexity, & overhead communication classification and side by side comparison of the existing systems is provided. In the block chain, we have researched the difficulties and feasible solutions. There are still a number of difficult study fields, such as resilience versus combined attacks, vibrant & adaptable safety structure, energy-efficient mining, social networks and trust management, to be explored in the near future.

REFERENCES

[1] Newsroom, G. Gartner SaysWorldwide IoT Security SpendingWill Reach $1.5 Billion in 2018. Available online: https://www.gartner.com/newsroom/id/3869181 (accessed on 30 March 2018).

[2] Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Int. Things J. 2018, 5, 1184–1195 [CrossRef]

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[4] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[5] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013, pp. 23–27.

[6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[7] Jesus, E.F.; Chicarino, V.R.; de Albuquerque, C.V.; Rocha, A.A.d.A. A survey of how to use blockchain to secure internet of things and the stalker attack. Secur. Commun. Netw. 2018, 2018, 1–27.

[8] Civic Technologies, I. CivicWhitepaper. Available online https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (accessed on 21 February 2018).

[9] Lykke. Lykke Exchange: Architecture, First Experiences and Outlook. Available online: https://www.lykke.com/ico/Whitepaper_LykkeExchange.pdf (accessed on 21 February 2018).

[10] Williams, S. Populous Whitepaper. Available online: https://populous.world/invoice-finance/populous_whitepaper_final_v1.pdf (accessed on 21 February 2018).

[11] Suwald, T. Security Token and Authentication System. U.S. Patent 9,898,695, 20 February 2018.

[12] Schor, L. 8 Important Things To Know About Security Tokens/Token Regulation. Available online: https://medium.com/@argongroup/8-important-things-to-know-about-security-tokens-tokenregulation-3d548a1a6367 (accessed on 10 January 2018).

[13] LO3ENERGY, 2017. Available online: https://lo3energy.com/. (Accessed 1 February 2018).

[14] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.

[15] G. Prisco, Slock. It to introduce smart locks linked to smart ethereum contracts,decentralize the sharing economy, 2016.

[16] Aigang, 2017. Available online: https://aigang.network/. (Accessed 1 February2018).

[17] [89] My bit, 2017. Available online: https://mybit.io/. (Accessed 1 February 2018).

[18] AeroToken, 2017. Available online: https://aerotoken.com. (Accessed 1February 2018).

[19] Chain of things, 2017. Available online: https://www.chainofthings.com/. (Accessed 1 February 2018).

[20] Chronicled, 2017. Available online: https://chronicled.com/. (Accessed 1 February 2018).

[21] modum, 2017. Available online: https://modum.io/. (Accessed 1 February 2018).

[22] Riddle and Code, 2017. Available online: https://www.riddleandcode.com. (Accessed 1 February 2018).

[23] Chain of things, 2017. Available online: https://www.blockchainofthings. com/. (Accessed 1 February 2018).

[24] Barboutov, K.; Furuskär, A.; Inam, R.; Lindberg, P.; Öhman, K.; Sachs, J.; Sveningsson, R.; Torsner, J.; Wallstedt, K. Ericsson Mobility Report. Available online: https://www.ericsson.com/assets/local/ mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 30 March 2018).

[25] Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. Comput. 2017, 50, 80–84. [CrossRef]

[26] Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660. [CrossRef]

[27] Sicari, S.; Rizzardi, A.; Cappiello, C.; Miorandi, D.; Coen-Porisini, A. Toward data governance in the internet of things. In New Advances in the Internet of Things; Springer: Cham, Germany, 2018; pp. 59–74.

[28] Hawlitschek, F.; Notheisen, B.; Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. 2018, 29, 50–63.