EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

IoT-Chain: Security of things for Pervasive, Sustainable and Efficient Computing using Blockchain

Mohd Majid Akhtar[1,*] and Danish Raza Rizvi[1]

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi, 110025 India

Abstract

This paper unfolds the infancy of the exquisite experience of the *'Internet of Things'*. It will address the thrilling potential of the looming opportunity of IoT & will echo the integration of things when harnessed with the bubble of internet. The topic is vulnerable due to handful factors but chiefly improves the insights and will observe exponential rise in the *'Next generation'*. The new rule enchanted for future will be "Anything that can be connected will be connected". Moreover, cognitive consciousness of people will understand that IoT is the next big thing without procrastinating, in particular. This paradigm will review the implementation and challenges of several domotics technologies and others in general within the communication field and its contribution to the *'Smart World'*, exploring supplementary in fields of healthcare, living culture, transportation and furthermore that collectively rise for the world of Ubiquitous computing or Pervasive computing around us. Pervasive computing in short serves as a meaning where smart devices are connected as network and available all time. By scratching past, we have seen DDoS attack happening in 2016 via botnet attacks & malware from the devices such as IP security cameras, routers, printers. IoT as of now, have taken steps for the security but still lacks for the major part. Blockchain, the revolutionary technology behind the famous Bitcoin, which is cryptographically secured and decentralized, hence, can act as the liberator for the security of IoT devices. Blockchain in short are distributed immutable ledger that maintains the integrity of the network by achieving consensus algorithms like Proof of Work or Proof of Stake. Hence, an attacker won't be able to take down the IoT devices as easy as it was taken down before and eventually, harder to attack or hack the network. This manuscript discusses the use of Blockchain technology implementation for the security of IoT devices along with the sustainable and energy efficient solution towards the problem stated and addresses the limitations, if any. We also discuss the future prospect for IoT, blockchain and other possible architectures.

Received on 27 March 2020; accepted on 02 May 2020; published on 20 May 2020

Keywords: Internet of Things, Blockchain, Security, Pervasive Computing, Sustainable and Energy Efficient Computing, Cryptography, Decentralization

doi:10.4108/eai.13-7-2018.164628

1. Introduction

This is a fact that we live in a far more complex digital age than what we use to live forty years ago. Digital era has acquired so much of place around us as well as in our life's ranging from handheld devices like mobile, tablets or laptops to home devices like Alexa, Google mini, smart A.C, smart T.V or even a smart fridge that is intelligently programmed to order eggs from supermarket on the behalf of owner whenever egg tray goes empty. We might never acknowledge each second that we are spending and interacting with the technology specifically IoT (Internet of Things) on a daily basis.

Internet of Things is the concoction of communication within devices with other devices in the physical real world. All smart IP enabled devices such as IP cameras, thermostat, fit-bit, smart geyser, or smart AC

*Corresponding author. Email: akhtarmajid273@gmail.com

all work in a complimentary fashion sharing real world data between them. For example, when a person enters into home, sensors might feel his presence or the camera can see him and convey AC to turn on in accordance with the thermostat sensing room temperature. IoT echoes the integration of things when harnessed with the bubble of internet. With the help of smartphones in our palms, everything is one touch operable from any part of the globe. According to Gartner Inc. Report, 5.8 Billion enterprise devices will be in use by 2020 with annual increase of about 21%[1]. Although other reports from Statista or IoT-Analytics forecast this number with a much higher value around 22 Billion devices by 2025[2] also seen in Figure 1.

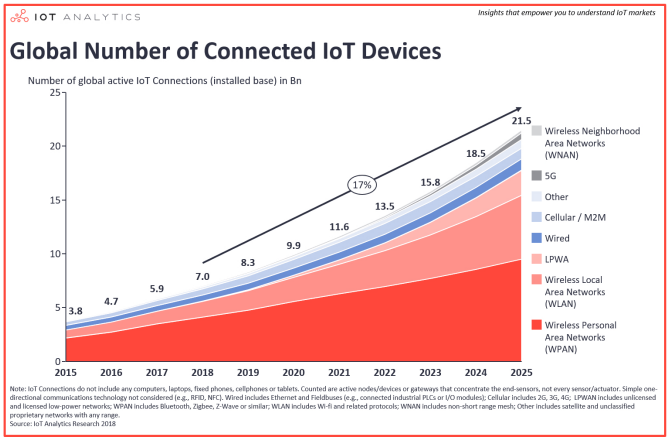

Figure 1. Expected Number of IoT devices by 2025, Source: IoT-Analytics

Internet of Things (IoT) is no longer a futuristic concept, instead it's already here. Many startups and companies are working day and night for building solutions around IoT for society. Yes, with the help of these innovations, we can now control the IP printers or IP cameras in our homes just from our smartphones from anywhere around the globe through internet. But little we know the journey of these interactions of communications between M2M (machine to machine) models, what is the state of security, and overall energy consumption. This paper aims to give the insights of future of IoT, as it is in the early development stages seen in the Figure 2 and nowadays getting more and more technical sounded people getting attached to it and the community is growing each day. You can easily order many smart gadgets online these days.

This paper is organized as follows: Section 2 explains the problems with current IoT implementation and the motivation of the research work. Section 3 discusses the existing solutions and lay basis for literature review and also highlights the implications of existing blockchain architecture. The proposed paradigm solution and the need of blockchain architecture are explained in detail in Section 4. Section 5 enlightens the critical analysis of proposed paradigm and gives the modification required for it. Future prospect for IoT, blockchain and other possible architectures is analyzed in Section 6 and Section 7 concludes the paper.

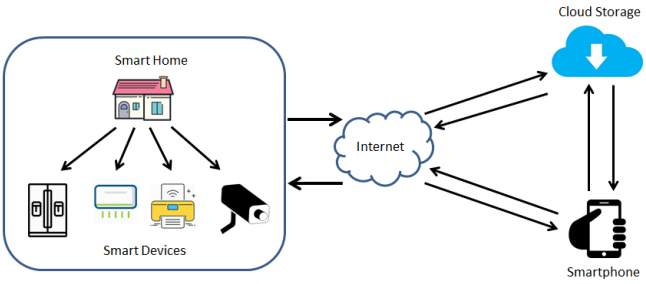

Figure 2. Architecture of IoT (Smart Home Example)

2. Problems with Current IoT Implementations

IoT applications come with lot of ease like it is omni-present and pervasive (in short serves as a meaning where smart devices are connected as network and available all time). However, the topic is vulnerable due to handful factors but chiefly improves the insights and will observe exponential rise in the 'Next generation'. The new rule enchanted for future will be "Anything that can be connected will be connected". Major problems seen in IoT implementations are:

(i) **Lack of Standardization**: Different countries or continent act differently towards creating solution related to IoT. Europe has different standards than what Asia showcase. Standardization is one of the reasons why we find different variants of IoT devices in market some running on Wi-Fi module others on Zigbee hinting towards heterogeneous variants of devices and lack of central control. European Union is making big efforts in presenting standard OneM2M model. With advancement even in the ICT (Information in Communication and Technology) sector, introduction of 5G, communications are enormously going to increase and a standardized protocol must be established;

(ii) **Security**: Privacy is always one's right to hold. No compromise can be made to this. Companies tends to say they have paid attention to the security and privacy but little we know these devices can be easily hacked as they hold weak

[1]https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io
[2]https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b

passwords by default and also no encryption is present at all in message sharing. Companies have realized that they can't send raw data in packets. Some encryption technique must be applied as the data is going to stay in air for anyone to listen. By scratching past, we have seen two DDoS attack happening in October, 2016 on Dyn (domain registration service to giants like Netflix, Twitter, etc.) with an uncontrollable speed of 665 Gigabytes per second, the largest DDoS ever recorded. Initially, it was assumed that it happened from a lab seeing that huge incoming bogus request. Later, it was known that it happened via Mirai botnet attacks & malware from the devices such as IP security cameras, routers, printers only. According to report by The Guardian, David Fidler, adjunct senior fellow for cybersecurity at the Council of Foreign Relations, said he couldn't recall a DDoS attack even half as big as the one that hit Dyn. "We have a serious problem with the cyber insecurity of IoT devices and no real strategy to combat it", Fidler added[3].

Initially, the attack was done on computers by sending them malware, but this malware got linked to all the IoT-devices, the computer was connected with. Ultimately, the attacker gained new set of computing power which was harnessed to do DDoS attack on Dyn and can affected areas can be seen in Figure 3. This was done three years ago when the adoption of IoT and the IoT-devices itself were much lesser in number. Now, we can imagine the risk involved as the devices will increase enormously in future and we don't want those many mini computers or smart devices getting in the hand of bad actors for their personal illicit use. To this same thought, Fiddler added, "imagine what a well-resourced state actor could do with insecure IoT Devices".

Motivation to carry out this research is derived from the problems stated above. It is must to resolve the current issues in implementations of IoT solutions in order to fully move to the next generation edge computing. Once we are assured of the security, integrity and authenticity of data and the hardware through the proposed solution discussed in the latter of this paper, automating these devices for edge computing will become an easy task to carry out. In edge computing, data can be troublesome due to its centralized based nature. This results in the motivation of this research work to discuss about a new paradigm which is distributed and decentralized in nature. The solution discussed in this paper will help the IoT Hardware vendors, a better data analytics which help in better decisions, and a secured & sustainable IoT ecosystem.

[3]https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

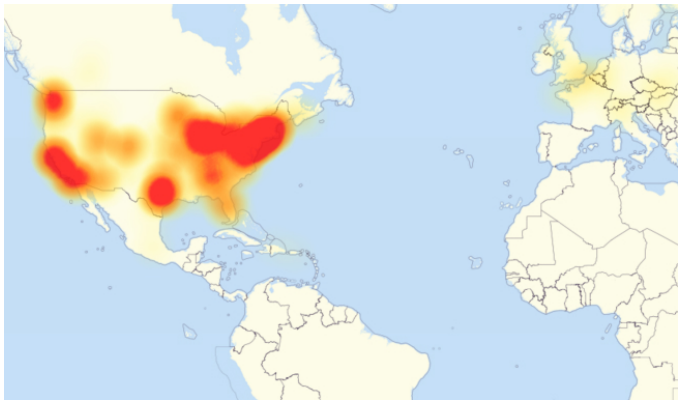

Figure 3. Map of areas most affected by attacks, 16:45 UTC, 21 October 2016, Level3 outage map – Down Detector/Level3

3. Literature Review

A tabular version of literature survey in the blockchain domain are given in Table 1. Security of IoT ecosystem is vulnerable with traditional methods. These exhaustive research surveys in aspect of security on the existing solutions show that there is need of better solution (Sadeghi et al. 2015, J. Granjal et al. 2015, F. Restuccia 2018)[1][2][3]. According to Tata Consultancy Services (TCS) whitepaper (Siva Gopal, 2016)[4], blockchain recommendations for IoT includes promotion of trust, reduction in cost, increased security for IoT and boosting of data exchanges. Ali (Ali Dorri et al. 2016)[5] in his paper gave blockchain based architecture for smart home using overlay network while considering the resource constraints of IoT devices. They also did evaluation on many known attacks like DoS attack, modification attack, dropping attack and mining attack[6]. Similar hub like architecture was proposed by (O. Novo 2018)[7]. Another attempt was done by IBM Research group for IoT using PoW sub-blockchains and performed evaluation on bitcoin simulator under settings with three different device locations i.e. Europe, Netherlands and others like Dhaka, Istanbul, San Diego and Melbourne known as the world. The number of IoT devices was varied and hence, 250 devices is found to be the optimal setup as it produces more genuine blocks and achieves the highest throughput. Block generation intervals should be minimum enough & blocks smaller than 1MB should be used as well. IBM paper also gave some valid guidelines after three evaluations where sub-blockchains must contain few IoT devices (G. Sagirlar et al. 2016)[8].

Table 1. Analysis of Related Papers in this domain

Author and Year	Short Description of Work	Techniques used	Performance	Source of Publication
Ali Dorri, Salil S. Kanhere, Raja Jurdak [Aug 2016]	This gave a theoretical model of Block based IoT Architecture in which Overlay network is used along with cloud storage.	Own architecture is given that is a lot like bitcoin blockchain but without mining.	Very complicated architecture that is not energy efficient. Also nothing is said about how miners or nodes are made.	Arxiv.org, Cornell University, under Cryptography and Security as "Blockchain in the Internet of Things: Challenges and Solutions"
Gokhan Sagirlar, Barbara Carminati, Elena Ferrari, John D. Sheehan published in [July 2018]	They used Bitcoin simulator to give metrics about the efficiency and throughout.	They distinguished the network based on the size of block, number of IoT devices and the device location and then evaluation is performed	This is just a simulator and not the system itself.	Arxiv.org, Cornell University, under Distributed, Parallel and Cluster Computing as "Hybrid-IoT: Hybrid Blockchain Architecture for IoT- PoW Sub-Blockchains"
Ali Dorri, Salil S. Kanhere, Raja Jurdak in [March 2017]	They tried to remove Proof of Work and gave blockchain based framework.	They used Smart Home miner and overlay network along with it.	They analyzed and evaluated the system based on energy consumption and time overhead.	IEEE International Conference on Pervasive Computing and Communications as "Blockchain for IoT security and privacy: The case study of a smart home"
Francesco Restuccia, Salvatore d'oro in [November 2018]	They reviewed various papers on scalability issues.	They addressed the scalability issues and reliability issues.	They analyzed IOTA and other solutions	IEEE Internet of Things Journal, Research Gate archive as "Blockchain for the Internet of Things: Present and Future"

(Muhammad Salek Ali, Massimo Vecchio et al. 2017)[9] did comprehensive survey on the same issue and concluded with summary of reviewed research contributions. They did analysis on parameters like privacy, identity management, data management, access control, etc. Similar kind of work was found from (Alfonso Panarello et al. 2018)[10] for blockchain and IoT Integration. (Sunghyun Cho 2019)[11] survey paper on the application of blockchain to IoT introduces research trend in this field. Although, all the attempt to solve the problem is very original but there is a lack of critical analysis in these papers stated above.

4. Proposed paradigm solution using Blockchain

Blockchain, the revolutionary technology behind the famous Bitcoin, which is cryptographically secured and decentralized, hence, can act as the liberator for the security of IoT devices. Blockchain in short are distributed immutable ledger that maintains the integrity of the network by achieving consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS). Bitcoin[12] and early Ethereum Blockchain (Vitalik Buterin, Gavin Wood, 2013)[13] run Proof of Work (PoW) algorithm as base protocol to achieve consensus in network and to verify the work done by miners. According to their work done for finding valid nonce, miners are rewarded back with the intrinsic token i.e. coin of the network. Doing any task on blockchain requires some gas amount (reward for miners) associated with each transaction. So in this paradigm, we add one more tier in the architecture of IoT i.e. Blockchain tier. Blockchain offers security, integrity, decentralization and scalability. Scalability (increase of computing nodes in the network)

in practice differs from blockchain to blockchain platforms like if the platform is permissionless blockchain i.e. Bitcoin and Ethereum; scalability is always an issue unless sharding is applied. On the other hand, if we have permissioned blockchain built on Hyperledger fabric or composer for enterprise, EOS, etc., in this scalability of nodes are not problem anymore. So, for scalability it depends on the type of problem and on whether we want permissioned blockchain or permissionless blockchain.

In our paper we will take example of Bitcoin Blockchain to understand the underlying technology and later understand other blockchain paradigms once we set a direction where we want to lead. Hence, in general, each transaction (if updating the state of blockchain) requires fees to happen and this transaction goes in a transaction pool waiting for miner to validate it & add it in a block which gets added to the main blockchain. If the transaction is only reading the data from blockchain then no fees will be charged. Blockchain just acts like a database with complex conditions on write operations. These conditions are jotted down in an electronic piece of code (logic) known as *'Smart Contract'* that interacts with blockchain. Smart contract was first time coined by Nicholas Szabo (Nick Szabo 1997)[14] but it was put best in work by Nakamoto. They are actually misguided by name. They are not actually smart, neither any contract in real sense. They are just a piece of code that codifies business logic and at the core, they perform three functions; they contain constraints (rule), they verify these logic constraints and they automatically execute them. Hence, this is basis for working of smart contract, so everything goes through them and since they are built on top of blockchain application, there is no broker, there is no agent, middlemen, government (in some cases), or a corporation, not even a lawyer. It executes automatically. Hence, to incentivize this method, we pay fees to miners for mining new coins and verifying transactions.

This fashion may seem little expensive, but this is what keeps a fraudulent away from the network as he/she would have to spends tons of dollars just for sending bogus requests to the server. Now imagine, will Dyn attack be possible? Probably not because who will pay for each bogus request. So ultimately it does put a stop on these types of bad actors.

Other feature that this paradigm offers is the security as we put our trust on cryptography, blockchain really provides a secured way of transactions and it uses key pairs (private key and public key) in which private key is use to sign these transactions and public key verify that these are authentic. This way it overcomes the different variety of security issues and concern in the IoT ecosystem present in (Bandar Alotaibi 2019, Kouzinopoulos et al. 2018)[15][16]. This new architecture is shown in Figure 4.

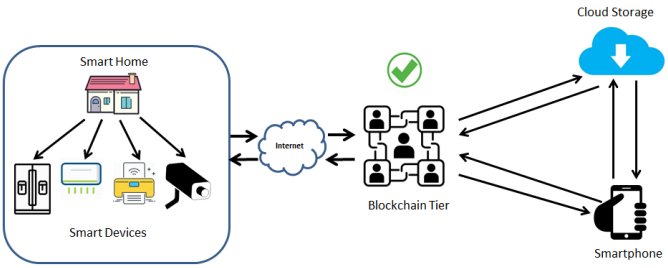

Figure 4. New IoT Architecture after adding Blockchain Tier

5. Critical analysis of proposed paradigm and other existing solutions

After the whitepaper (Satoshi Nakamoto, 2008), blockchain is hardly ever looked more on the negative side. But blockchain do have some limitations, they are not a *'master key'* to all the problems. Blockchain naturally comes to solve many problems but not every problem is built to get solved with blockchain. The engineer must understand why and when to use blockchain. In this paper, blockchain is looked as the liberator for the security of IoT devices but what about the energy consumption used by blockchain powered platforms or a miner? According to Satoshi Nakamoto, he wanted number of Bitcoin (BTC) to remain constant, so difficulty level increases annually. In 2009, you could mine 200BTC from your personal computer, but now in 2019, it would take your 25 years to mine 1BTC. Now, with continuous increase in difficulty level, miners invest more energy on the algorithms like Proof of Work (PoW). *Digiconomist* report ascertains bitcoin mining account for 0.29% of the world's annual electricity consumption. Under observation, in order to mine a single block (containing multiple valid transactions), it is found to consume energy equivalent to energy consumed by 28 U.S. homes for a day[4]. It also estimates that Bitcoin uses as much energy as Chile country as a whole.

PoW is truly computationally expensive, and as more and more bitcoin will be mined, difficulty level will increase and eventually computation for solving mathematical problem (finding nonce value) will take more energy and time. So only miners with high computation power resources is able to do so. We often see mining pools, where if one miner is not able to mine bitcoin alone, he get associated to a groups of miners known as mining pool, leading to enough resource that mining is possible and everyone gets their

[4]https://digiconomist.net/bitcoin-energy-consumption

share in accordance to their input mining hash power. Monopoly has started showing its sign as a weakness and it is hindrance to new miners that want to enter into the mining game. As shown in pie chart Figure 5, pools like F2Pool, Poolin & BTC.com are giants in this market and also Chinese pools lead among the world shown in other Figure 6. Hence, Proof of Work often sometimes is regarded as Proof of Waste. To make this sustainable and energy efficient solution, we can replace the consensus protocol Proof of Work (PoW) with Proof of stake (PoS).

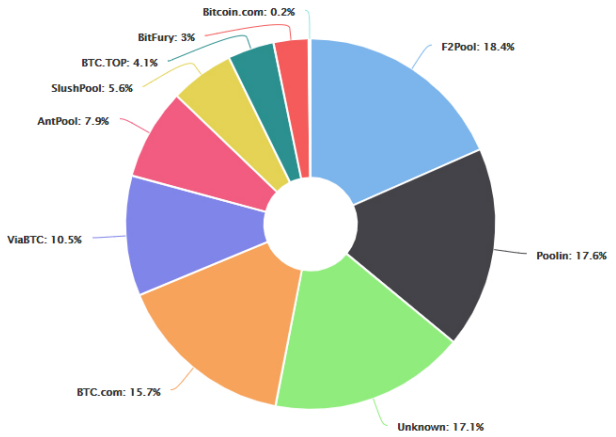

Figure 5. Hashrate Distribution of 2019 (October), Source: Blockchain.com/pools

PoS was first time introduced in 2011, in Bitcoin Talk forum. In PoS protocol, systems start by distributing precoins or the system may start with PoW initially and later convert into PoS like Ethereum is soon going to change into proof of stake. Since, PoS is another consensus protocol where many miners compete against each other for forging a block rather than mining a block. Here different parameters are kept in mind, like randomized block selection & coin age selection. In randomized block selection, validators present stakes and hash value before becoming validator and these stakes are public. Then algorithm is set to choose one with optimal hash value and stakes. Coin age selection method chooses nodes according to the number of days coins are staked and coin age value. This is calculated by multiplying 'number of days staked' and 'number of coins staked'. After becoming validator, that node in particular can forge a block and then the age of coin stake will go to zero. To forge again in future, the node has to wait. This put stop to big giants from dominating the blockchain network. In this, the forger gets fees associated with each transaction as reward for verifying all transactions. If a node doesn't want to be forger anymore, its stake and the reward are kept for some time within the network for verifying fraudulent blocks added to the blockchain by this node. If all goes well then the coins are released but if anything is found wrong, the forger will be penalized, and lose right to enter again as validator.

Summary of Mined Blocks

Miners/Pool	count
Poolin	57
F2Pool	55
Unknown	52
BTC.com	49
ViaBTC	38
AntPool	26
SlushPool	14
BitFury	11
BTC.TOP	9
Bitcoin.com	1

Blocks Mined By Miners/Pools in the last 48 Hours (As of October 2019)

This summary shows the dominance of Pools in Mining

Figure 6. Blocks Mined by Top Pools according to market share, October 2019, Source: Blockchain.com

Blockchain using PoS are also known as greener blockchains, as well as there is a nonprofit organization named Bitcoin Green, that estimates their blockchain will use at the very most 0.06 percent of bitcoin current network energy consumption[5].

Sustainable development is the need of the hour. To support sustainable and energy friendly solution, this blockchain architecture can also add up following benefits to the society around us:

(i) **Reward healthy behavior**: This solution can reward cryptos to users based on their healthy behavior i.e. user can sync their fit-bit data with a mobile app, and based on the steps they take, they earn more cryptocurrency rewards. This promotes more healthy behaviour and user is more motivated to earn these rewards;

(ii) **Bike Sharing**: More and more people can rent their bike (cycle) to others and earn cryptocurrency rewards on the portion of time they rented it. This way it save more petrol and reduce fuel consumption;

[5]https://www.eniday.com/en/technology_en/blockchain-goes-green/

(iii) **Data Exchanges and transactions**: Blockchain with enhanced consensus algorithms produces low carbon emission and is more scalable than before. Moreover, data exchanges between devices are more secured due to underlying cryptography;

(iv) **Sharing of energy using grid management**: People can have their own solar cells on top of their house, and they can rent this energy stored to nearby areas. All this can be done by smart contracts. Power transmissions from power plants are estimated to lose 8% of energy while travelling[6]. If power is transmitted from these solar panels, this way user can also earn rewards for renting stored energy and also this energy can be used for mining operations in blockchain as shown in Figure 7.

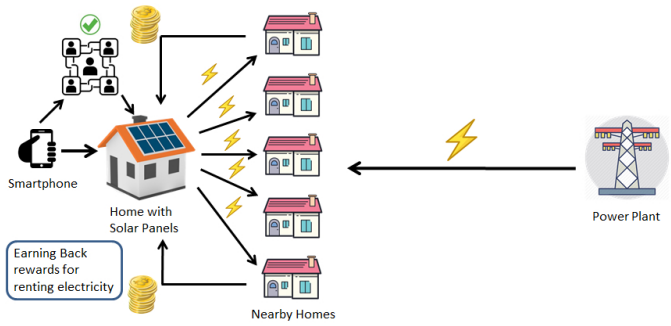

Figure 7. Sharing of energy using blockchain for energy saving environment

6. Future prospect for IoT and Blockchain

IoT is here to stay, but blockchain is just an architecture similar to a door, which is upon us, how to use it. IoT problems can also be solved by using other techniques like IOTA[7], which uses Tangle as the core protocol. It is theoretically more scalable than any blockchain platform. It is fast and it uses protocol in which as more and more number of people will join the network, it will behave more stable and better. IOTA is new, and more recent developments are coming up day by day. Experts suggest that IOTA could be the 'next big thing' for IoT devices as it will also provide support for micro payments and transactions that will happen between machine to machine (M2M).

Another possible vision for IoT devices could be Elastos OS[8]. It is blockchain powered OS with inbuilt support for IPFS (InterPlanetary file System)[9], and development of Elastos started around 18 years ago. It will use same interface as Android and since it is built through blockchain, it will be prevented from hacking, malwares, phishing, prevent content tampering etc. This will trigger more adoption and attention for security of IoT devices and also increases trust in using more domotics technology.

[6]https://blog.se.com/energy-management-energy-efficiency/2013/03/25/how-big-are-power-line-losses/
[7]https://www.iota.org/
[8]https://medium.com/gurucapitalng/what-is-elastos-a-simple-summary-3c4eb5831271
[9]https://ipfs.io/

7. Conclusion

Integration of IoT and blockchain (using PoS) harness a sustainable and energy efficient solution as well as provide security, accountability, and offers other benefits like energy sharing using smart contracts, getting rewards, etc. Blockchain in short are distributed immutable ledger that maintains the integrity of the network by achieving consensus algorithms like Proof of Work or Proof of Stake. Hence, an attacker won't be able to take down the IoT devices as easy as it was taken down before and eventually, harder to attack or hack the network. This paper discussed the use of blockchain technology implementation for the security of IoT devices along with the sustainable and energy efficient solution towards the problem stated and addressed the limitations of reducing high computational power while solving extensive mathematical puzzle in PoW. We also discussed the future prospect for IoT, blockchain and other possible architectures like IOTA and Elastos OS. Blockchain is surely the liberator for security of IoT devices and the security of things for the pervasive, sustainable and energy efficient computing, giving rise to IoT-Chain.

References

[1] Sadeghi, C. Wachsmann and M. Waidner (2015) *Security and privacy challenges in industrial internet of things*, Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015, pp.1–6.

[2] J. Granjal, E. Monteiro and J. S. Silva (2015) *Security for the internet of things: a survey of existing protocols and open research issues*, IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312.

[3] F. Restuccia, S. D'Oro and T. Melodia (2018) *Securing the internet of things in the age of machine learning and software-defined networking*, IEEE Internet of Things Journal.

[4] Siva Gopal (2016) *Blockchain for the Internet of Things*, Tata Consultancy Services, Whitepaper.

[5] A. Dorri, Salil S. and R. Jurdak (2016) *Blockchain in Internet of Things: Challenges and Solutions*, arXiv, arXiv:1608.05187.

[6] A. Dorri, Salil S., R. Jurdak and R. Gauravaram (2017) *Blockchain for IoT security and privacy: The case study of a smart home*, In proceedings of IEEE International Conference on Pervasive Computing, pp. 618-623.

[7] O. Novo (2018) *Blockchain meets iot: An architecture for scalable access management in IoT*, IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195.

[8] G. Sagirlar, B. Carminati, E. Ferrari, J.D. Sheehan and E. Ragnoli (2016) *Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things – PoW Sub-Blockchains*, arXiv, arXiv:1804.03903v3.

[9] Muhammad Salek Ali, Massimo V., M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani (2017) *Applications of Blockchains in the Internet of Things: A comprehensive survey*, IEEE Communications Surveys & Tutorials, Vol. 21, NO. 2, Second Quarter.

[10] Alfonso Panarello, N. Tapas, G. Merlino and F. Longo (2018) *Blockchain and IoT Integration: A Systematic Survey*, MDPI Journal, Sensors, 2575; doi:10.3390/s18082575.

[11] Sunghyun Cho and Sejong Lee(2019) *Survey on the Application of BlockChain to IoT*, IEEE International Conference on Electronics, Information, and Communication (ICEIC).

[12] S. Nakamoto (2008) *Bitcoin: A Peer-to-Peer Electronic Cash system* (Online), Available: http://bitcoin.org/bitcoin.pdf.

[13] V. Buterin and G. Wood (2013) *Ethereum: a secured decentralized transaction ledger*, (Online), Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[14] N. Szabo (1997) *Formalizing and securing relationships on public networks* (First Monday), Vol. 2 , NO. 9.

[15] Bandar Alotaibi (2019) *Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review*, IEEE Sensors Journal PP(99).

[16] C. S. Kouzinopoulos, G. Spathoulas, K. M. Giannoutakis and K. Votis et al. (2018) *Using blockchains to strengthen the security of internet of things*, International ISCIS Security Workshop. Springer, 2018, pp. 90–100.