Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 155 (2019) 704–709

Procedia Computer Science

www.elsevier.com/locate/procedia

2nd International Workshop on Recent advances on Internet of Things: Technology and Application Approaches (IoT-T&A 2019)
August 19-21, 2019, Halifax, Canada

Blockchain - based IoT: A Survey

Riya Thakore [a], Rajkumar Vaghashiya [a], Chintan Patel [a], Nishant Doshi [a,*]

[a] *Department of Computer Engineering, School of Technology, Pandit Deendayal Petroleum University, Gandhinagar, India*

Abstract

Blockchain and Internet of Things (IoT), two of the top disruptive technologies, are already on their way of reshaping our future of the digital world, characterized by a drastic change in the current network architecture. Incorporation of IoT has brought the objects around us to life, making them 'smart' and capable of communicating with each other, thereby amassing massive data by constantly capturing the physical world, for analyzing and performing some intelligent action based on the same. It has made possible our dream of seamless integration of the digital and physical worlds, changing the very essence of our perception of the physical world. But, the problem with current IoT solutions is its need for a centralized party (like a cloud server), for connecting and communicating via the Internet, which poses a great threat to the privacy and security of the vast sensitive data being generated, whereas the original architecture design demands for a decentralized one like distributed or peer-to- peer (P2P) system. So, blockchain comes into play, providing a secure and trustworthy way of sharing information using a distributed/P2P model, to achieve transparency, security, privacy, auditability, resilience, access authentication, data immutability, etc. In this paper, we will look into how to combine both the technologies to overcome their shortcomings and obtain a greater gain from their benefits. We have presented a comprehensive survey on the basics of both the technologies, and the blockchain-based IoT (BIoT) architecture, protocols and functioning, and few examples BIoT applications that can be built on top of it, and comparison.

Keywords: Internet of Things (IoT), Blockchain, BIoT, Applications, Protocols

1. Main text

In order to bridge the gap of the digital and physical world, IoT has brought it to life by lending the objects cognitive senses to serve us better. IoT has been incorporated into various sectors to provide an increasingly cognitive environment for delivering tailored services to the users and improve their overall experience. Due to various problems as discussed in the paper below related to IoT, a well-connected and concerted operation and management is needed. So, Blockchain comes into the picture and the combination helps enable autonomy and support P2P communication since the combination would remove technical bottlenecks and inefficiencies.

* *Corresponding author*. Tel: +91 79 23275458;
E-mail address: Nishant.Doshi@sot.pdpu.ac.in

10.1016/j.procs.2019.08.101

Future research suggestions for BIoT could be inventing a feature or a new technology having similar characteristics to Blockchain which would decrease power consumption and computation time. Other future work includes the method to assure the safety and confidentiality of devices in Blockchain and the best cost-efficient way to use blockchain based safety clarifications. Following is the organization of the paper: Section II provides Strength and Platform for IoT and the problems in current IoT solutions, Section III provides Working and Types of Blockchain and the motivation for BIoT and Section IV provides Design for optimized BC for IoT which includes Architecture and Cryptographic algorithms. The above outline of the contributions of this paper relative to other literature can be highlighted since we have provided a detailed summary of IoT and Blockchain and the need to integrate both these technologies.

2. IoT

The concept of IoT started way back in the 1970s, by British technology pioneer Kevin Ashton while working on RFID at Procter and Gamble [1]. The increasing availability of the Internet has improved information exchange worldwide and IoT promises to deliver new opportunities which can provide competitors edge over the others as it can span across huge domains ranging from a single system to multiple-platform deployments and cloud systems in real time [2][3].

Strength of IoT

Due to the network of devices, a person can access data irrespective of their location making it convenient for people to use. When communications are not fluent and transparent, inefficiencies are caused, but with a network of interconnected devices, better communication is possible, as transferring data packets over connected network save time and money[5]. IoT not only helps to save time and money but achieve automation- the most important aspect in today's tech-savvy life where all the tasks can be achieved without human intervention, with increasing quality of services.

Platform

IoT system utilizes hardware part (sensors) to collect information from the environment and needs connectivity to transmit and receive data to and from cloud/server. The software part in IoT helps in analyzing data and make decisions, and a user interface helps users to interact with system[6]. IoT platforms are the support software that connects everything in an IoT system, facilitating communication, data flow, device management, security, authentication and the functionality of applications[7]. For efficient inter-process communication and management of the network, various standardized protocols such as CoAP, XMPP, MQTT are used.

Problems in current IoT solutions

By design, IoT is a decentralized network in which devices communicate with each other to carry out the specific tasks. But current IoT solutions have a centralized brokered communication framework, wherein all the data is stored at a central data storage, like cloud servers, making it susceptible to Byzantine failure. This makes it a critical bottleneck factor affecting the performance of the system, owing to the large scale of devices in the network and increasing traffic which introduces operational delays and redundant data transfers. Also, the client-server model is very expensive in terms of high infrastructure costs, low inter-operability due to restricted data aggregation and heterogeneity of devices, coordination with other centralized IoT frameworks, maintenance costs, networking equipment costs, etc. and cloud server becomes a single point of failure, hence disrupting the entire network and renders services useless in event of an attack [8][9]. In order for IoT to succeed, well-connected and concerted operation and management are needed. IDC had predicted that almost 90\% of organizations implementing IoT will suffer IoT-based breach of back-end IT system in near future [10].

Using a decentralized architecture will alleviate if not eliminate all such costs, such as the reduction in redundancy and amount of data transfers, improvement of services, Byzantine fault resistant, better protection against threats and attacks, privacy and secrecy of data, autonomous operations, management and operational costs of servers. But IoT applications deal with a huge amount of sensitive and personal data and it requires a standardized P2P communication model, which is able to provide validation of devices and authentication of data generated by them in order to prevent mistrust and theft in the network. To cater to these problems, Blockchain is one of the major such technology which includes many of these features in its design, and hence can be leveraged for securing IoT network.

3. Blockchain

Blockchain consists of two parts – Blocks, which contains a set of transactions and other records like hash values and Chain, which is a cryptographic arrangement of blocks using hash values of previous blocks. It is designed to overcome the need for a central arbitrator to provide digital trust for coordinating transactions among entities [13], and is robust to Byzantine Fault Tolerance, since everything recorded is available to all nodes in the network, to verify and audit independently and inexpensively [15], and also solves the double-spend problem. It leads to the formation of an incorruptible shared digital ledger[16] having the capability of recording everything. Blockchain introduced in 2008 underpinning a cryptocurrency Bitcoin ("Bitcoin: A P2P Electronic Cash System") [17]. But the most primitive form of blockchain technology was depicted by Stuart Haber and Scott Stornetta in 1991, which prevented tampering of cryptographic hash linked timestamped digital documents [18]. Later, Merkle tree [19] was used for combining multiple such documents into a single block to improve efficiency.Since the last decade, blockchain has gained much momentum, leading to rapid development in the community, and its scope is now no longer limited to cryptocurrency

Working

The basis for building a blockchain is a P2P network comprising of all the devices required to meet the goals of the application. Asymmetric cryptography is employed, such that each of the nodes is assigned two keys: Public key for identifying a device in the network and Private key for signing the transactions to itself or other devices in the network [24].Whenever a device wants to carry out a transaction, it signs using its private key and sends it to its neighbors for verification, which disseminates it further into the network. The private key serves for authentication and integrity and once validated by the network, various such transactions are packed into a timestamped block by miners. The validation of block can be done by various methods, and then it is broadcasted into the network, where all the nodes verify the block and its transactions, and the hash linkage to the previous block. Once verified, it is added to the chain and updated, otherwise discarded. Blockchain is based on four main concepts:

- **P2P network -** Removes the central Trusted Third Party implying all nodes within the network have the same privileges.
- **Open and distributed ledger** - Transparent network and each node can determine the validity of a transaction individually.
- **Ledger copies synchronization** - Nodes have their own copy of the same ledger. Hence to synchronize ledgers across techniques are used to publicly broadcast the new transactions to the network, to validate the new transactions and to add the validated transactions to the ledgers.
- **Mining** - In a distributed system, there are network delays and not all of the nodes receive the transactions blocks at the same time. Thus, there is a need to prevent every node from adding a transaction to the chain because the chain must only have a single valid and ordered branch.

It is the most critical aspect of the blockchain and its whole strength lies in it. It must be asymmetric, that is difficult to find and compute, but easier to verify. For validation, the basic prerequisite is that the majority of the nodes in the network must be honest. One of the typically used consensus algorithms is Proof of Work (PoW). In PoW, the miner must solve a very computationally difficult problem- a very resource and energy consuming task. Though it is criticized, it is what gives the value to the performed work. The miner who first solves the puzzle broadcasts the block into the network for validation and gets a reward for the same, hence incentivizing the miners to stay honest. This creates a "democracy of computing power", which is assured by the multitude of nodes in the network. Various other consensus algorithms are Proof of Stake (PoS) - a biased one wherein the miner is selected on basis of the 'stake' (resources) it possesses- Delegated-Proof-of-Stake, Proof of Capacity or Proof-of-Space, Ledger Consensus Protocol(XLCP), Stellar Consensus Protocol (SCP), etc. The block in the chain contains two elements: Header consisting of a timestamp, difficulty target of the PoW, the hash value of the previous block header, a Merkle tree root, and the nonce which is required for solving the PoW and to prevent a replay attack and Block content containing all the inputs and outputs of each transaction. Based on its functioning, it can be categorized into two types: Permissioned which limits the actors which can participate in limited system consensus and Permissionless which allows any number of actors to join the system system.

Types of Blockchain

Table 1. Comparison of types of blockchain

	Public Blockchain	Private Blockchain	Consortium or Federated Blockchain
Aim	Used for solving efficiency, security and fraud problems within traditional financial institutions, and reshape the way the financial system works, and has potential to disrupt current business models through disintermediation	Mostly used in database management, and auditing among other fields. Used for tasks to a single company, by setting up groups and participants who can verify the transactions internally.	Operate under the leadership of a group, for a specific cause. But no entity having access to the Internet can involve in transaction verification.
Nature	Open and decentralized	Restricted	Controlled and restricted
Operation	The code to operate is open i.e. it gives anyone the right to participate in the consensus process as well as the current shape and size of the Blockchain.	Takes advantage of the technology by setting up groups and participants who can verify transactions internally. Write permissions are kept centralized to one organization	Faster (higher scalability) and provide more transaction privacy, mostly used in the banking sector.

Features	Transactions are anonymous and transparent, secured by game theoretic incentive mechanisms, with no infrastructure costs.	Existence of state compliance of data privacy rules, but there is a risk of security breaches just like in a centralized system.	Reduced transaction costs and data redundancies, and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms
Consensus Algorithms	PoW, PoS, DPoS	PBFT, RAFT	No
Examples	Bitcoin, Ethereum, Monero, Dash, Litecoin	MONAX, Multichain	R3(Banks),EWF (Energy), B3i (Insurance), Corda

Motivation for Blockchain-based IoT

IoT has a major concern for security. Blockchain is used to track sensor data and prevent duplication with other malicious da ta. So, instead of going through a third party for establishing trust, sensors can exchange data through a blockchain. Combining blockchain and IoT helps enable autonomy and support P2P communication since the combination would remove technical bottlenecks and inefficiencies. Due to the absence of any other mediator, cost of deployment of IoT can be reduced substantially. IoT and blockchain combination is well suited for business purposes and achieving cost efficiency.

IoT can exploit blockchain technology in 4 ways, namely Trust building, Cost reduction, Accelerated data exchange, Scaled security [26]. It will lead to the creation of new value business models, optimize ecosystem, reduce risk, free up capital, lower transaction costs, speed processing, provide security, trust, certification validation, design integrity, anti-counterfeit, diagnostics, remote services, micro-transactions [22]. For enabling message exchanges, devices can leverage smart contracts which then models agreement between two parties, enabling autonomous functioning of smart devices without central authority [11]. But the main problem in the blockchain is the issue of scalability and high throughput of transactions owing to the billions of devices in the network, which continuously generate a huge amount of data. For solving this, Hybrid IoT design [16] exploits PoW blockchains and Byzantine Fault Tolerant. Main benefits of BC are Distributedness which is a shared system of records among participants on a business network, Permissioned where each member has access rights and Secureness where consensus is required from all the network members [11].

Although blockchain is a better solution for building IoT applications, it is not always the best idea to use it. It can be used only when the nature of the applications demands the features provided by it because aimlessly doing it will only incur additional costs. Hence, the application must be fully studied before deciding the architecture base. Blockchain is viable to use only when certain factors like Decentralised system, P2P system, Public and sequential transaction logging, Micro-transactions and Computation capacity are taken into account.

4. Designing an optimized BC for IoT

Architecture

- Wireless Sensor Networks- a communication network allowing connectivity in applications with limited power and light requirements.
- Agent Node- Specific blockchain node in architecture responsible to deploy the smart contract.
- Blockchain Network- Network of interconnected and tiered blockchain system.

The architecture of the BIoT application must be such that it is able to handle the vast traffic generated by the network and also provide security to data, and threat and attack-resistant. It has many advantages for providing access control such as light-weight, scalability, transparency, mobility, accessibility, concurrency, etc.

Cryptographic Algorithms

Privacy is maintained as only the nodes having the sender's public key can decrypting/read the transaction. Integrity is maintained from the fact that any alteration or error will prevent correct decryption. Security is maintained via the use of private keys. RSA [27] and Elliptic Curve Diffie-Hellmann Exchange, based on Ephemeral Diffie-Hellman and Elliptic Curves [30] are some of the most secure, powerful and widely used PKC schemes, recommended by NIST [28] for Transport Layer Security (TLS) [29]. RSA is found to be slow and computation-intensive and energy draining for nodes hence is not used. Similarly, Ephemeral Key Exchange incurs heavy overhead and computation hence is not suitable for deployment. So, a much lighter version of RSA, Elliptic Key Cryptography [32][33] is used and is much efficient and has better performance on resource-constrained devices too [34][35][36][37][38][39][40]. The hash functions required by the blockchain are of prime importance with respect to its working. If the weak mathematical model is used, the system loses its meaning since it can be easily be broken or altered. But again, powerful hash function requires high amount of computation, resources, time and energy, all of which are limited in IoT network wherein the lower layer is constituted primarily by the IoT nodes which are resource constrained, while the powerful resource-bearing nodes are placed in the upper tiers, which perform these energy-intensive tasks, hence providing security as well as efficiency. Some of the widely used hash function for consensus algorithms are SHA-256d by Bitcoin, PeerCoin, Namecoin; SHA-256 by Swiftcoin; Scrypt by Litecoin, Gridcoin.

5. Conclusion

Blockchain and IoT are the two great technological disruptions and their combination would yield a better result in every possible domain. It has the power to provide efficiency and security to the field it had been employed to. The paper presents a brief survey, discussing the basics about the technologies, their integration, and their scope of applications. It presents an individual description of IoT and Blockchain. It also describes the IoT and Blockchain relationship and the motive behind their integration. Further the advantages of incorporating IoT with Blockchain has been discussed to intrigue researchers to contribute and study more in this field.

References

[1] K. Ashton, 'That 'Internet of Things' Thing', 2009, URL: https://www.rfidjournal.com/articles/view?4986 [visited : 15/02/2019]

[2] S. Schneider, 'Understanding the Protocols behind the Internet of Things', 2013, URL: https://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things [visited: 15/02/2019]

[3] Ahmed Banafa, 'How to Secure the Internet of Things (IoT) with Blockchain', August 2018, URL: https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228 [visited: 10/02/2019]

[4] Chrisjan Pauw, 'How Significant Is Blockchain in Internet of Things?', December 2018, URL: https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things [visited: 10/02/2019]

[5] URL: Khwaja Shaik, 'Pros and Cons of Internet of Things', May 2018, URL: https://www.redalkemi.com/blog/post/pros-cons-of- internet-of-things [visited : 15/02/2019]

[6] Calum McClellan, 'What is an IoT platform?', August 2018, URL: https://www.iotforall.com/what-is-an-iot-platform/ [visited : 15/02/2019]

[7] Santosh Singh, 'Top 20 IoT platforms in 2018', March 2019, URL: https://internetofthingswiki.com/top-20-iot-platforms/634/ [visited : 15/02/2019]

[8] Jon Wood, 'Blockchain of Things—cool things happen when IoT & Distributed Ledger Tech collide', April 2018, URL: https://medium.com/trivial-co/blockchain-of-things-cool-things-happen-when-iot-distributed-ledger-tech-collide 3784dc62cc7b [visited: 10/02/2019]

[9] IBM Research Editorial Staff, 'A Blockchain Architecture for the Internet of Things', October 2018, URL: https://www.ibm.com/blogs/research/2018/10/blockchain-internet-of-things/ [visited: 10/02/2019]

[10] "NSA Prism program taps in to user data of Apple, Google and others", URL: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [visited:09/02/2019]

[11] IBM Research Editorial Staff, 'What is blockchain?', 2018, URL: https://www.ibm.com/downloads/cas/K54GJQJY [visited: 10/02/2019]

[12] Bernard Marr, 'A Very Brief History of Blockchain Technology Everyone Should Read', February 2018, URL: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#33df967c7bc4 [visited: 10/02/2019]

[13] Swati Goyal, 'The History of Blockchain Technology: Must Know Timeline', November 2018, URL: https://101blockchains.com/history-of- blockchain-timeline/ [visited: 10/02/2019]

[14] URL: : https://www.investopedia.com/terms/b/blockchain.asp [visited: 10/02/2019]

[15] URL: https://en.wikipedia.org/wiki/Blockchain [visited: 10/02/2019]

[16] URL: https://blockgeeks.com/guides/what-is-blockchain-technology/}[visited: 10/02/2019]
[17] S. Nakamoto.(2008),'Bitcoin: APeer-to-Peer Electronic Cash System'
[18] S. Haber and W. S. Stornetta.(1991), 'How to Time-Stamp a Digital Document', Journal of Cryptography, **3 (2)** : 99-111
[19] R. Merkle. (1980) 'Protocols for public key cryptosystems', IEEE Symposium on Security and Privacy, **1**: 122-122
[20] URL: https://www.dotcominfoway.com/blog/growth-and-facts-of-blockchain-technology[visited: 10/02/2019]
[21] URL: https://thecoinoffering.com/learn/blockchain-statistics/ [visited: 10/02/2019]
[22] URL:https://www.transparencymarketresearch.com/blockchain-technology-market.html[visited: 10/02/2019]
[23] H. Mel and D. Baker.(2001) "Cryptography Decrypted", Addison Wesley
[24] N. Ferguson, B. Schneier.(2003) "Practical Cryptography", Wiley
[25] A. Panarello , N. Tapas, G. Merlino, F. Longo and A. Puliafito (2018) 'Blockchain and IoT Integration: A Systematic Survey', Sensors 2018, **18(8)**:2575
[26] S. Gopal, 'Blockchain for the Internet of Things', Tata Consultancy Services White Paper, URL: https://www.tcs.com/blockchain-for- iot
[27] R. L. Rivest, A.Shamir, L. Adleman.(1978) "A method for obtaining digital signatures and public-key cryptosystems", in ACM Commun., **21(2)**: 120-126
[28] NIST official web page. URL: https://www.nist.gov [visited: 10/04/2018]
[29] T. Polk, K. McKay, S. Chokhani.(2005) "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations", NIST Special Publication 800-52 Revision 1
[30] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, L. Castedo. (2017) "A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications", in Sensors. **17(9)**:1–39
[31] A. Levi, E. Savas.(2003) "Performance evaluation of public-key cryptosystem operations in WTLS protocol", in Proceedings of the Eighth IEEE Symposium on Computers and Communications, Kemer-Antalya, Turkey. **(20)4**:625-635
[32] M. Habib, T. Mehmood, F. Ullah, M. Ibrahim. (2009) "Performance of WiMAX Security Algorithm (The Comparative Study of RSA Encryption Algorithm with ECC Encryption Algorithm)", in Proceedings of the 2009 International Conference on Computer Technology and Development, Kota Kinabalu, Malaysia.**(2)**:108-112
[33] Gura, N., Patel, A., Wander, A., Eberle, H., Shantz, S. C. (2004) "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", in Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, United States.
[34] M. Savari., M. Montazerolzohour, Y. E. Thiam. (2012) "Comparison of ECC and RSA algorithm in multipurpose smart card application", in Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Kuala Lumpur, Malaysia.
[35] M. Bafandehkar, S. M. Yasin, R. Mahmod, Z. M. Hanapi. (2013) "Comparison of ECC and RSA Algorithm in Resource Constrained Devices", in Proceedings of the International Conference on IT Convergence and Security, Macau, China. **3(3)**:86-93
[36] A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz. (2005) "Energy analysis of public-key cryptography for wireless sensor networks", in Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, Kauai Island, United States.
[37] E. Noroozi, J. Kadivar, S. H. Shafiee. (2010) "Energy analysis for wireless sensor networks", in proceedings of the 2nd International Conference on Mechanical and Electronics Engineering, Kyoto, Japan. **(2)9**:328-338
[38] P. R.de Oliveira, V. D. Feltrim, L.A. Fondazzi Martimiano, G. B. Marcal Zanoni. (2014) "Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", IEEE Latin America Transactions, **(12)6** 1141-1148
[39] T. K. Goyal, V. Sahula.(2017) "Lightweight security algorithm for low power IoT devices", in Proceedings of the 2016 International Conference on Advances in Computing, Communications and Informatics, Jaipur, India. **8(1)**:1-10
[40] M. Feldhofer, C. Rechberger. (2006) "A Case Against Currently Used Hash Functions in RFID Protocols", in Proceedings of On the Move to Meaningful Internet Systems Workshops, Montpellier, France.