A Review of Blockchain Technology and Its Application in Internet of Things

Siva Rama Krishna T

Jawaharlal Nehru Technological University Kakinada

K. S. N. Murthy

Baba Institute of Technology and Sciences

ksnm1925@bitsvizag.com

Dr. A. S. N. Chakravarthy

Jawaharlal Nehru Technological University Kakinada

Abstract- Blockchains and Internet of Things (IoT) are undoubtedly the most predominant technologies of current digital era. IoT is the broader term used to refer enormous embedded devices that are connected to Internet to communicate with each other and with rest of the world. Blockchain refers to a network and a distributed storage of transactions stored in blocks that are cryptographically connected with each other through. Now IoT and Blockchains are going hand in hand to open up new opportunities and to create a better world. This paper reviews different aspects of Blockchain technology like consensus and forks, and the areas of IoT where Blockchains can be incorporated for better computing and security. This paper also addresses the challenges of implementing traditional Blockchains in IoT and also suggests mechanisms to address those challenges.

Keywords: Blockchain; IoT; Security; Privacy; Authentication.

1. INTRODUCTION

Internet of Things (IoT) has evolved into a game changer technology in almost every domain. Next generation services like self driven cars, self flying drones, automated production chains, smart homes and cities are all actualized by IoT based products. Even though IoT is one of the most emerging markets in the world, there are concerns about reliability and security of IoT based systems. As per Bain IoT Customer Survey 2016 [1], 45% of the IoT buyers are worried about security concerns and it is the first in top ten barriers to implementation of IoT based solutions. Recently Blockchain technology is transforming all the major application areas of IoT by enabling a decentralized environment with anonymous and trustful transactions. Combined with the Blockchain technology, IoT systems benefit from the decentralized resource management, lower operational cost, robustness against threats and attacks, and so on. Therefore, the convergence of IoT and Blockchain technology aims to overcome the significant challenges of realizing the IoT platform in the near future.

Rest of the paper addresses the challenges and concerns of IoT, and suggests solutions based on Blockchain technologies. Section 2 describes basic terms and technologies involved in Blockchain operations, different consensus models and smart contracts. Sections 3 cover the areas of IoT that can be improved by Blockchains; Security, Authentication and Industrial IoT devices. This section also introduces IOTA, an IoT based Cryptocurrency. Section 4 focuses on the challenges for use of Blockchains in IoT environments, which include lack of an IoT based consensus model and resource requirement for Blockchain operations.

2. BLOCKCHAIN TECHNOLOGIES

The ideology of Blockchains evolved from crypto currencies, especially from Bitcoins. However, this technology is now used in variety of domains like supply chain management, e-governance, asset management, education … etc.

Blockchains are tampering proof distributed shared ledgers, usually without a centralized control. These ledgers hold set of digitally signed transactions, known as a block. Each block is connected to its previous block with a cryptographic hash link i.e. Each block holds the cryptographic hash value of the previous block's header, as illustrated in Figure 1. Each block undergoes validation and consensus decision before adding it to the Blockchain. New blocks are

distributed across nodes in the network. Unlike in traditional databases, the transactions recorded in Blockchain ledges are never overwritten. As the similar copy of ledger is available across all the nodes in the network, the Blockchain system is completely transparent. This transparency establishes trust among the users of the Blockchain network to transact with each other, even when they are not known to each other.

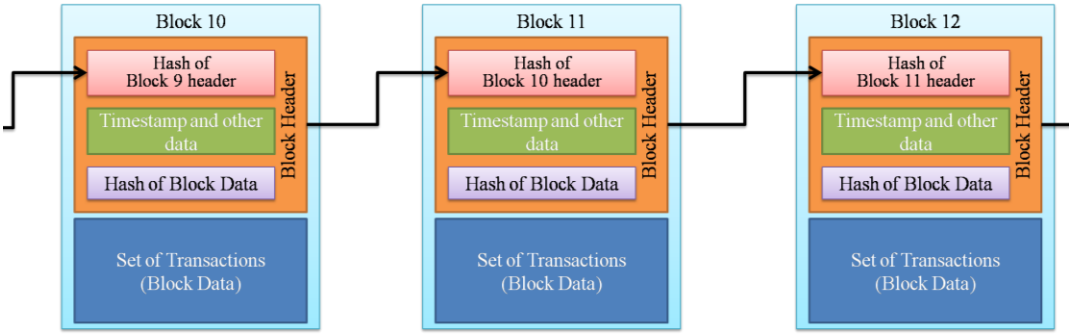

Figure 1. A Portion of the Blockchain with Cryptographic Hash Links

2.1. Classification

Based on 'who can publish a new block', Blockchains are classified into two broad categories: Permissioned and Permissionless Blockchains. In simple terms, if anyone can publish new blocks then it is a Permissionless/Public Blockchain and if only few users can publish new blocks then it is a Permissioned/Private Blockchain.

2.1.1. Permissionless Blockchains: In a Permissionless Blockchain any user of the distributed network can read or write transactions to the shared ledger. As Permissionless Blockchains allow anyone to publish blocks, malicious users may use this to damage/bring down the system. To minimize this type of activities, Blockchains use a set of rules known as Consensus Model that qualifies a user for publishing a new block (explained in detail in Section 2.2). Consensus Models insist the users to possess/maintain resources to publish a block, making it hard for malicious users to damage the system.

2.1.2. Permissioned Blockchains: In a Permissioned Blockchain, to read or write transactions to the shared ledger, the user must be authorized by a centralized or a decentralized authority. Since there is a provision for authorization, access control can be implemented on reading and writing of transactions. It is also possible to allow anyone to submit transactions for inclusion in Blockchain, and restrict the read access to only authorized users. Even though access restrictions are imposed, Permissioned Blockchains exhibit transparency, robustness and traceability on par with Permissionless Blockchains. Permissioned Blockchains also use Consensus Models for publishing blocks. But as only authorized users are allowed to publish blocks, these models need not be as expensive (in terms of resources) as in Permissionless Blockchains. Permissioned Blockchains are usually implemented by organizations that require more control and protection for their Blockchains. Permissioned Blockchains can also be implemented between several organizations to have transparent shared ledgers among business partners, with Consensus Models for establishing trust. In some Permissioned Blockchains, privacy of the transactions can be protected through selectively revealing the transaction information to users based on their credentials.

2.2. Consensus models

Determining which users can publish blocks is the key issue of Blockchain technology. In Permissionless Blockchains usually there are many user competing to publish blocks and the anonymity makes them mutually distrusting. Consensus Models are used in Blockchains to make these mistrusting users work together.

When users join the Blockchain network, they all agree to the initial state of the Blockchain. This agreement is recorded in a preconfigured genesis block. Thus genesis block becomes the first block and subsequent blocks must follow it in the chain. Every new block can be validated by each Blockchain network user. By combining genesis block and the ability to validate every new block, all users of the network agree with the current state of the Blockchain, all times. User need not be

aware of these things as an algorithm takes care of everything. To publish a new block, all nodes of Blockchain network need to come with a common agreement on the consensus model. Such models are discussed in the below sections [2].

2.2.1. Proof of Work (PoW) Consensus Model: In this consensus model, the user who first solves a computationally complex puzzle publishes the next block. The solution of the puzzle serves as the proof for computational work done by the user. The puzzle is designed such that finding the solution is hard and verifying the solution is easy. This makes other nodes of the network to validate the block to be published. Blocks submitted for publishing that do not solve the puzzle are rejected. A popular puzzle that fits this scenario is finding a block header with desired cryptographic hash value. Sometime the difficulty level of the puzzle is dynamically adjusted to meet certain yield, like in Bitcoins. As this model involves solving a computationally complex puzzle the publisher need to possess/invest on sufficient hardware and electricity. Once a publishing node solves the puzzle, it sends the new block to other nodes in the Blockchain network. The receiving nodes verify the validity of the new node against the puzzle, adds it to their copy of Blockchain and send it to other nodes of the network.

2.2.2. Proof of Stake (PoS) Consensus Model: This model is based on the idea that more a stakeholder invested on the system, more the chances of him contributing towards the success of the system and very unlikely he wants to damage it. PoS Blockchain models use the amount of stake invested/possessed by a user as the factor for determining his chances of publishing the next block. Thus this model avoids the need for investing on resources like computational hardware and electricity as in PoW consensus model. Based on how stake is considered for selecting the next publishing node there are four variants of PoS, explained in Table 1.

Table 1. PoS Node Selection Models

Node Selection Model	Method of Selection
Chain based PoS	Based on the ratio of stake i.e. a user with 20% stake is considered 20% of times.
Multi-round Voting	Several users are selected to publish their blocks and the final block to be published is selected based on multiple rounds of voting by all users of the network [3].
Coin Age PoS	Once a user is selected to publish the block, the age of his stake is reset and he is not allowed to publish his next block until certain time.
Delegated PoS (DPoS)	Users of the Blockchain network vote and select the next publishing node. The weightage of each vote is directly proportional to the stake owned by the user.

2.2.3. Round Robin Consensus Model: Nodes take turns to publish their blocks. This is the simplest of the consensus models and has the least power consumption. If the next publishing node doesn't have a block ready to publish this model may impose a time limit of wait and moves on to other nodes, to avoid Blockchain to be halted by slow/misbehaving nodes. But there is a chance of a malicious user adding more nodes to improve his chances of publishing more blocks and there by damaging the system. So this consensus model is not suitable for Permissionless Blockchains.

2.2.4. Proof of Identity (PoI) Consensus Model: This model relies on a partial trust of publishing nodes through their identities in real world. Each publishing node must possess a verifiable identity and each node can improve its reputation by behaving in manner agreed by the network user. The more the reputation of a node, more the chances of it publishing the next node. This model applies only to Permissioned Blockchains with high amount of trust.

2.2.5. Proof of Elapsed Time (PoET) Consensus Model: In this model each publishing node requests a wait time from a time source within their system. The time source will generate a random wait time and submit it to the publishing software. The publishing node sleeps for the time submitted by the time source and after waking up publishes its block. This model require a secure time source returning a random time to ensure that no malicious node is submitting a fake random time to wait for minimum time and dominate the system.

There are few more consensus models like the one based on Byzantine Fault Tolerance used by Hyperledger [4]. A comparison of consensus models is given in table 2.

Table 2. Comparison of Consensus Models

Consensus Model	Advantages	Disadvantages	Applications
PoW	Difficult to flood the network with malicious blocks	Requires possession of sufficient hardware and electricity (expensive)	Permissionless Blockchains
PoS	Less computational overhead than PoW	Several stakeholders my collaborate to take control of the network	Permissionless Blockchains
Round Robin	Simple and least power consumption	Presence of high trust is required between participating users	Permissioned Blockchains
PoI	Permits dynamic block publishing rates and can be combined with other consensus models	Relies on the assumption that identities of nodes are not compromised	Permissioned Blockchains
PoET	Less computational overhead than PoW	Requires the presence of a secure time source and fault proof software	Permissioned Blockchains

2.3. Forking

In Permissionless Blockchains like Bitcoin, it is highly essential to have proper methodology for updating the changes across the network and it is difficult to do so due to the presence of vast number of nodes across the globe. The changes to either the Blockchain or the governing protocol are referred as forks. There are two classes of forks: soft forks and hard forks.

Smart forks are the changes that are backward compatible. That is a non updated node can still communicate and transact with an updated node. However updated nodes reject the transactions by non-updated nodes if the transaction is based on updated data/protocol. On the other hand hard forks are the changes that are backward compatible. That is all nodes of the network need to update before communicating/transacting with other nodes. But the non updated nodes can still transact with other non updated nodes and same is the case with updated nodes. This results in a split in the network with nodes in one part rejecting the blocks published by nodes in another part. Due to an attack in 2016, Ethereum (a cryptocurrency network like Bitcoin) proposed a hard fork to return the stolen funds [5]. This fork resulted in a split, non updated users operating Ethereum Classic and updated users moved to the new Ethereum.

2.4. Smart Contracts

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions, minimize exceptions and the need for trusted intermediaries [6]. A smart contract is a set of cryptographically signed transactions containing code and data, published on a Blockchain. All the participating nodes of the contract have to execute the smart contract and the results are recorded on the Blockchain. Smart contracts must have deterministic nature i.e. on all participating nodes they have produce same results when executed with the given input data. Just like Proof of Work, smart contract execution also rewards the users in cryptocurrency networks.

Figure 2. Phases of Smart Contract Implementation

3. BLOCKCHAIN FOR IOT

Integrating Blockchains with IoT ensures the transparency and traceability of critical data ensuring trust among diverse and vast number of devices across the IoT network. Blockchains can be used for authentication, security, privacy and traceability of IoT devices. But not everything related to IoT can be effectively stored on Blockchains. A better solution would be a hybrid approach [7] of combining Blockchain and Fog/Cloud computing. Data that need be distributed and that requires transparency is published on Blockchains, and data that is huge which needs analysis is left to the centralized computing facilities like cloud.

3.1. Blockchain for IoT Security and Privacy

As mentioned in section 1, security is the major concern in IoT based systems. Blockchains can be integrated with IoT to enhance the security and to ensure the privacy of users and devices in IoT based networks. Privacy sensitive devices like smart home devices can be linked with a local Blockchain to record and track events. Because of the tamperproof nature of Blockchains, this data can be used track, detect and prove malicious activities. A Permissioned Blockchain ensures that home data is only accessible to authorized users. A good consensus model ensures that the data recorded by an IoT device is not altered for any malicious purpose, before it gets published on the Blockchain. The consensus may be done by considering similar such devices in the proximity. For example is a temperature sensor in kitchen is reporting incident of a fire, the same may be cross checked with or compared with another temperature sensor inside kitchen or in the next room, before alerting the inmates, ensuring there is no false alarm by error or by malicious activity of a device (as illustrated in Figure 3).

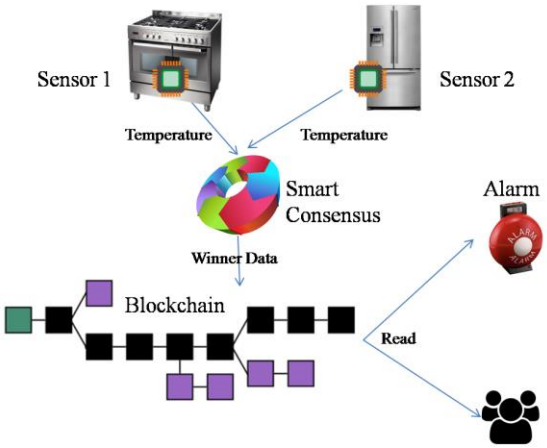

Figure 3. Blockchain based Smart Consensus for Fire Detection Systems

3.2. Blockchain based IoT Authentication

Having a centralized authentication in IoT increases the cost of communication and limits the scalability of network. Blockchain technology trashes these limitations by implementing a distributed authentication mechanism, which doesn't depend on a central authority. On the other hand Blockchain in an ever growing structure and requires sufficiently larger memory for storing it. A copy of the Blockchain cannot be maintained at every IoT node, where resources are scarce.

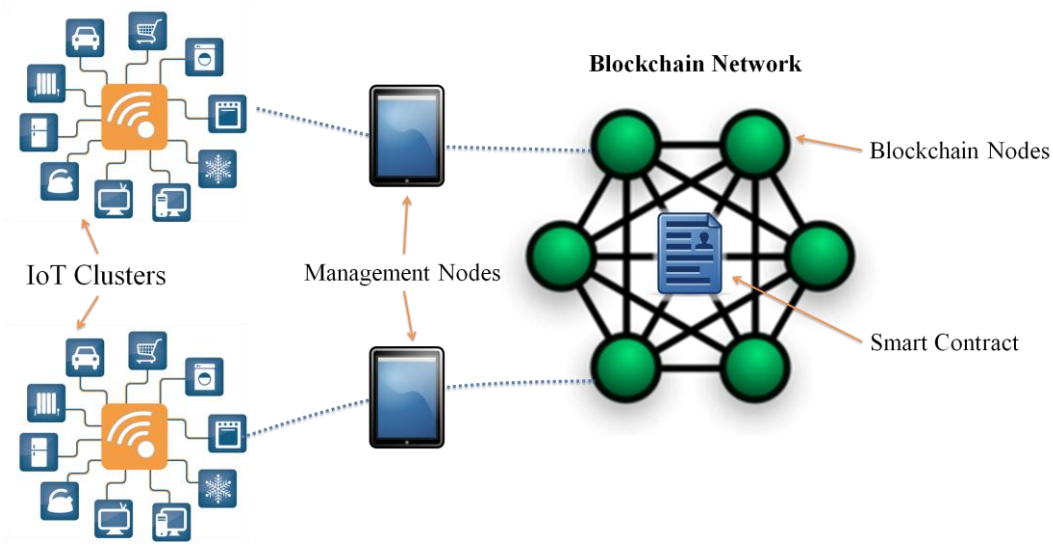

Figure 4. Blockchain based Access Control System

O. Novo [8] proposed a solution for these challenges with a Blockchain based decentralized access control system for IoT, illustrated in Figure 4. In this system every node must be a part of the Blockchain network, except the IoT nodes, which can't have enough resources to be a Blockchain node. This system also defines a new set of nodes called Management Nodes, through which IoT nodes request access control information stored on the Blockchain. Management nodes are usually the ones with more computational and memory resources. A single smart contract defines all the allowed operations. A node of the Blockchain network called the agent node creates the smart contact. Only few other Blockchain nodes called managers are allowed to define/change policies in the smart contract. Management nodes are directly connected to Blockchain nodes and in turn multiple IoT clusters may be connected to a management node. So management nodes must be able to simultaneously handle requests from many IoT devices. When a new IoT device is added to the cluster, a manager node informs its credentials and other information to corresponding management node. All the interactions happen through public key cryptographic protection and recorded in Blockchain.

3.3. Blockchains for IoT Device Tracking

When a product is on sale, sometimes the manufacturer needs to track the ownership and other details of the product for proper disposal of services like warranty and insurance. For example a car manufacturer needs to track all the cars that were sold in a production batch, to make a recall when he finds something faulty in that car model. Device tracking is also helpful for the potential buyers when used products are on resale in platforms like ebay. Device tracking in this scenario prevents the buyers from going to an out dated or faulty product. On the other hand tracking of devices without proper access control may lead to personal data leakage. Blockchain based device tracking can rightly handle this situation [9]. Blockchain based tracking system records the transactions like manufacturing of a product, ownership creation on first sale, and transfer of ownership on subsequent resale … etc. A user of the product can access data related to devices owned by him. Smart contacts enable current user of the device to access/share data generated by the device and he is no longer able to do that once the device is sold to another user. A part of the Blockchain must be designed as permissionless, which stores non private data of the device that can be accessible to manufacturers, auditors, insurance companies and potential buyers when it is on resale.

3.4. Blockchains in Industrial IoT (IIoT)

IoT already established huge market in industrial domain by contributing to automated production chains, supply chain management, predictive maintenance … etc. Blockchains can now be used to record and distribute the data captured from industrial IoT device across business network [10]. Permissioned Blockchains are best suitable to be used with IIoT because of their

secure and authorization based approach for consensus. Figure 5 illustrates an IIoT based industry with Blockchain for data management.

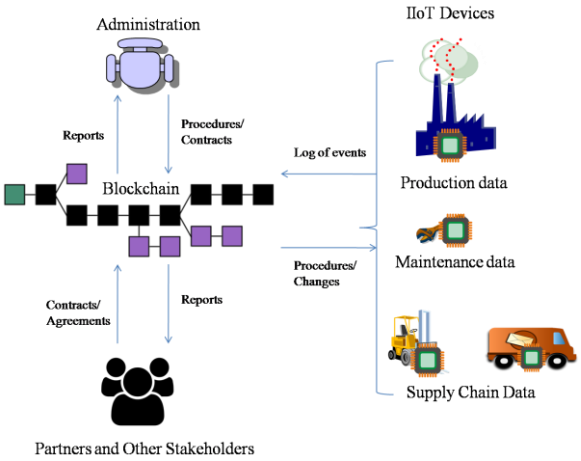

Figure 5. Blockchain Applications for IIoT

Smart contracts are the best way to implement rules and procedures over Blockchain. This feature can be used in IIoT to design and implement procedures for product manufacturing and other key management features [11]. A smart contract has to be distributed, executed and validated by all participating nodes before agreeing for it. This enhances transparency and accountability of procedures in industries, yielding more productivity and fewer disputes. Another reason for using smart contracts in IIoT is current procedure cannot be altered without the approval and knowledge of stakeholders.

In some implementations of the Blockchain, it is possible to rollback to a previous state from current state, to create or follow an alternate path. But these rollbacks are to be approved/agreed by users through a consensus model. This feature of Blockchains can be used in IIoT, where a product that is underdevelopment or almost developed has to go back to its previous state in an emergency. The consensus model is such that the rollback of product state has to be initiated by concerned supervisor and published only if approved by users with higher stake (Managers/Directors).

3.5. IOTA: Cryptocurrency for IoT

Having billions of IoT devices already on globe, machine-to-machine economy is making new pace. But security and authentication are the biggest concern when devices transact with each other with limited or no human intervention. Cryptocurrencies like Bitcoins can easily address this challenge, but the client programs of most of the cryptocurrency networks are too heavy for IoT devices, as they require huge computational resources. IOTA is a permissionless open source distributed ledger that uses an extremely light weight client program, specially designed run on IoT devices [12].

Instead of holding the transactions on a sequential chain of blocks, IOTA uses a Directed Acyclic Graph (DAG) based protocol called Tangle. To create a transaction, the node has to validate two other transactions on Tangle. As every node is a validator there is no need for mining like in other cryptocurrency networks. This reduces the need for huge computational resources and also increases the scalability of the network. More validator presence on the network increases the speed of the economy. A sample Tangle state for an IOTA transaction is illustrated in Figure 6. Unconfirmed transactions on tangle are called tips. For a user to publish his transaction on tangle, he needs to randomly select two tips and validate them. Validation is nothing but checking tip's signature and confirming that the tip is not conflicting with any confirmed transactions in the reference path (blue shaded region in Figure 6). After the validation of two tips user publishes his transaction on tangle and it becomes a tip. All of the IOTAs that will ever exist were created in the genesis block. The amount will never increase or decrease [13].

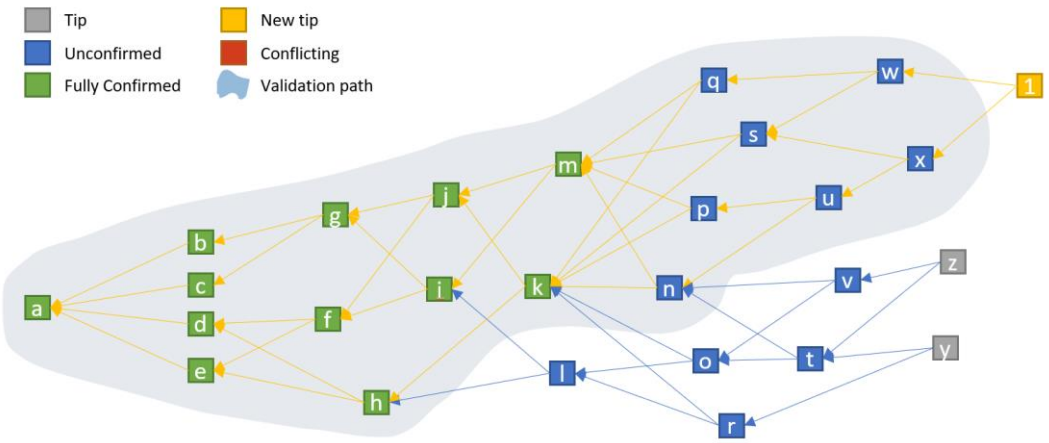

Figure 6. A Sample Tangle State for IOTA transaction
(Image Courtesy: IOTA Official Documentation at http://untangled.world/)

4. CHALLENGES TO BLOCKCHAIN USE IN IOT ENVIRONMENTS

This section highlights the setbacks in traditional Blockchain technologies [14], which are critical for designing and developing a secure IoT eco system with Blockchain as its backbone.

4.1. Consensus Model for IoT

As discussed in Section 2.2, each class of consensus model has their own merits and demerits. But to be able to implement on IoT based networks, the consensus model needs to be liberal on resources and have rigid transaction validations happening at faster pace. Forks are another form of threat to Blockchain based IoT networks, as they may lead to splits in the networks and bringing down entire system there by. PoW is the least preferred consensus model for IoT Blockchains because of higher computational complexity, requirement of huge power source and the possibility of forks. PoS, PoET and IOTA consensus models are liberal on resource requirements, but still are prone to forks and lacks consensus finality. Byzantine Fault Tolerance consensus models can be seen as an alternative because of consensus finality and non possibility of forks. Yet they are highly complex and are vulnerable to faulty nodes.

4.2. Transaction Validation and Resource Requirements

In traditional Blockchain networks transactions are validated by checking their format, signature and verifying the transaction data is not previously present on any other block. But this validation model is not suitable for IoT based environments because of the presence of heterogeneous devices, each with a different format and range for similar measurement. More over these validations require few hundred gigabytes of hard disk space, a high end processing node and an ultra speed network bandwidth. These resources are usually not available on most of the IoT devices.

4.3. Scalability and Device Security

Unlike traditional computing networks, IoT networks accommodate huge number of nodes in a small area. With each node present on the Blockchain network, this enormously increases the Blockchain size and also greatly influences the consensus process. If consensus protocol has less throughput that automatically increases the latency in transaction validation. IoT devices can be easily hacked due to the non availability of complex threat prevention models in limited resource environments. Presence of more number of versatile nodes also makes it complex to identify a malicious node. This scenario leads to lack of trust and there by leading to nodes disapproving a consensus decision quoting the possibility of a false consensus.

5. CONCLUSION

Blockchain has revolutionized the technological world with its distributed network architecture, decentralized control and ability to sustain autonomous, self-regulating, self-managed and fault

tolerant IoT systems. Blockchains can improve security and access control in IoT through distributed tamperproof structure. They can also leverage efficient IIoT systems for next generation industrial solutions. IOTA is another dimension of cryptocurrency with its revolutionary consensus protocol, tangle and light transaction validation process. However, still there exist some open research challenges that need to be resolved to leverage Blockchain's benefits at the optimum. Few solutions for the challenges mentioned in Section 4 are as follows. A consensus model with IoT centric transaction validation and environmental awareness is essential. Sharding is to be considered for reducing transaction confirmation time. In Sharding method a subset of Blockchain nodes validates a subset of transaction. To address the scalability issue of IoT Blockchains new architecture models like side chains and tree chains have to be considered. Device enrollment where only approved devices are allowed to communicate and smart contracts for access control are to be implemented for better device security.

REFERENCES

[1] Ann Bosche et. al., “How Providers Can Succeed in the Internet of Things”, Bain & Company, 2016.

[2] Dylan Yaga et. at., “NISTIR 8202: Blockchain Technology Overview”, National Institute of Standards and Technology, USA, Oct 2018.

[3] Bahsoun, J.P., Guerraoui, R., and Shoker, A., “Making BFT Protocols Really Adaptive,” 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, pp. 904-913, 2015.

[4] “Hyperledger Architecture, Volume 1”, Hyperledger, 2017.

[5] Wong, J. and Kar, I., “Everything you need to know about the Ethereum ‘hard fork,’” Quartz Media, July 18, 2016.

[6] Szabo, N. “Smart Contracts,” 1994

[7] Ana Reyna et. al., "Blockchain and its integration with IoT, Challenges and opportunities", Future Generation Computer Systems, Elsevier, 2018.

[8] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018.

[9] Yu, Bin, et al. "TrustChain: Establishing Trust in the IoT-based Applications Ecosystem Using Blockchain." IEEE CLOUD COMPUTING 5.4 (2018): 12-23.

[10] Dennis Miller, "Blockchain and the Internet of Things in the Industrial Sector", IT Professional, IEEE Computer Society, May/June 2018.

[11] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," 2017 21st Conference of Open Innovations Association (FRUCT), Helsinki, 2017, pp. 321-329.

[12] Alexander, Roman. "IOTA-Introduction to the Tangle Technology: Everything you need to know about the revolutionary blockchain alternative" (2018).

[13] Serguei Popov, “The Tangle, version 1.3”, IOTA Whitepapers, October 1, 2017.

[14] Makhdoom, Imran, Mehran Abolhasan, and Wei Ni. "Blockchain for IoT: The Challenges and a Way Forward." Proceedings of the 15th International Joint Conference on e-Business and Telecommunications-Volume 2: SECRYPT. INSTICC, 2018.