ISSN (e): 2250 – 3005 || Volume, 07 || Issue, 12|| Decmber – 2017 ||
International Journal of Computational Engineering Research (IJCER)

Internet of Things: Beyond Blockchain

Imopishak Thingom[1],Th. Prameshwor Singh[2]
[1, 2] National Institute of Electronics & Information Technology, Imphal
Corresponding Author: Imopishak Thingom

ABSTRACT
Internet of Things and blockchain are two breakthrough and transformative technologies. Blockchain is a type of distributed ledger technology. It is a decentralized or distributed peer-to-peer network. The applications of blockchain have moved beyond traditional financial services. In this paper proposed applications of blockchain in IoT are reviewed. Challenges of IoT and limitations of blockchain in the context of IoT are highlighted. Going beyond traditional blockchain, we review a distributed ledger technology known as Tangle which is an extension of blockchain but different from traditional blockchain technology. This technology is gaining support of industry and academia and is designed for applications in IoT.

Keywords: Bitcoin, Blockchain, DAG, IoT, IOTA, MCMC, Smart contracts, Tangle, Virtual blocks

Date of Submission: 25-12-2017 Date of acceptance: 09-01-2018

I. INTRODUCTION

As we move towards Industry 4.0 where intelligent network control each other without human intervention, the Internet of Things (IoT) and Internet of Everything (IoE) are envisioned to transform lives and businesses. On the other hand distributed ledger technology (DLT) such as blockchain is being widely seen as revolutionary technology with potentially diverse applications ranging from cryptocurrency to distributing food vouchers to Syrian refugees in Jordan. It has reached an inflection point with application beyond financial services such as in IoT, supply chain management and health records.

Many organizations are increasingly trying to create the ecosystem and incorporate blockchain technologies in their businesses. At 2017 World Internet of Things held in Wuxi, China, Chinese media and Internet firm Tencent and Intel announced a partnership centered on blockchain targeted at enterprise customers. The focus is on enhancing security capabilities of IoT by developing a secure blockchain system for IoT. On September 19, 2017 Bosch, Cisco, Slock.It, Chronicled, Skuchain, HCM International of Foxconn Group and others launched ‘Trusted IoT Alliance’ with the goal to catalyze the development of a blockchain-enabled trusted IoT.

In IoT and Cyber Physical Systems (CPS) the ultimate goal is to enable machine - to - machine transactions without central coordinator. Along this line, we explore different potential applications and adoption of blockchain in the industry. We also highlight the challenges of these technologies which might prevent quick adoption in areas such as IoT. This article assesses the current landscape of blockchain and IoT. This paper is organized as follows. In part II principle of blockchain technology and smart contracts are introduced. Part III discusses the applicability of blockchain technology to IoT. It reviews proposed applications of blockchain in IoT. Part IV reviews Tangle and IOTA. Conclusion is in section V.

II. BLOCKCHAIN AND SMART CONTRACTS

According to a whitepaper by World Economic Forum [1] “Blockchain technology can give rise to a new Internet era even more disruptive and transformative than the current one, generate unprecedented opportunities to create and trade value in society.” Also, “a smooth future for the Internet of Value won’t just happen; it will be achieved.” Satoshi Nakamoto is credited with developing blockchain when it was used in an implementation of blockchain called Bitcoin [2]. Blockchain is a distributed public ledger which aggregates records called blocks. Each block contains data and contains all transactions that were executed and which are signed cryptographically using a hash. These transactions are timestamped and chained to other blocks. New blocks can only be linked with the end of a chain and hence the transactions are immutable. There is no central authority involved in managing these blocks and exist in peer-to peer networks. Transactions from a peer is validated and relayed to other peers. These transactions are pooled by nodes called miner to create a new block. The block is mined by performing a proof of work. This is done by calculation of cryptographic hash. This new block is relayed to other nodes. Any other node receiving this block validates and adds to its blockchain. A blockchain transaction can be used to exchange such as digital currency, document or smart contracts. Blockchain provides the following benefits:

- A distributed network tolerant to node failure
- Transparency, verifiability and auditability
- Enforcing of data ownership of different parties without central authority
- Enabling interaction between non-trusting parties

A smart contract is ‘‘a computerized transaction protocol that executes the terms of a contract [3]. Smart contracts are codes which run on the blockchain. It contains conditions which are validated to perform certain actions. It allows transaction between parties by self-enforcing contractual clauses.”

III. IOT AND BLOCKCHAIN

The IoT, as used today, is a client-server model using cloud services along with edge and fog computing. These rely on centralized trust brokers. Key challenges of IoT are security, privacy, lack of central control, scale and inherently distributed structure of IoT with billions of devices expected to be connected. There is an increasing need for legal framework for protecting users and consumers. Other challenges are cost and capacity, deficient architecture, cloud server downtime and susceptibility to manipulations. However with blockchain technology it may be possible to address the challenges of IoT. Using blockchain it is proposed that IoT be built as a decentralized architecture. The following characteristics of blockchain suggest that it may be able to make security and privacy decentralized. This are:

- No single point of failures, scalability and robustness due to its distributed nature
- The users participating in a blockchain is anonymous
- Data are encrypted and blockchain creates a trusted network

However, adoption of blockchain has its challenges:

- Device in IoT are resources constrained while mining is expensive
- Mining introduces delays and increases latency
- Poor scalability while billions of devices are expected to be connected in IoT

A lightweight architecture for IoT is proposed [4] which aim to overcome the challenges and take advantages of blockchain. Blockchain is used in a smart home setup. It consists of a local blockchain, an overlay network and cloud storage. However, the blockchain is maintained centrally by the user in the local network (here the Smart Home). The blockchain owner adds new devices by creating a starting transaction. Devices communicate with authorization of the owner using Diffie-Hellman algorithm. The overlay network is similar to that of Bitcoin. Data may be stored in a cloud. It describes how transaction handling and distributed trust can be implemented. It considers various attacks that threaten accessibility, anonymity, authentication and access control over several tiers such as smart home, overlay networks and cloud storage. The proposed architecture is able to enforce security and privacy in each tier. The qualitative overhead analysis shows it has constant performance overhead at best while transactions scale with the number of clusters in the network at worst case.

The use of blockchain and smart contracts in the context of IoT is explored [5]. The use of blockchain and smart contracts has the potential of creating a marketplace of services between devices where it is possible to share any service and physical assets such as homes or cars by using tokens which are bought on a blockchain network such as Ethereum. Blockchain and smart contracts that reside on blockchains are used to automate multistep process such as in supply chain. This idea is extended to IoT to facilitate sharing of resources and services which will result in a marketplace of services between devices and automate workflows in a cryptographically verifiable manner. It also addresses issues with using blockchain with IoT. It highlights performance degradation due to the decentralized model used and lack of parallel task executions as each node performs the same task. Privacy is another issue where use of a private key between transaction partners may lead to inference of identities. It proposes ways to mitigate this such as using a key for every transaction. However communication of the new key could be problematic.

A blockchain based secure and auditable IoT management system is described [6]. The proposed system separates access control from the data plane. The access control plane is implemented with a blockchain whereas the data plane is implemented with a distributed data plane. Due to inherent characteristics of IoT data which are generated continuously, datastreams are abstracted as data chunks which are a set of data records. The data are compressed which improves performance such as bandwidth and storage requirements. The data are encrypted using a symmetric cypher. The key is shared with services with read access rights. A Distributed Hash Table (DHT) is used as the data storage interface. This tries to tackle several issues such as privacy, security, scalability and fine-grained access control.

Flowchain [7] is a distributed ledger system designed for IoT. It is a cryptocrrrency for IoT. It considers a peer-to- peer network system for IoT and is designed for real-time applications such as IoT. It uses a new blockchain data structure design called Virtual Blocks and cryptocurrency system. The system does not use a proof-of-concept system, as in Bitcoin, as the devices of nodes do not compete in mining new blocks. It uses an algorithm which is different from that is used in Bitcoin and is designed for IoT devices which are diverse and resources-constrained.

Currently there are several platforms providing blockchain solutions for IoT such as Slock.it, Modum.io and Chronicled. Blockchain platform Ethereum is used to implement Slock.it[8]. Slock.it is a framework combining IoT and blockchain with smart contracts enabling a sharing economy where one can share or rent anything from house, cars to bicycles. It tackles security, coordination and privacy of devices and objects. It aims to decentralize the sharing economy system by:

- Handling safe direct peer-to-peer funds without centralized providers
- Providing a mechanism of deposits and/or insurance coverage
- Freeing the customers from having to coordinate with one another to hand over key

A smart lock (Slock) allows sharing among untrusted parties using smart contracts and blockchain. This is the first physical implementation of the blockchain. It allows application to be built on the platform, connect physical objects to blockchain and makes smart contracts enforceable. It is built on Ethereum blockchain.

Modum.io [9] platform implements blockchain and IoT technologies for supply chain in pharmaceutical industry. It is built using Ethereum blockchain. Modum's product provides services for shipping temperature sensitive pharmaceutical products. Sensor devices record environmental conditions and monitor package conditions along the delivery chain. Smart contracts act as an automated compliance auditor. Data collected by sensors are used to determine if regulatory requirements are satisfied. The solution is composed of four components - smart contract, IoT sensor devices that monitor conditions during transit, dashboard for generating shipments and setting for blockchain based smart contracts and a smart phone application for recovering and reading data from the sensors before transmitting that data back to the blockchain. Using blockchain and smart contracts, immutable records of maintenance of contract's conditions are recorded. Sensors collect data which are sent to blockchain where the results are evaluated using smart contracts which determines the adherence to the smart contract. Modicum uses Ethereum blockchain and proprietary sensor devices. In the context of IoT and supply chain management, the advantage of blockchain is that it provides a distributed ledger for transactions which are immutable and verifiable. The aim is to reduce cost of supply chain logistics.

IV. BEYOND BLOCKCHAIN

Despite its many advantages, blockchain has limitations:

- Scalability: blockchain cannot scale large number of transactions
- Transaction fees: the disadvantage of blockchain technology as a generic platform for cryptocurrencies is the transaction fee. This is more relevant in IoT where the transactions involve micropayments and nanopayments.

Moving beyond traditional blockchain such as Ehereum, here we review a new permissionless distributed ledger known as Tangle [10] designed specifically for IoT. It uses a cryptocurrency called IOTA based on Tangle network. This may be considered as an extension of blockchain ecosystem. However this is different from traditional blockchain. This is designed as the next step in blockchain technology or as competing technology to blockchain such as Bitcoin and Ethereum and aims to improve existing blockchains such as Ethereum. This is to be used for feeless micropayments between autonomous machines, cyber physical systems such as supply chains, smart cities and healthcare systems for economy of things. Recently organizations such as Deutsche Telekom, Bosch, Microsoft, Accenture and Fujitsu, and several other companies launched the first publicly accessible data marketplace for IoT [11] based on IOTA and Tangle. As per the whitepaper "IOTA makes it possible to securely store, sell, and access data streams". The public marketplace aims to give connected devices the ability to securely transfer, buy and sell diverse dataset. IOTA does not involve mining. Security and consensus is not divided among miners and users. Users only validate two transactions. This involves no rewards and transaction fees. Many see Tangle network as the next generation DLT which can overcome the limitation of blockchain such as scalability and transaction fees.

Tangle is different from blockchain. First, unlike a global blockchain Tangle is distributed ledger architecture based on Directed Acyclic Graph (DAG). The site set of the graph are the transactions issued by the nodes. This is the ledger used to store the transactions. Users who issue transactions need to perform proof of work to approve other transactions. Thus, the users contribute to the security of the network. The IOTA network is asynchronous. Nodes may see different transactions. Secondly, how a consensus is reached differs from blockchain. Here a single transaction references two past transactions using Markov Chain Monte Carlo

(MCMC) algorithm. Unlike blockchain, all active participants or devices making transactions are responsible for approval of transactions. This means the process of reaching consensus is intrinsic part of the network and no miners are involved. Thus the process of reaching a consensus occurs in parallel whereas in blockchain this process is sequential in blocks. This in turn allows IOTA to scale without transaction fees for either the sender or recipient. Tangle opens the possibilities of several uses such as a sensor selling data or buying computational resources, consumer buying electricity from the grid, device buying bandwidth on demand and so on. All this takes place machine-to-machine without involving humans.

V. CONCLUSION

Blockchain and IoT are transformative technologies. Blockchain technology looks attractive for IoT. Also other technologies which are essentially extension of the traditional blockchain are being developed such as Tangle which appears very attractive. However it is in nascent stage. Many applications have been proposed. However these are still proof of concept. Many established organizations and startups are getting into blockchain and other DLTs in areas such as IoT. The adoption of blockchain and similar DLTs in IoT would requires a strong ecosystem with legal and regulatory frameworks and other technology aspects such as scalability, processing power, storage, privacy and security and standards.

REFERENCES

[1]. Don Tapscott and Alex Tapscott. Realizing the Potential of Blockchain. A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. Retrieved on November 2, 2017 from WEF website http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

[2]. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved on December 1, 2017 from the website https://bitcoin.org/bitcoin.pdf

[3]. Nick Szabo. Smart Contracts, 1994. Retrieved on 2nd November from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[4]. Konstantinos Christidis, and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, vol. 4, 2292 – 2303, 2016

[5]. Ali Dorri, Salil S. Kanhere, and Raja Jurdak Blockchain in Internet of Things: Challenges and Solutions, arXiv: 1608.05187[cs.CR), Aug. 2016

[6]. Hossein Shafagh, Anwar Hithnawi, Simon Duquennoy. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. Retrieved on December 12, 2017 from the website https://people.inf.ethz.ch/mshafagh/mshafagh_NSDIposter17

[7]. Jollen Chen Flowchain: A Distributed Ledger Designed for Peer-to-Peer IoT Networks and Real-time Data Transactions 2017. Retrieved on December 12, 2017 from the website https://flowchain.co/Flowchain-WhitePaper.pdf

[8]. https://slock.it

[9]. https://modum.io

[10]. Serguei Popov. The Tangle. Retrieved on December 7, 2017 from https://iota.org/IOTA_Whitepaper.pdf

[11]. https://data.IOTA.org.

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.

Imopishak Thingom "Internet of Things: Beyond Blockchain." IInternational Journal of Computational Engineering Research (IJCER), vol. 7, no. 12, 2017, pp. 44-47.