IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

The Blockless Distributed Ledger: A Cryptocurrency for the IoT Industry

Shloka Bhalgat

UG Student, Department of Computer Engineering, Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: The need for decentralized consensus system and the risks associated with centralization suggests a solution for storing transactions in a distributed ledger and a standard permissionless protocol which governs the same. A Blockless Distributed Ledger is primarily based on a DAG (Directed Acyclic Graph) for storing transactions. Unlike Blockchain there are no miners which removes any possibility of decoupling. Furthermore, it offers features for machine to machine micropayment system using a cryptocurrency for the Internet of Things industry known as "IOTA". The main aim of IoT industry now is to connect daily used objects to the Internet which have the ability of sensing and actuation which may or may not involve humans.

This paper discusses how a Blockless Distributed Ledger implemented by "IOTA", stands apart over a traditional Blockchain of which "Bitcoin" is a well-known example for storing transactions as well as description of a use case involving a smart cable and a smart socket which pays for its electricity through IOTA and shares its remaining power with other cables.

Keywords: Directed Acyclic Graph (DAG), IOTA, Bitcoin, micropayments, Transactions per Second (TPS)

I.INTRODUCTION

The rise of the use of Bitcoin as a generic platform for crytocurrencies is notable, but it comes along with a number of banes. The concept of transaction fees for mining the blocks which serves as a universal problem is also a part of this cryptocurrency. Another drawback is the heterogeneous nature of the system because removal of the fees is not possible as it serves as motivation in the form of a monetary value to the block miners. Also, due to decoupling between the end user and the miners there is a notion of centralization around the globe of block miners and end users. The aforesaid problems give an insight to search for solutions which are different from Blockchain technology which is currenty the foundation for Bitcoin and many other cryptocurrencies.

As the Internet-of-Things keep expanding, the need for interoperability and sharing of resources has become a necessity. IOTA seems a key enabler for exploring new business-to-business models by making every technological resource a possible service to be traded on an open market in real time, with no fees. Furthermore, by using a Blockless DAG i.e. The Tangle to incorporate these needs for the mentioned issues proves to be a success as stated in IOTA's Whitepaper [1].

II.BACKGROUND

The existing Decentralized Consensus Systems for IoT can be broadly categorized according to the data structure used and the network ledger types which are used to come to a mutual consent to approve a transaction in the network as shown in Fig 1. The use case discussed in Section III is based on this particular classification.

A. Data Structure: This subsection describes two main categories of data structures which are blockchain and blockless namely. A blockchain can be called as a DAG since all blockchains are subsets of trees and DAG is a superset of tree.

i) Blockchain: The blockchain type of data structure incorporates a group of trustless participating nodes which initiate transactions for trade without any middleman involvement. It involves mining of blocks by block miners and adding it to the chain of blocks and hence the name. These transactions are recorded in a public ledger database which is visible to everybody in the network. On the basis of complicated state-of-the-art principles, the transactions are verified by so-called block miners who also maintain the ledger. To avoid any disturbed environment until the blockchain network reaches towards consensus, each transaction should follow a predetermined rule like the Longest-Chain-Rule in Bitcoin. Otherwise the network would fail to establish a common acceptance of truth.

ii) Blockless: The blockless data structure uses a Directed Acyclic Graph to form a tree of its transactions from one node to the other in a single direction towards the *genesis* in a network. The *genesis* transaction is the first created transaction in the DAG. The Tangle used in IOTA which is a DAG, is able to achieve high transaction throughput (buy

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

parallelizing validation) and so no transaction fees is required on transactions. There is only one type of participant in The Tangle, unlike block miners and users in Bitcoin. That participant has to approve two unapproved transactions in order to get his transaction approved. This is the 'fees' which is to be paid in real time.

B. Consensus Ledger Types: In light of existing cryptocurrencies, a scalable consensus ledger is used and maintained for unanimity of trade. In this consensus ledger all the participating nodes have to vote and select a sequence of succeeding transactions or blocks. A copy of this ledger is kept at every node and is accessible to every node. The scalable ledger can be shared with anyone on the basis of the accuracy of transactions or blocks ordering through consensus by anyone with either a permissionless or permissioned participation. Here we will see the permissionless type of scalable ledger because they are the basis on which IOTA and Bitcoin work.

i) Unpermissioned Consensus Ledger: In a permissionless distributed ledger anyone can use the copies of the shared ledger and maintain its integrity through consensus. In Bitcoin, the ledger is maintained and kept up to date by the block miners and the whole copy of the database is available to the end user. This, in a way is not helpful for abstracting the required data and history of all transactions because of its huge size. On the other hand IOTA practices partition tolerance over availability and hence only the required information can be gathered from the whole ledger and kept on the device.

ii) Proof-Of-Work: It is possible that an attacker may have a plethora of Sybil identities which are not required to approve tips but still gains many votes. Bitcoin provides resistance to such attacks by having a computationally "costly" mining such that the computing resources are insufficient to pose as many entities. IOTA on the other hand provides security by using a new Tip-Selection algorithm as explained in the Whitepaper [1]. This algorithm uses random walkers which reference unapproved transactions also known as tips (unapproved nodes) which have to be genuine. Proof of work is said to be created when the node searches for the correct nonce (random number) and solves the complicated cryptographic puzzle.

iii) Proof-Of-Stake: In proof of stake there are elected members chosen via various combinations of random selection and 'the stake' they own. These members are elected by the creator of the next block. Proof of stake currencies are more energy efficient as they require low computational power because they do not have to solve the complicated cryptographic puzzles.

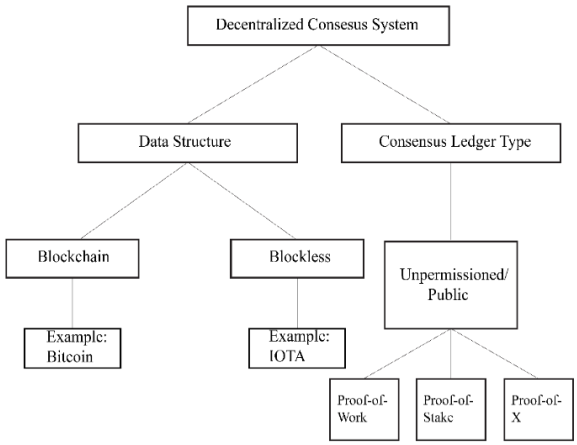

Fig. 1 Classification of Decentralized Consensus System

III.USE CASE

This section applies the Blockless Decentralized protocol which encompasses the various aspects of an IoT devices so that sharing of resources is possible between the “things” of IoT. A use case involving a smart cable and smart socket as shown in Fig. 2 is taken into consideration as described in [3].

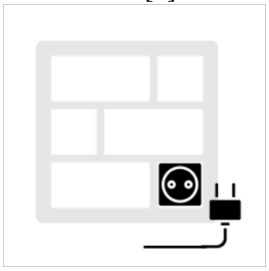

Fig. 2 A smart cable and smart socket

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

The scenario is such that one end of the smart cable is plugged into the smart socket and the other end to the appliance or "thing" of the IoT. The socket when not plugged is in standby mode. This means that the socket is providing a limited amount of power just enough to power the smart cable for a limited time. When the smart cable is inserted, the cable turns on and starts communicating with the socket. During this communication the cable requests for power and pays for a certain amount of electric energy using IOTA cryptocurrency. This request converts the socket from standby mode to paying mode. In the case where the cable is unable to pay, the socket waits for some time and then goes back to standby mode. In the case where the payment is done by the cable, and after usage if the energy is about to expire, the socket can notify this to the cable and it can choose to make a payment for continuous flow of electricity.
The purpose of using a third party API for payment that is IOTA, is because of the benefits this cryptocurrency offers over traditionally used Bitcoin. There is no transaction fees even for a transaction equal to 0.0000006 cents (1 Iota). On the other hand Bitcoin has a fees of 0.4628 cents (52 Satoshi/byte) as listed on 13th of March, 2018. The capability of the network to handle transactions in IOTA is much higher than Bitcoin. The IOTA network can handle 1000 TPS whereas Bitcoin can handle a maximum of 7 TPS because the Bitcoin protocol restricts the size of the block to just 1MB. Moreover as mentioned in [1], IOTA has resistance to various malicious attack scenarios like double spending, entering in fork state, “large weight” attack, parasite chain attack, Sybil attack, gaining of irrational computational power. The tip selection algorithm is used to select two tips (tips are nodes in The Tangle with unapproved transactions) instead of randomly selecting two tips. An additional security is provided against quantum computers which can calculate the required nonce in a small amount of time, but the IOTA implementation is structured such that the time required to find the correct nonce is not much larger than the time needed for other tasks like issuing a transaction.

Another important perspective to look at this use case is when the socket has excess energy and wants to earn money by selling it to another “thing” in the network. This is possible by using a technology that allows the smallest of the devices to connect to the internet. The Low-Power Wide-Area Network (LPWAN) network technology is used for the same. The devices with LPWAN have a battery life of about a week and hence are better than LTE using devices for data transfer and allows long range communication at low bit rate among “things”. Hence by using such a technology the socket can sell/transfer the remaining power through the Internet thereby having a secure transaction at no cost with no wastage of resources.

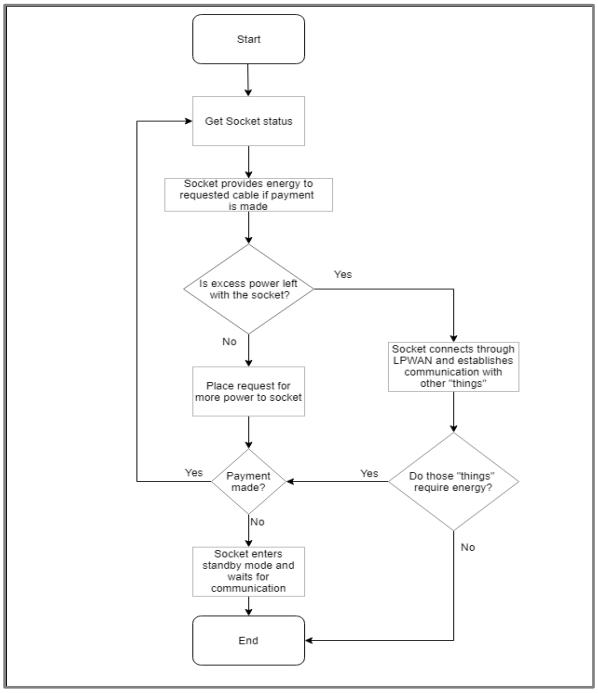

Fig. 3 Flowchart for request, payment and sharing of energy

In Fig 3, the flow of events occurring while communicating with the smart cable through the smart socket is shown. Also an additional event of excess resource being shared with other “things” through communication by the socket is also shown. In general, these “things” can connect over a LPWAN which is a wireless wide area network technology that interconnects many such low-bandwidth, battery operated devices over 2km to 1000km. Hence by combining the network technology with an appropriate payment and data transfer protocol which is permissionless and secure can initiate thing-to-thing payment for the IoT industry without any human intervention.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

IV.CONCLUSION

By looking at the scalable property as well as security provided for machine-to-machine economy by The Blockless Decentralized Protocol and its corresponding cryptocurrency that is IOTA, it is inevitable to say that accepting such a distributed network protocol universally is indeed a boon to boost the economy of "things". The required aspects of a decentralized consensus protocol for the working of micropayments without fees and at a faster rate suggest one answer and that sums up to the IOTA protocol. The IOTA network being asynchronous offers various advantages over other cryptocurrencies: (i) the no miner policy where the initiator of the transaction is itself the one who approves other transactions in the tangle (ii) the no transaction fees policy enables transactions to be executed free of cost (iii) the quantum resistant hashing algorithm (Winterrnitz Hashing Algorithm) enables the Tangle to be prevented from parasite chain attacks as well as from losing the hashing power to one sole proprietor. These points suggest a faster rate of 1000 TPS which is still better than Bitcoin.

The transfer of useful data between IoT devices like sensors, actuators, or any household device connected to the internet over a long range and at a faster speed can be achieved by using the same permissionless protocol. These devices can communicate for their requirement of certain useful data to another device connected to the Internet and hence receive the data through the mentioned protocol. This paper discusses only sharing and payment of services/resources offered by one "thing" to another "thing" which in our case is a smart cable to the smart socket and the smart socket to other "things" through LPWAN.

REFERENCES

[1] Sergui Popov, "The Tangle", October 1,2017, Version 1.3 Ph.D. in math (1997, Moscow State University)
[2] Kimcahi Yeow, Abdullah Gani, Raja Wasim Ahmed, Joel J.P.C. Rodrigues, Kwangman Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy and Research Issues", IEEE Access Journal, vol. 6, December 6, 2017, 10.119/ACCESS.2017.2779263
[3] Thomas Lundqvist, Andreas de Blanche, H. Robert H. Andersson,"Thing to thing Electricity micropayments using Blockchain Technology", Global Internet of Things Summit (GIoTS) 2017, IEEE Journal, June 2017.
[4] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," 2015, University of Berlin
[5] Scalability topic on Bitcooin wiki. [Online]. Available: https://en.bitcoin.it/wiki/Scalability
[6] Iota real world use cases. [Online]. Available: https://hackernoon.com/Iota-real-world-use-cases-are-coming-ab1d8240cf09
[7] The MatchX website. [Online]. Available: https://matchx.io/