AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 3(1) (2022) 93-99
DOI: 10.22060/AJMC.2021.20153.1055

Applying IOTA into distributed computing to master the uncertainty

Morteza Mozaffari[a], Farhad Rahmati*[a]

[a]*Department of Mathematics and Computer Science, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran*

ABSTRACT: In distributed computing, the uncertainty is the most challenging issue which is caused by the asynchrony of distributed entities' communication and many other reasons such as geographical scattering of distributed entities, their mobility, and etc. In this paper, IOTA, a DAG based Distributed ledger technology is used in order to cope with asynchronous communications and uncertainty. Moreover, IOTA private network is chosen to deal with other mentioned problems inside distributed computing. As a case study, a system is presented which could be implemented inside Tehran Polytechnic university to bring computational power of computers with low resources together in order to solve many problems which can be solved in distributed computing manner.

Review History:
Received:09 June 2021
Accepted:31 August 2021
Available Online:01 February 2022

Keywords:

Distributed ledger technology
Blockchain
IOTA
Directed acyclic graph
Distributed computing

1. Introduction

By emerging bitcoin as a peer-to-peer cash system in 2008 [9], distributed ledger technology(DLT) has been considered by researchers from many fields such as computer science, mathematics, engineering and etc. Hence, many DLTs have been introduced which have its own special features, for instance, in 2013 Ethereum, adds smart contract to DLTs [2]. These DLTs have been used in many fields such as energy trading [4, 8], intelligent traffic system [13], supply chain [7] and etc. The core of these DLTs is blockchain. Blockchain is composed of blocks which each one references to the previous one by using hash functions and each block includes a group of transactions. Blockchain is used as data structure to store data(transactions) which is transferred in the peer-to-peer network. From now on, we call these DLTs blockchain-based DLTs.

As mentioned above, blockchain has linear structure, meaning that blocks are generated after previous ones. This feature reduce the number of transactions that are sit in ledger, for example, creating a block in bitcoin takes 10 minutes (this happens because of the proof of work which should be done before spearing blocks) and the size of blocks are limited so that almost seven transactions are processed per second. Although, this number has been increased by using proof of stake instead of proof of work in other blockchain-based DLTs, many applications need more transactions to be appended to ledger per second. Limited blocks size and low transactions process are the main reasons of the scalability issues [3].

In 2015, IOTA was introduced by Serguei popov [11] which uses Tangle instead of blockchain. IOTA and blockchain based DLTs have been compared by Huma Pervez et al [10] and etc. The main features of IOTA which make it a suitable alternative for blockchain are as the following:

- Tangle is DAG which its vertices present transactions of the nodes, so that transactions can be appended to the ledger at the same time. This feature increases number of transactions processed by network, makes IOTA more scalable than blockchain based DLTs and also increases the transaction confirmation rate.

*Corresponding author.
E-mail addresses: m_mozafari@aut.ac.ir, frahmati@aut.ac.ir

- As well as value transaction which is used for transfer cryptocurrency, IOTA has zero-value transaction which can be used to transfer data between nodes and store those data in the ledger.
- In the blockchain based DLTs, miners are interested in the transactions with high transaction's fee. On the other side, the importance of micropayments is increased in the industry. IOTA has no miner so that transactions do not have any fees.

After IOTA, other DLTs have been raised with the same idea, for instance, Hashgraph and Dledger. Instead of proof of work, DLedger utilizes proof of authentication which makes DLedger more IOT-friendly than IOTA. Apart form this, DLedger is built upon a data-centric network called Named Data Networking (NDN), which facilitates the peer-to-peer data broadcasting in heterogeneous IOT networks [14]. Hashgraph is based on a gossip protocol, meaning that the participants don't just gossip about transactions. They gossip about gossip. They jointly create a Hashgraph reflecting all of the gossip events. By doing this, Byzantine agreement is accomplished through virtual voting[1]. From now on, we call these DLTs DAG-based DLT.

Distributed computing emerges when a problem has to be solved in terms of distributed entities such that each entity has only partial knowledge of the many parameters involved in that problem. Hence, in any distributed computing problem, there are several computing entities, and each of them has to locally compute a part of the problem, whose scope is global. The uncertainty is not under the control of the programmer [12]. The most fundamental concept in distributed computing is the task which is defined as follows:

Definition 1.1. *Let $p_1, p_2, \cdots p_n$ be computing entities and O, I be the set of output and input vectors respectively. The task, the basic unit of distributed computing, is the mapping T from I to O such that for each input vector $i \in I$ there is an output vector o such that $o \in T(I)$ [12].*

Remark 1.2. *Let $i = [in_1, in_2, \cdots in_n] \in I$ be an input vector, each entity p_i is only known about its input in_i. Similarly, let $o = [out_1, out_2, \cdots out_n] \in O$ be an output vector, each entity p_i can only compute its own output out_i[12].*

The uncertainty is caused by many reasons such as asynchrony of distributed entities' communication, geographical scattering of the computing entities, their mobility and etc. In distributed computing, entities are expected to communicate with each other, and type of their connection is asynchronous. In this type of communication, entity A (sender) sends data which is required by entity B to make a decision and the sender does not have any knowledge about receipt process. If entity B does not receive the data, it will make a wrong decision which results in uncertainty. In this paper, DLT is applied into distributed computing in order to use its features to cope with the uncertainty which is the most fundamental issue inside distributed computing(at least at the authors point of views). The advantages of applying IOTA inside distributed computing can be listed as follows:

- In IOTA, all data has been saved in a ledger immutably such that each node in the network has one copy of the ledger. This data can be used by distributed entities in order to be sync with the rest of the network. In DLT especially in IOTA, nodes make themselves sync by the rest of the network, therefore, they never lose data.
- IOTA has a cryptocurrency, called IOTA, so that we establish a payment system, meaning that each entity can be paid in exchange for resource that they have shared with the network.
- That transaction rate (data which is added to the ledger) will increase and it is more scalable than blockchain-based one.
- As mentioned above, the geographical spreading of distributed entities and their mobility can result in uncertainty. We choose private network instead of the public so that distributed entities are controlled by the service provider.

As a case study for the system, we deploy it in the Tehran Polytechnic university. This system is used to take advantage of universities' unoccupied computers in order to carry out computations inside university which can be done with distributed computing manner.

The rest of this paper includes four sections: In section 2 IOTA is summarized. System architecture is described in sections 3. In section 4 we present a case study. And finally, section 5 includes future work.

2. IOTA

In this section, for readers' convenience, some concepts of IOTA will be reviewed. This section is collected from [6, 5]

Definition 2.1. *IOTA is a DLT that allows devices in an IOTA network to transact in micropayments and to send each other immutable data. IOTA uses Tangle to store this data.*

Definition 2.2. *Tangle is a DAG(figure 1) IOTA uses as distributed ledger in order to contain an up-to-date history of transactions. All nodes in the IOTA network have one copy of the Tangle.*

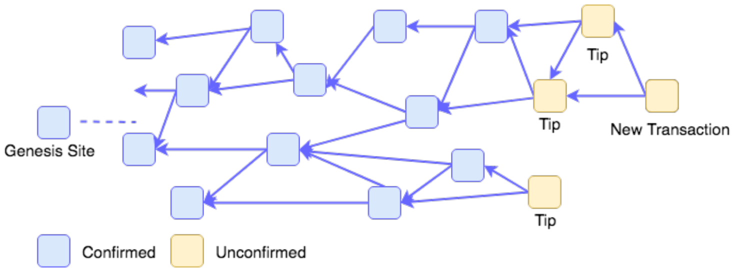

Figure 1: The Tangle

Each site(vertex) in the Tangle indicates the transaction and each edge represents the approval of the transaction. If there is a directed edge from transaction x to y, it means that transaction x directly approves the transaction y. Also, transaction x indirectly approves the transaction y if there is a directed path from x to y.

Definition 2.3. *The transaction which is not approved by any other transaction is called the tip.*

In the IOTA, any data should be transmitted as a transaction and nodes should execute the following steps in order to send transactions to the network:

1. Create the transaction.
2. Do a light proof of work.
3. Select[1] two tips transaction and approve them.
4. Send transaction to its neighbors.

When the neighbors receive the transaction, they validate it. In case of authentication, they will add the transaction to their local ledger and send it to their neighbors. By continuing this approach, the transaction is distributed among the network. There are three types of transactions in the Tangle including, tips, confirmed, and unconfirmed.

In order to measure the transaction's level of acceptance by the rest of the Tangle, IOTA introduce a concept called confirmation confidence which is computed as follows:

1. Select 100 tips by tip selection algorithm.
2. Count how many of those 100 tips approve the transaction, and call it A.
3. The confirmation confidence of our transaction is “A percent”.

In this consensus, one can use its computational power to send many tips to approve one transaction and increase the confirmation confidence of the transaction so that IOTA uses the coordinator which is responsible to confirm the transactions. Coordinator periodically sends milestone transactions. The transactions which are approved by milestone transactions are considered as confirmed transactions.

3. system architecture

The system is composed of six components including distributed task(DT), distributed entities(DEs), task manager function(TMF), answer finalizer function(AFF), outputs database(ODB) and service provider(SP). Each component is defined as follows:

- DT is a problem which is going to be solved by the assumption that each entity has only partial knowledge about its parameters.
- Distributed entities are the main part of the system. They contribute in the system by computing out_i according to in_i. A distributed entity can be an IOTA node or a client which connects to an IOTA node in order to interact with IOTA private network. Distributed entities which run the IOTA node softwares [2] form the IOTA private network.

[1] The selection of two tippes is done by tip selection algorithm which is discussed in [11].

[2] IOTA networks consist of interconnected nodes that run the same node software. This software gives nodes read/write access to the Tangle, allows them to validate transactions, and allows them to store transactions in their local ledgers.

- TMF is responsible for finding the best entities in order to contribute to problem-solving. TMF has knowledge about entities' computational power and resources that are required to obtain $out_i (i = 1, 2, ..., n)$.
- ODB is a local database which is used to store entities outputs.
- AFF is a function which get entities' outputs and then calculates the final answer.
- SP is a utility that runs the private network. All distributed entities in the system should be confirmed by SP. SP also pays for nodes or clients who brought their computational power to the network.

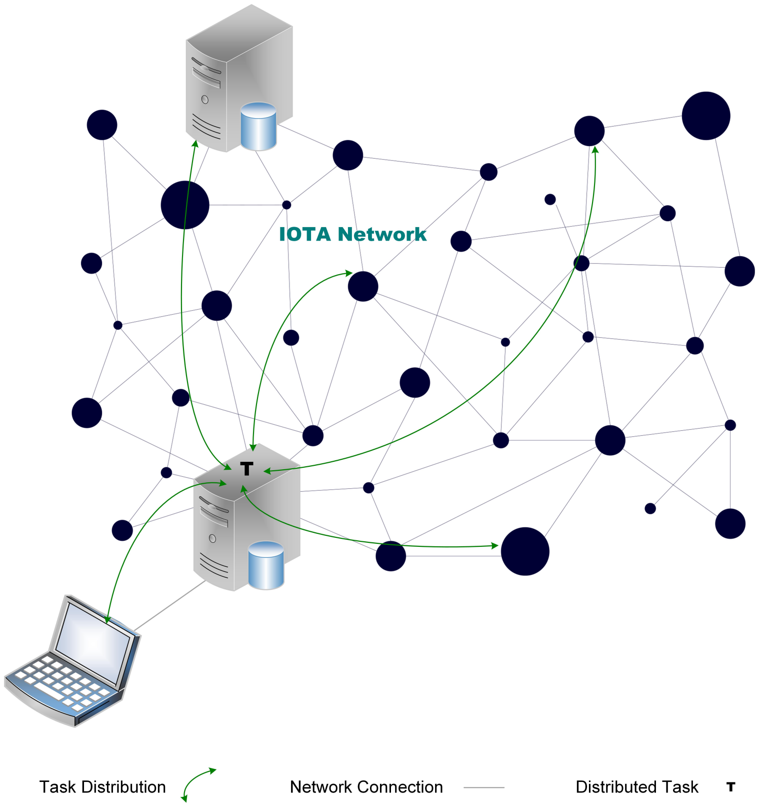

Figure 2: system architecture

Consider input vector $i = [in_1, in_2, \cdots, in_n]$ and output vector $o = [out_1, out_2, \cdots, out_n]$, $out_i = f_i(in_i)$. Also, let μ_i be the computational power which is required to run f_i. To calculate the output vector, the system follows these steps:

1. Functions($f_i \;\; i = 1, 2, \cdots, n$) would be defined then, DEs would be selected by TMF.
2. Zero-value transactions [3] are sent to the selected DEs. Data which is required to run functions is stayed on the message field of the transactions. This data includes inputs, functions which DEs are asked to invoke, time(in the future), when the outputs should be computed. These transactions have the same tag.
3. According to the message field of the transactions, DEs will start invoking functions. After computing outputs, they are sent to the network as message filed of new transactions(response transactions). These new transactions have the same tag as transactions in the previous step. Each output should be sent before the mentioned time, on the other hand, new DE will be replaced.
4. The message fields of the answer transactions are saved in ODB. By storing outputs in the local database(ODB), the ledger will not be searched in order to find the outputs.
5. When all outputs are saved in OBD, the final output is achieved by AFF.

Distributed computing is about mastering uncertainty [12]. As we mentioned above, entities are aware of just their own inputs, on the other hand, in some cases, they are assumed to interact with the rest of the network. This interaction can be necessary in order to obtain some data which is required to figure the outputs. In these cases, they communicate in asynchronous way. Consider node i, which is supposed to compute out_i, should have received some data from node j. In traditional distributed computing, node j sends the data and it does not concern about

[3] A zero-value transaction has a value of 0 in the value field. These transactions are useful for sending messages without IOTA tokens.

the way that node i receive the submitted information. If node i doesn't acquire the data, it will make a wrong decision. In our system, considered data is available in the distributed ledger so that it can be used by node i in order to obtain out_i. Each DE, which considered to carry out an output, should do its job in the period which is supposed, on the other hand, new DE is asked to figure out the output. By these measures, the final output will be obtained under any circumstances.

We opt for IOTA private network so that all nodes and clients in the network are authenticated by SP. Doing so, when they are asked to call a function and send the answer to the network, they really will do their tasks correctly. In the private network, distributed entities are controlled by SP and all entities trust the SP. This help to improve the certainty by coping with the geographical scattering of distributed entities and their mobility.

4. Tehran Polytechnic university's distributed computing system

Tehran Polytechnic university has almost 6500 PCs and 220 servers. The servers can approximately do 175000 billion operations per second and their total memory size is roughly 60000 GB. It is anticipated that 50 percentage of the CPU and 40 percentage of the memory are unconsumed. For PCs, they are distributed among university, for example, in the department of mathematics and computer science there are almost 410 computers. Information about their CPUs is not available but it can be estimated that their whole memory size is 19000 GB. These computers are unused in most of the time, for instance, computers are shut down at night, or faculty's computers are unoccupied in class time. Furthermore, some students have Laptop they do not use all of its resources. On the other side, the university has to pay for expensive supercomputers for computations. Although the supercomputer has high resources, students must wait for a long time to be able to use the computer. Remarkable part of these computations can be done in distributed computing manner so that the university can establish an IOTA private network and conduct these computation without paying for those supercomputers.

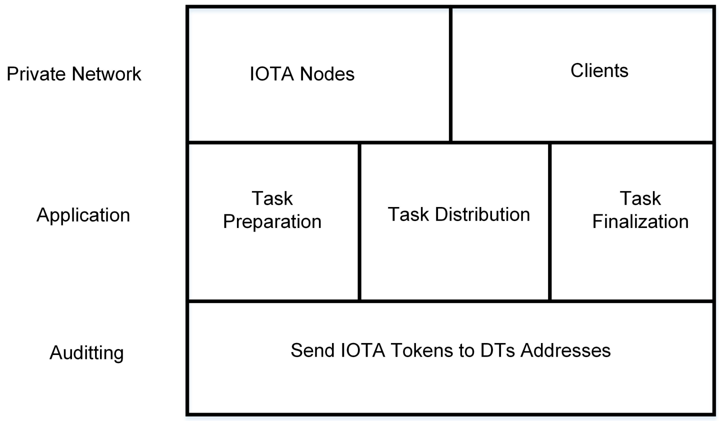

Figure 3: system architecture

In this section, we propose a system which use unoccupied computers in order to leverage the resources of all devices in the university. In our system, university can establish an IOTA private tangle [4]. It is composed of the computers of the university and students computers. This system is divided into three components including private network, application, and auditing (figure 3).

4.1. Private Network

The private network includes computers which run IOTA node software. These computers belong to the university or its students. The motivation for the university to bring its computers to the private network as node, has been discussed. For students, there are two options to contribute to the system, running an IOTA node software or connecting to a node. Students have to pay for facilities which they use in the university such as gym, restaurants and etc. Also, some of them pay for tuition. So, they have enough motivation to participate in the network instead of paying directly. It is worth mentioning that the billing process is different for nodes and clients. The computational power of the system is equal to the computational power of the nodes and clients and it is known at any time.

[4] A private Tangle is an IOTA network that you control and that contains only nodes that you know. A private Tangle uses the same technology as the public IOTA networks, except you control it by running an open-source implementation of the Coordinator called Compass. You can use Compass to allow nodes in your own IOTA network to reach a consensus on Compass' milestones instead of the Coordinator's ones

4.2. Application layer

The application layer is divided into three parts including task preparation, task distribution, and task finalization, as follows:

First step in the system is task preparation, that is the problem(task) which should be solved, required functions and its inputs should be figured out. As well as this, computational power which is required in the execution of the functions, should be determined. The output of some functions might be required to run other ones, therefore, these functions should be run as soon as possible. For this reason, we assign more computational power to these functions.

According to the computational power of DEs and functions, TMF distributes functions among DEs. In this case study, the functions are added to the message field of zero-value transactions as well, so that DEs do not have access to the functions. Each function and the entity which is considered to run it are saved in the ODB. All DEs are listening to transactions which its receiver address belongs to them. When they access transactions, the function will be executed. By obtaining the output, entities will have sent it to the network by IOTA transaction(response transaction). As it's shown in figure 2, the server which runs the application could be a node in the private network, therefore, it can contribute to the problem-solving. The last step is finalizing the DTs outputs by AFF. This function does not need computational power, for instance, if the task is computing $f(x) + g(y)$ and two DEs are responsible to find $f(x)$ and $g(y)$, AFF is the $+$ operation. The server is listening for response transaction and save them to the ODB. When all responses are saved in the database, the AFF is involved. By saving outputs in ODB, we do not need to search on the distributed ledger, solving process can be tracked and also these data can be used to accounting.

4.3. Auditing

Similar to the public network, IOTA private tangle has token called IOTA. It is worth mentioning that this token has no value in the public network and cannot be negotiated. In order to encourage students to bring their computational power, the university sends them a bill at the end of the each month, meaning that send IOTA tokens to their address. These tokens can be used to pay for university's facilities, or pay for tuition. Data that is saved in the ODB can be used to prepare bills.

5. Future Works

In our system, we assume that entities are controlled by SP so that they follow the instructions which are defined by SP. In the future, we plan to develop our system in the public environment, meaning that the entities could be malicious ones and the system should be able to cope with them. In the public area, data (such as inputs, functions and etc.) will not be sent clearly. This measure is done in order to preserve privacy of data. Homomorphic encryption will be used, meaning that the outputs can be computed by using the encrypted form of the data.

References

[1] L. Baird, The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. Swirlds, Inc. Technical Report SWIRLDS-TR-2016, 1, 2016.

[2] V. Buterin, A next generation smart contract & decentralized application platform (2013) whitepaper. Ethereum Foundation.

[3] A. Chauhan, O. P. Malviya, M. Verma, T. S. Mor, Blockchain and scalability. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (2018), 122-128.

[4] P. Ferraro, C. King, R. Shorten, Distributed ledger technology for smart cities, the sharing economy, and social compliance. IEEE Access, 6 (2018), 62728-62746.

[5] IOTA fundation. what is the iota. Available online https://docs.iota.org/.

[6] A. Gal, Confimation confidance. Available online https://blog.iota.org/the-tangle-an-illustrated-introduction-f359b8b2ec80/.

[7] M. Iansiti, K. R. Lakhani, The truth about blockchain, Harvard Business Review, 9, 2017.

[8] N. Lasla, M. Al-Ammari, M. Abdallah, M. Younis, Blockchain based trading platform for electric vehicle charging in smart cities. IEEE Open Journal of Intelligent Transportation Systems, 1 (2020), 80-92.

[9] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. bitcoin, 2008.

[10] H. Pervez, M. Muneeb, M. U. Irfan, I. U. Haq, A comparative analysis of dag-based blockchain architectures. In 2018 12th International Conference on Open Source Systems and Technologies (ICOSST) IEEE (2018), 27-34.

[11] S. Popov, The tangle. Available online https://www.iota.org/foundation/research-papers, 2015.

[12] M. Raynal. Parallel computing vs. distributed computing: a great confusion?(position paper). In European Conference on Parallel Processing, pages 41-53. Springer, 2015.

[13] P. Zeng, X. Wang, H. Li, F. Jiang, R. Doss, A scheme of intelligent traffc light system based on distributed security architecture of blockchain technology. IEEE Access, 8 (2020), 33644-33657.

[14] Z. Zhang, V. Vasavada, X. Ma, L. Zhang, Dledger: An iot-friendly private distributed ledger system based on dag. arXiv preprint arXiv:1902.09031, 2019.

Please cite this article using:

Morteza Mozaffari, Farhad Rahmati, Applying IOTA into distributed computing to master the uncertainty, AUT J. Math. Comput., 3(1) (2022) 93-99
DOI: 10.22060/AJMC.2021.20153.1055