Toward a mixed Tangle-Blockchain architecture

Motaz BEN HASSINE [a,1], Mourad KMIMECH[b] , Hussein HELLANI[c] and Layth SLIMAN[d]

[a] *ISIM Monastir, Tunisia*

[b] *LIPN, Sorbonne University Paris-Nord, France*

[c] *Pau University, Pau, France*

[d] *EFREI Paris, VilleJuif, France*

Abstract. This paper presents the design and implementation of a new platform that takes into consideration the requirements and constraints resulting from the industrial context based on IoT. This platform combines the "Tangle" and "Blockchain" techniques. Tangle is primarily designed to address scale-up issues and the relatively high cost (time and resource) of transactions in a traditional blockchain-based platform. Unlike the "blockchain" structure, it consists of a solid mathematical foundation called DAG (Direct Acyclic Graph). It uses a validation process in which transactions are entered into the distributed registry after authenticating two other randomly selected transactions according to a Poisson distribution (thus, the locations of the new transactions are chosen using random runs in the graph) . Therefore, it is an easily scalable system that does not require mining or transaction fees. We aim to study the integration of Tangle and Blockchain techniques to improve the performance and scalability of distributed registry-based platforms to be adapted in industrial enterprises whose processes incorporate or are based on IoT.

Keywords. Blockchain, IoT, Tangle, Transactions

1. Introduction

Nowadays, connected objects have appeared in our daily life. Examples include, smart thermostats that regulate the temperature of our home based on our habits and weather data borrowed from the web, smart lights that only turn on when someone is in the room, the refrigerator that is capable of order all you need on your own or smart locks which are capable of automatically closing a house. These objects are equipped with more or less intelligent sensors that are present in our environment. These objects are characterized by their intelligence. They are equipped with processors aiming to operate algorithms capable of learning our habits and therefore of adapting to our daily life while combining the information collected on their environment with the data found on the Internet. In current studies, Strategy Analytics [10] has looked at Internet of Things- IoT, predicting 38.6 billion connected devices by 2025 and 50 billion by 2030, with irregular growths. This growth movement will certainly raise important questions, starting with storage and security. One good candidate for these issues is Blockchain infrastructure. Actually, Blockchain has many advantages, including its fully decentralization nature, data integrity, privacy preservation, and anonymity [11]. However, the scalability and

[1] Corresponding Author, Motaz Ben Hassine, ISIM Monastir, University of Monastir, Tunisia, E-mail: motazbenhassine@gmail.com

transaction cost of these infrastructures are considered as a real brake for their use in IoT based industry. To cope with this drawback, Tangle protocol, used in the IOTA platform [4] Has been designed. On the other side, installing DLT tangle-based will solve scalability and working offline issues. However, a smart contract does not run on a tangle-based environment. In addition, the peripheral IoT devices are usually incapable of cooperating with Blockchain requirements due to their limited resources and specs. A real use case was the agriculture-based industry where no robust internet infrastructure and law enforcement is not guaranteed [7].

In this paper, we will present in section 2 the background by taking a general view about distributed ledgers and explaining some related works about using Blockchain in IoT uses cases. We will present in section 3 Tangle integration with Blockchain starting by in first with some motivations then its architecture, its behavior and finally the importance of Blockchain integration with Tangle and its keys of success. Then, in section 4, we will explain our connector implementation. We will focus on the architecture of this implementation then the connector behavior and finish by an implementation validation. This section will be like an execution scenario using DS18B20 temperature sensor. Finally, we will present the conclusion and future work in the last section.

2. Background

In this section, first, we will take a general view about distributed ledgers. Second, we will present related works about using Blockchain in IoT.

2.1. Distributed ledgers overview: Tangle and Blockchain

Blockchain [1] is a technology for storing and transmitting data that guarantee its integrity and transparency. This technology works without a trusted third party. The blockchain contains the history of the data exchanged in the network. This secure database is replicated in all the nodes of the network. The blockchain contains a set of blocks, which are chained; each block contains a list of transactions and some other specific data.

Any Blockchain consensus tries to achieve some features; the most important of them are decentralization, immutability and irreversibility.

- Decentralization

  The network is decentralized [2], which means that it does not have a single authority. A group of nodes maintains the network, which makes it decentralized. Add to that, Blockchain is fully distributed into the network this guarantees that data will never be lost.

- Immutability

  Each node in the system has a copy of the ledger. To add a transaction, each node must check its validity, after having added it to his own ledger, the transaction is added into a block, then it is appended to the Blockchain ledger. Therefore, nobody can simply go back and modify it. In fact, no user on the network can modify, delete, or update it [2].

- Irreversibility

  The hash is quite complex and, it is impossible to modify or reverse it [2]. No one can take a public key and find the private key. In addition, a single change in entry could lead to a completely different ID; insignificant changes are not a luxury in the system.

- Smart Contract

With the birth of Etherum [3], a new concept, smart contract, was added. Vitalik Buterin invented it. It is a contract that makes agreement between two entities (a sender and a receiver).This contract is self-executed into the Blockchain; technically, the smart contract is a set of lines of codes written in specific language like solidity.

The consensus algorithm [12] has been studied for many years in distributed system. Some transplantable consensus algorithms are applied in blockchain. In the section below, we make a detailed description of the principles of these consensus algorithms. We focused three main consensus algorithms:

- PoW (Proof of Work)

The proof of work [12] consists in asking the miners to solve a complex mathematical problem requiring a significant computing power. A miner is a node in the Blockchain network with powerful resources and capacities having the right to create a block and validate it. The first node who solve this problem will be the miner and will create the next block on the blockchain. The chosen node (miner) applies a hashing algorithm to the same group of data until the desired result is found. The proof of work is the same as a competition and the motivation for this competition is that the winner will be paid afterwards.

- PoS (Proof of Stake)

A proof of stake algorithm [12] is presented as follows. There are a number of crypto currency owners who deposit them as part of the proof of stake mechanism: they become validators. The algorithm randomly selects a validator (the hazard being weighted by the total amount deposited, for example a validator with 10,000 crypto will be ten times more likely to be selected than a validator with 1,000 crypto) and assigns it the right to create the next block. If this validator does not create the block in a given time interval, a second validator is selected, and so on. As in the proof of work mechanism, the longest chain is by default considered the valid chain.

- PBFT (Practical Byzantine Fault Tolerance)

The principle of this PBFT algorithm [12] is as follows: The nodes of the system share messages between them to validate a block in the chain. Malicious nodes, in this case, can broadcast forged blocks. Therefore, the block, which is considered valid by a maximum number of nodes, is considered valid by the whole network. If f is the number of malicious nodes then we must have 3f +1 nodes required in the system and you need 2f + 1 node required for block validation.

Tangle [4] is a data structure that works in the background of IOTA. It allows storing data in the form of a direct acyclic graph (DAG). In this graph, a node represents a transaction and an arc represents the validation between two nodes. When a new transaction (node) added to the Tangle, it always validates two other transactions. Figure 1 below illustrates the shape of the Tangle data structure:

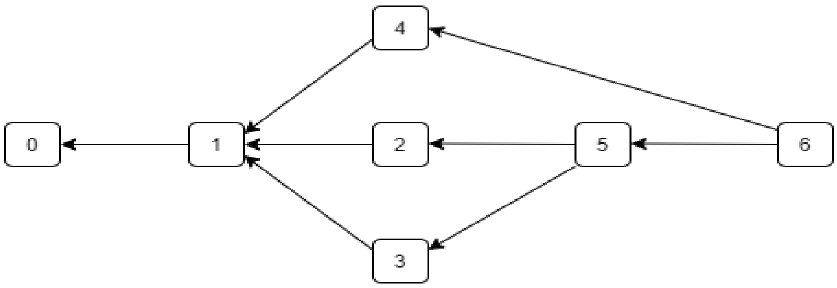

Figure 1. DAG [4].

Like other ledgers, Tangle had some features the most important of them is scalability and zero fees:

- Scalability

The primary motivation behind Tangle technology is to develop a scalable framework for manipulating transactions related to IoT [5]. Since each transaction requires the sender to verify two other transactions on the Tangle, more transactions can be confirmed as the number of users sending them increases, this means that IOTA [4] scales proportionally to the number of transactions ad infinitum. IOTA scalability is depicted in this graph [6].

- Zero fees

To send an IOTA transaction, a user's device must simply confirm two other transactions on the Tangle (the network). To confirm these two transactions, a device performs low difficulty "proof of work", which is essentially just a series of math problems. Almost any modern device including laptops and phones can do these math problems. The user and validator (miner, staker, etc.) are no longer decoupled entities in IOTA. This removes the need to waste large quantities of energy on mining, or risk inevitable validation centralization. More importantly, because the Tangle eliminates the requirement of miners, stakers, etc., newly minted units of currency and transaction fees do not need to be extracted from the system to pay validation fees. The result is that IOTA has zero fees [6].

To validate transactions in Tangle DLT, Iota foundation [13] has invented two main validation approaches:

- Random Tip Selection

This approach was very simple. In fact, the new incoming transaction randomly chooses two other unconfirmed transactions [4].

- MCMC (Markov Chain Monte Carlo) Walk Tip Selection

This approach puts a walker starting from the genesis transaction (oldest transaction), then this walker begins to walk in the opposite direction of the arc until reaching a transaction is not yet validated and therefore at the moment that the walker reaches the transaction (not yet validated) so this will be chosen to be validated. Before the walker's walks from a transaction to another transaction the criterion for choosing the path will be according to a calculated probability, which designates the percentage of choice of a node [4]. The probability is calculated as follows in Eq. (1).

$$\mathrm{P}_{xy} = \frac{e^{(-\alpha(\mathrm{H}_x - \mathrm{H}_y))}}{\sum_{z:z \to x} e^{(-\alpha(\mathrm{H}_x - \mathrm{H}_z))}} \tag{1}$$

In the equation above, **x** is the starting current transaction and **y** is the destination transaction.
$\mathbf{H_x}$ was the cumulative weight of transaction x, $\mathbf{H_y}$ was the cumulative weight of transaction y and $\mathbf{H_z}$ was the cumulative weight of transaction z.
$\boldsymbol{\alpha > 0}$ is the given parameter, which affects the level of chance in walk tip selection.

Z is a transaction belonging to the set of all the transactions validating directly the transaction x.

2.2. Related works

Blockchain was first introduced in the crypto currency environment; the same idea can be used in various other environments. Therefore, there is a need to conduct research on the possibilities of using Blockchain in other environments among which we can cite Blockchain in IoT systems. Iago Sestrem Ochôa and al [18], have worked on the use of Blockchain in the Smart Grid system. An innovation has the potential to revolutionize the transportation, distribution and conservation of energy. In fact, the current system of supplying electrical energy is almost entirely a mechanical system, with only limited use of the sensors, minimal electronic communication and almost no electronic control [19]. They proposed a Blockchain architecture, which uses SideChains [20] to make the system scalable and adaptable. They used three Blockchains to guarantee confidentiality, security and trust in the system. Another research work done by Bogdan Cristian Floreab and al [21], they worked on the integration of Blockchain in smart electric vehicles. They presented two different implementations, one for the smart vehicle and the other for the battery management system using Blockchain as the network and application data layer. The first implementation uses Ethereum as a Blockchain framework to develop smart contracts, while the second uses IOTA. Then they compared these two technologies demonstrating that the two platforms can provide a viable solution for an efficient, semi-decentralized, data-driven battery management system.

3. Tangle the Blockchain platform

In this section, we will explain the important motivations that encourage us to think about this new platform. Equally, we will explain the architecture of the platform. Then, we will adopt how our platform works and finally the importance of Blockchain integration with Tangle and its keys of success.

3.1. Motivation

In IoT systems, to enhance their security, the primarily used technology was Blockchain. However, Blockchain, which is directly installed on the nodes, is not possible because the peripheral IoT devices are usually incapable of cooperating with Blockchain requirements due to their limited resources and specs. On the other side, installing DLT tangle-based will solve scalability and working offline issues. However, a smart contract does not run on a tangle-based environment. In addition, Tangle was not fully decentralized because of the existence of the coordinator [7].

For that reason, we thought about a new platform that combine Blockchain and Tangle trying to guarantee feature of both (Tangle and Blockchain).

3.2. Tangle the Blockchain Architecture

This system is composed of the blockchain back-end platform and Tangle DLT frontend platform. These two platform are connected by an entity named connector that gets data from Tangle and sends it to Blockchain as shown in Figure 2 [7].

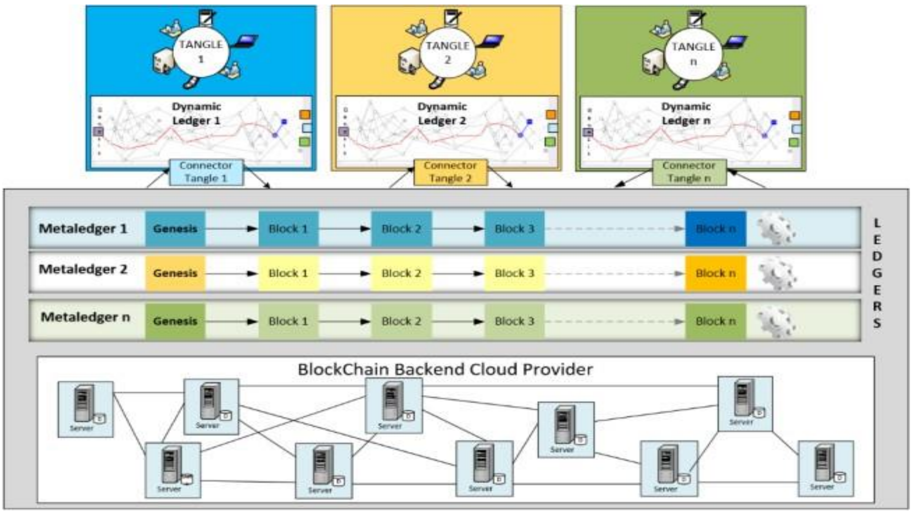

Figure 2. Tangle the Blockchain architecture [7].

3.3. Tangle the Blockchain behavior

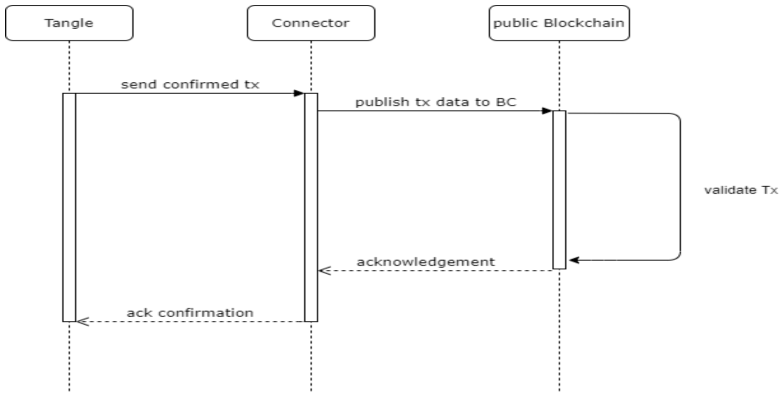

Figure 3. Tangle the Blockchain behavior.

In Figure 3 Tangle, ledgers validate the received data, validate the confirmed data and send it to the connector. This latter tries to adapt the data and reach to Blockchain consensus to send it into the blockchain.

3.4. The importance of Blockchain integration with Tangle and its keys of success

In Tangle, there is no exploitation or no competition on the realization of the proof of work "POW" to incite the node winner. Each node that aims to issue a new transaction must validate two other transactions by inspecting its local registry content and perform a local POW. In addition, a Tangle-based node can operate offline and synchronize transactions with the general ledger once connected. However, Blockchain cannot work offline. Whereas, IOTA is not entirely decentralized because it uses a trusted third party server named the « coordinator » [7]. Therefore, Blockchain was more decentralized than Tangle.

Another challenge for Tangle is the activation of smart contracts because Tangle cannot work with them. We notice that Blockchain alone and Tangle alone are unable to present a complete decentralized solution. Each has its features and limitations. We are merging Tangle and Blockchain to reap the benefits while minimizing their limits [7]. In fact, Blockchain complete Tangle limits and vice versa, so completion between these two technologies is the most important raison that made us to think about the integration of Blockchain with Tangle. The best practice for this new type of integration is to work upon three dimensions: **storage**, **computing,** and **end-user program**.

The success of any system will result from the equilibrium of these dimensions, where the weakness of any of these three parameters will affect the whole system [7].

- **Storage:** In our proposed architecture, the Blockchain ledger is independent of applications and participants. It is cloud-based running as a platform as a service (PaaS) where every data owner will preserve the required space or "quota" to run its application within a fully decentralized environment [7].
  Computing: it is a sensitive metric in any decentralized system. I t reflects time to apply the consensus algorithm and validate transactions. As the frontend tangle-based system is in continuing developments, the transaction confirmation will be shortened. Thus, its validation becomes faster [14]. The BFT [15] algorithm used with the backend Blockchain is up to the computing challenge for certain limit. In future work, we will consider the huge incoming tangle-based transactions and BFT capacity to sort out with the best practice to have maximum through put [7].
- **End-user program:** is represented by the software that is shared with the participants themselves or the application of IoT devices. A tangle-based platform includes communication protocols such as MQTT (Message Queuing Telemetry Transport) used in [16]. It permits end users and peripheral devices to interconnect and store their transactions and outputs within a fully decentralized storage platform. The end-user program is one of the three main sensitive metrics that have a direct impact on transaction speed. Thus, scalability is affected by the application type and architecture. There are standard measurements and tools (such as average response time, error rate, loop time, etc.) to monitor the performance and the functionality for any application [7].

4. Connector Implementation

In this section, we will explain our contribution by explaining our implementation architecture. Then, we will focus into the connector behavior, and an implementation validation.

4.1. Implementation architecture

To validate the feasibility of our intra-DLT model and test the interconnection between them the implementation of both Tangle and Blockchain has been realized.

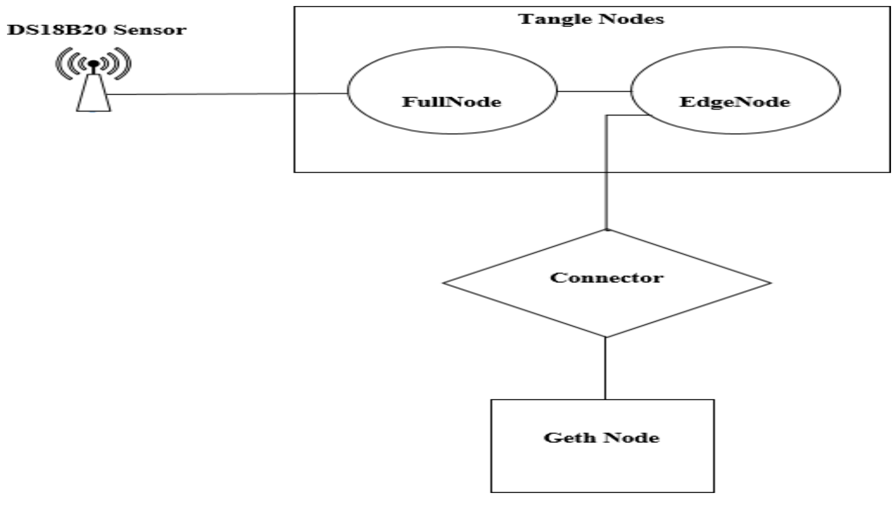

Figure 4. Implementation architecture.

In figure 4, we installed two Tangle nodes; FullNode, EdgeNode and a Blockchain node named GethNode (Go Ethereum Node). The FullNode and EdgeNode are two extension files ".jar" they are launched using the following commands: "**java –jar FullNode.jar -c FullNodeConf.ini**" and "**java –jar EdgeNode –c EdgeNodeConf.ini**". The files “FullNodeConf.ini” and “EdgeNodeCong.ini” are configuration files for each of the FullNode and EdgeNode. They make it possible to specify the reception ports, neighboring nodes, etc. The most important part in this architecture is the connector, which connects the Tangle nodes with a Blockchain node. It transfers the data received from the Edge Node and adapt to the Blockchain node. To generate the obtained data, we installed a DS18B20 temperature sensor, connected to FullNode to validate and store the data. FullNode receives the data, validates it, and then broadcasts it to EdgeNode. The latter will store a copy of this data, and then it will send the data to the connector. This one is in infinite listening, it receives the data as validated transactions, and therefore, it will adapt these transactions by transforming it into initial format (ASCII) and sending it as transactions to Blockchain (Geth Node).

4.2. Connector behavior

The connector works with the zero MQ (zero message queue) [8] protocol, it is a protocol operating in asynchronous messaging mode using a queue (message queuing). The connector is always listening into an infinite loop, indeed the EdgeNode is the data editor (Publisher) and the connector is a subscriber (Subscriber).The connector attaches to the Geth node using web3.js [10] framework then attaches to the Tangle EdgeNode node thanks to the zero MQ framework. If a confirmed transaction was received, it will adapt it by searching for the data with its initial format using the hash of the transaction. Finally, the connector sends the extracted data as a transaction sent to Geth node and returns to listening and so on.

The connector was implemented using JavaScript Language. This implementation available at [17].

4.3. Implementation validation: Execution scenario with a DS18B20 temperature sensor

We have implemented a script allowing recovering every 15 seconds a data coming from a DS18B20 temperature sensor, this script will send the data to the Tangle EdgeNode and FullNode nodes and therefore the scenario is as follows:

We start to launch the two Tangle nodes EdgeNode and FullNode using the commands written in section 4.1 and then we launch the Blockchain node named Geth using "**geth [options] command [command options] [arguments...]** ". The options can be port receipt of node, network id, name of Blockchain database, etc. The commands can be attach that means attach transaction data to the Blockchain database, init that means create new Blockchain database, etc.

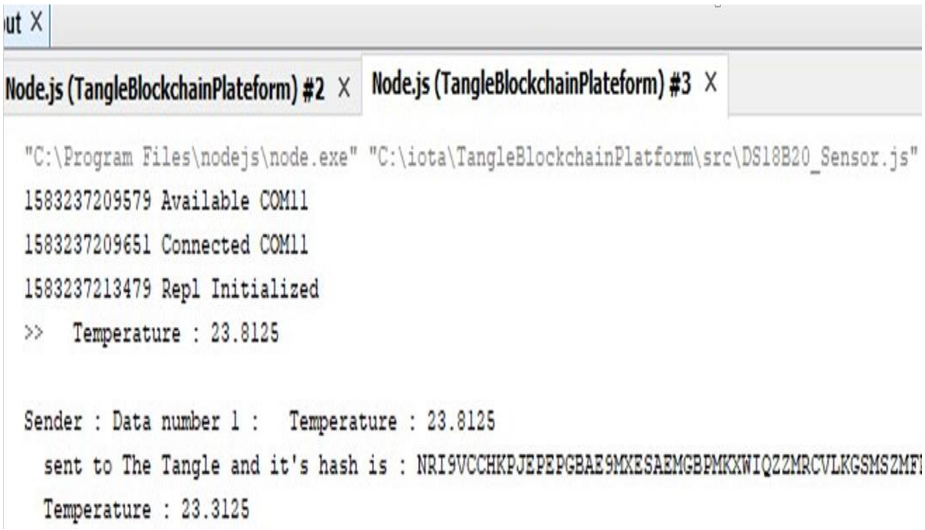

Figure 5. DS18B20_Sensor.js script launched

In the figure above, the script is launched and has started sending data from the sensor to the Tangle nodes. To see the execution results we put some figures below which illustrate its results:

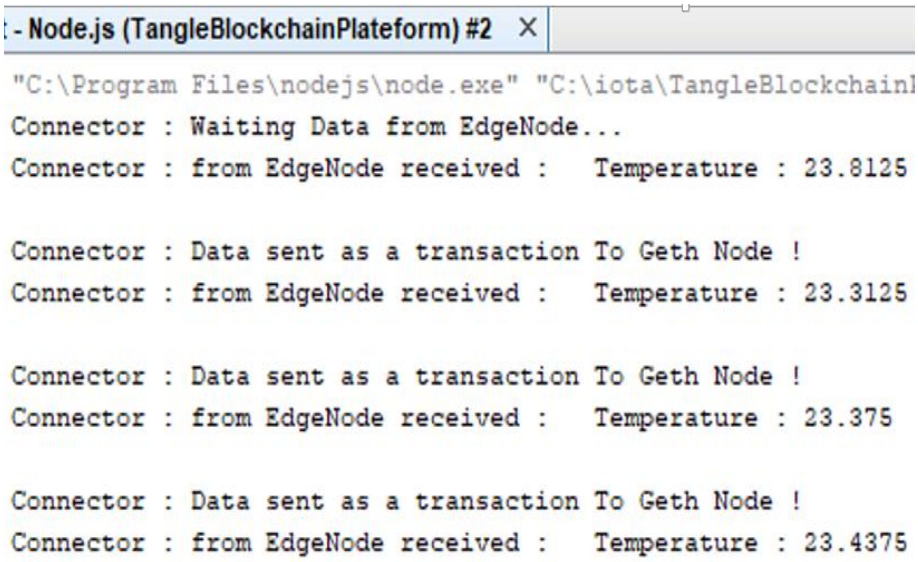

Figure 6. Connecting Tangle with Blockchain

In the figure above the connector receives the hashes of the transactions coming from the Tangle node (EdgeNode), then it allows to extract the data using the hashes of each transaction, these data are in ASCII format and it sends the data as transactions to the Blockchain node (Geth node).

To follow the number of transactions we can see the state of the Tangle nodes in the figure below:

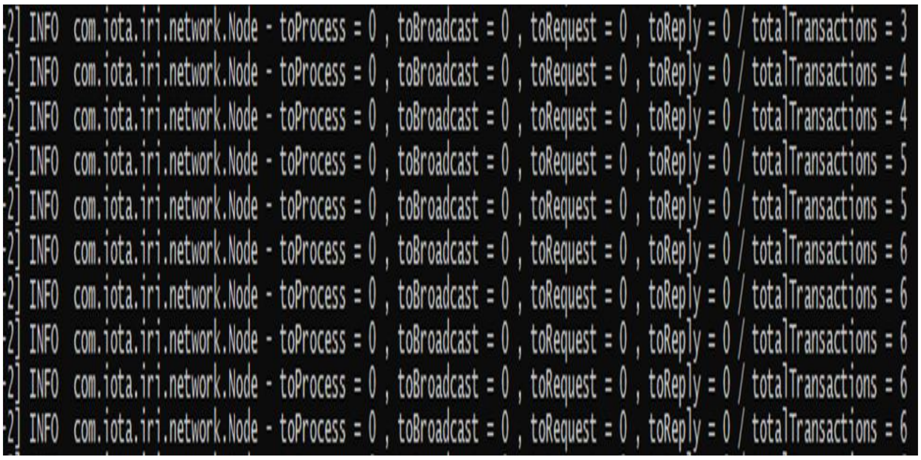

Figure 7. Tangle nodes after receiving data

To follow the current state of Blockchain, the figure below illustrates this:

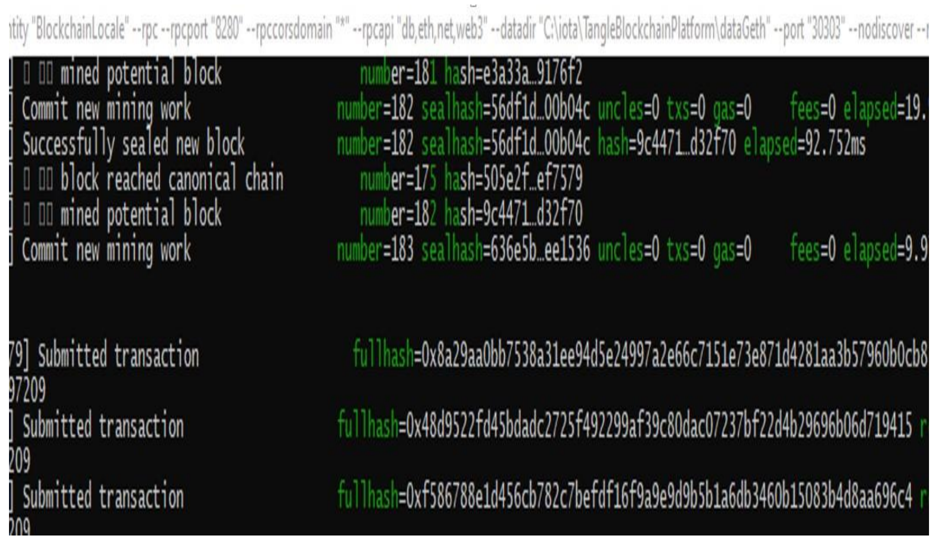

Figure 8. Blockchain Geth node after receiving data

The Figure above illustrates the execution of the Blockchain Geth node (Go Ethereum node) but the results are not very clear due to the speed of the display. That is why we have implemented a Dashboard using react js framework that allows following the state of our Geth node. The figure below shows the number of mined transactions:

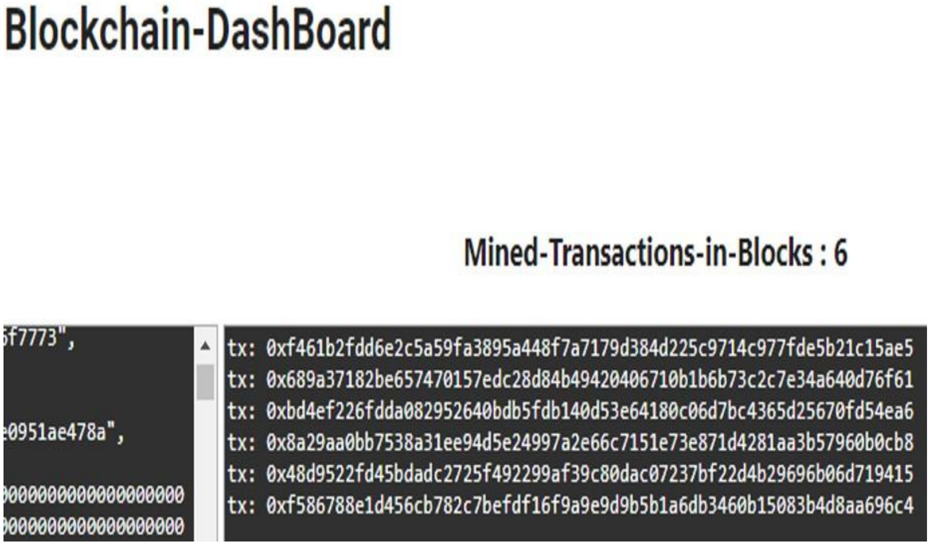

Figure 9. Current state of the Blockchain node.

5. Conclusion and future work

In this paper, we started in section 2 by presenting the background by taking a general view about distributed ledgers and explaining some related works about using Blockchain in IoT uses cases. After that, we explained in section 3 the Tangle integration with Blockchain starting first with some motivations then its architecture, its behavior and finally the importance of Blockchain integration with Tangle and its keys of success. Then, we explained in section 4 our connector implementation. We focused on the architecture of this implementation, then the connector behavior and an implementation validation. Future works will focus on searching how to add smart contract into our intra-DLT by extracting the main challenges of it and trying to find an optimized solution and validating it into a real use case like supply chain management. In fact, we will use the smart contract to be running on top of it as workflow data orchestrators. In addition, we will try to install our Blockchain node in real cloud servers to see the real performance of our platform.

References

[1] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[2] https://101blockchains.com/introduction-to-blockchain-features/#prettyPhoto

[3] B.Vitalik, "A next-generation smart contract & decentralized application platform".(2014). https://github.com/ethereum/wiki/wiki/White-Paper .

[4] Popov, S. The Tangle. Available online: https://iota.org.

[5] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, Rich Picking « *A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)* », September 2015.

[6] https://iotasupport.com/whatisiota.shtml

[7] Hussein Hellani, Layth Sliman, Motaz Ben Hassine, Abed Ellatif Samhat, Ernesto Exposito,Mourad Kmimech« *Tangle The Blockchain : Toward IOTA and Blockchain integration for IoT Environment* », The 10th IAS Conference on HIV Science – known as IAS 2019 –in Mexico City, Mexico, 21-24 July 2019.

[8] Celar Stipe, Mudnic Eugen, Seremet Zeljko «*State-of-the-Art of Messaging For Distributed Computing Systems* » International Journal - VALLIS AUREA • Volume 3• Number 2• Croatia, December 2017.

[9] Fabian Vogelsteller, Marek Kotewicz, Jeffrey Wilcke, Marian Oance « *web3.js Documentation Release 1.0.0* » Jun 05, 2019.

[10] https://news.strategyanalytics.com/

[11] H. Hellani, et al « *On Blockchain Technology: Overview of Bitcoin and Future Insights.* » IMCET, 2018.

[12] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun «A Review on Consensus Algorithm of Blockchain » 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017.

[13] https://www.iota.org/the-foundation/the-iota-foundation

[14] Jiang, Yiming, ChenxuWang, YaweiWang, and Lang Gao. « *A Cross-Chain Solution to Integrating Multiple BCs for IoT Data Management* », 2019. DOI: 10.3390/s19092042 Sensors 19(9):2042.

[15] Ethan Buchman, Jae Kwon and Zarko Milosevic « *The latest gossip on BFT consensus* ». September 24, 2018.

[16] D. Strugar, et Al. « *On M2M Micropayments: A Case Study of Electric Autonomous Vehicles* ». 2018 IEEE International Conference on Internet of Things. https://arxiv.org/pdf/1804.08964.pdf

[17] https://sourceforge.net/projects/tangleblockchain/

[18] I. Sestrem Ochôa, L. Augusto Silva, G. de Mello, N. M. Garcia, J. Francisco de Paz Santana and V. Reis Quietinho Leithardt « *A Cost Analysis of Implementing a Blockchain Architecture in a Smart Grid Scenario Using Sidechain* », 5 February 2020.

[19] https://smartgrid.epri.com/, June 2020.

[20] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille « *Enabling Blockchain Innovations with Pegged Sidechains* », 22 October 2014.

[21] B. Cristian Florea and D. Daniel Taralunga « *Blockchain IoT for Smart Electric Vehicles Battery Management* », 13 May 2020.