# Comparative Analysis of Distributed Ledger Technologies

George Suciu
*R&D Department*
*BEIA Consult International*
Bucharest, Romania
george@beia.ro

Carmen Nădrag
*R&D Department*
*BEIA Consult International*
Bucharest, Romania
carmen.nadrag@beia.ro

Cristiana Istrate
*R&D Department*
*BEIA Consult International*
Bucharest, Romania
cristiana.istrate@beia.ro

Alexandru Vulpe
*Telecommunications Department*
University Politehnica of Bucharest
Bucharest, Romania
alex.vulpe@radio.pub.ro

Maria-Cristina Dițu
*R&D Department*
*BEIA Consult International*
Bucharest, Romania
maria.ditu@beia.ro

Oana Subea
*R&D Department*
*BEIA Consult International*
Bucharest, Romania
oana.subea@beia.ro

***Abstract*—Distributed Ledger Technology (DLT) refers to a digital method for registering virtual transactions and other similar data in multiple locations simultaneously. The main characteristic of distributed ledgers is that they do not have a central administration component, due to advanced algorithms and methods used for record-keeping. Thus, transactions are faster and reasonable, as they do not require a central authority to validate them. The network is formed by multiple nodes through which the participant can access recordings, making the network become less vulnerable when referring to cyberattacks. After several years of technological development in this area, different distributed ledger technologies are available. This article presents Blockchain and Tangle technologies along with their main characteristics, in order to make an extended comparison of their approaches. In addition to this, the paper contains experimentation details and results for each technology presented.**

***Keywords—Distributed Ledger Technology, virtual transactions, cyberattacks, Blockchain, Tangle.***

## I. INTRODUCTION

A distributed ledger is basically a database composed from certain number of nodes or devices. Each of these components has a copy of the ledger, and each copy is updated individually. Modifications of the ledger are recorded by the nodes, which vote on every single update in order to agree upon a conclusion. The eventual update of the ledger depends on the final agreement of its nodes, which also save the latest version of the ledger.

Distributed ledgers propose a variety of advantages to government and other public/private organisations, as they can be distributed in a precisely controlled fashion. Changes by any participant with the necessary permission to modify the ledger are immediately reflected in all copies of the ledger, and, on the opposite side, they can be robust in rejecting changes by unauthorized parties, making the corruption of the ledger extremely difficult. This makes them suitable for avoiding the "single point of trust" problem.

The key underpinning concepts that characterize DLT [1] systems can be seen as being the following: distributed ledger, consensus algorithms, cryptography and smart contracts.

The ledger is a data structure consisting of an ordered list of transactions. Examples range from monetary transactions to goods exchanged between known parties, and, more general, to any exchange of data. The distributed ledger is basically a replicated data-structure which can only be appended to. A system that supports distributed ledgers is characterized by its target applications (most popular being crypto-currencies, digital assets in general and general user-defined computations or smart contracts), by the number of ledgers and by the ledger ownership.

Since the ledger is replicated, the updates to the ledger have to be agreed to by all parties. This might occur between trusted parties but also between nodes that do not trust each other, or both. There is vast literature on consensus algorithms and they can be classified from purely computation-based protocols (e.g. Bitcoin's Proof-of-Work - PoW) to purely communication-based protocols (PBFT implemented in earlier versions of Hyperledger). In between them there are hybrid protocols that aim to improve the mentioned protocol types, a well-known example being Proof-of-Elapsed-Time (PoET) which replaces PoW with protocols based on trusted hardware (e.g. Intel SGX). Other examples include Proof-of-Authority (PoA), Stellar or Ripple. that are used in private blockchains.

Integrity in the ledgers refers to the ability to detect tampering in the ledger data. This is very important in open distributed ledgers where there is no pre-established trust. Usually there are two levels of protection.

For instance, in Bitcoin blockchain, global states are protected by a hash tree whose root hash is stored in a block. Then the block history is protected by linking the blocks through a chain of cryptographic hash pointers (block $n$+1 contains the hash of block $n$), therefore any modification in block $n$ immediately invalidating all subsequent blocks.

Smart Contracts refer to the computation executed when performing a transaction. Smart Contract execution depends on the input, output and states affected and is agreed on by every node in the network. There are smart contracts that have a finite set of opcodes from where users can write scripts (Bitcoin an example), while on the other hand, there are smart contracts that can specify arbitrary computations (e.g. Ethereum) called also Turing complete code. Among them, there are smart contract systems that enable more than the finite set of opcodes but do not accept Turing-completeness. Examples are Kadena [2] and BigchainDB [3].

The paper is organized as follows. Section 2 presents applications of the most popular distributed ledger technology, namely Blockchain, while Section 3 analyzes a more recent distributed ledger, named Tangle, based on the concept of distributed acyclic graph (DAG). Section 4 provides some experimental results of the two technologies, while Section 5 presents the conclusions and envisions future work.

## II. Applications of Blockchain Technology

Blockchain technology, which has emerged in the recent years, still represents an unsettling entity. The economy and business processes started adapting to a new paradigm and will be governed by smart contracts, cryptographic coins and decentralized applications. A blockchain can actually be considered a dynamic list of records, which can only grow. Other modifications such as deleting previously records are impossible.

Blockchain technology allows the digital information to be distributed. Information is not stored in a single location, making the records easy to be verified. Moreover, blockchain is not controlled by one entity and does not have a point where something can fail, making this technology safe and robust.

Blockchain merges transactions into blocks that are attached to each other in a chain and then allocated to all the nodes in the network. For example, when two entities are about to exchange a certain digital currency, they have to launch a transaction. It is loaded together with other transactions that have been initiated into a block. The new block is then included in the network formed by all of the computers in the chain. In order to verify and evaluate the initiated transaction, the network components (or miners) execute mathematical algorithms to state if the transaction is valid. This means that at least 51% of the involved computers agree that the transaction is accurate. Another important step is assigning a cryptographic hash to each block of valid transactions, which also contains a reference to the previous block in the chain. This procedure helps creating a chain of records that is very hard to distort. Finally, the transaction is considered successful and complete after the unit of value is transferred between participants.

The biggest advantage of the blockchain is that you have your wallet always with you, not at the bank or somewhere else. Some of the coins have instant transactions as well as zero fees. Some more advantages of the blockchain are that the data isn't centralised, the transactions can't be modified or manipulated because those are always verified by a massive group of miners.

Blockchain also provides a turning point in the smart energy domain introducing transactions mechanisms which divide the trading process in two stages, namely the call auction stage and the continues auction stage [4].

However, blockchain has got also a dark side, e.g. one would be able to make illegal payments due to the anonymous nature of the payment process using these private coins.

The blockchain technology has many utilities in the IoT (Internet-of-Things) domain [5]. Any material object is only a "thing" until it is connected to a computer network. Then, it becomes more than just an object. For example, a printer can automatically order cartridges when it runs low. Or a coffee machine that can be programmed to make coffee when your alarm clock goes off.

Other applications can be the supply chain sensors. Those are giving companies end-to-end visibility of their supply chain by providing data on the location and condition of the supplies as they are transported around the globe.

Furthermore, smart appliances could be another area where blockchain could prove to be useful. A smart appliance is a device connected to the internet that gives you more information and control than before

## III. Applications of Tangle Technology

In order to analyze the Tangle [6] technology, the concept of the directed acyclic graph is introduced. This type of graph is represented by a collection of squares that are connected to each other through arrows, having the same direction.

The Tangle is essentially a directed acyclic graph that can hold transactions. When a new transaction appears in the Tangle, it needs to approve two other transactions. Transactions that are not allowed yet are called tips. It can be implemented a strategy that will randomly choose between tips that are available. The first transaction is called the genesis.

Tangle can be easily used in everyday situations. Microtransactions are now possible as this system can adapt to many situations, making almost all transactions cheap and quick.

Bank Transfers can also be done using Tangle. This way, expensive transfers can be done without wasting time. The Tangle is directly linked to the IoT field as it facilitates machine to machine transactions. One problem that can occur is caused by several divergences as transactions cannot be shared all at once.

Tangle functions based on the IOTA Reference Implementation (IRI), a Java written software which connects the user of a Node to other neighbors within a peer-to-peer network. By running a Node within the Tangle, decentralization is encouraged, and also no third-party node is necessary to further access this ledger.

There are three types of nodes which can be created:

- Full node, a running IRI, being accessed on the user's machine. This node requires to get the neighbors nodes through a static IP, so it can perform;
- Light node, a local GUI which accesses a full node in other environment with the user's seed;
- Headless node, a full node running locally, having the capacity to open more than just one seed simultaneously.

A seed basically represents the user's IOTA account, the password. In IOTA terminology, there is also the receive ID behaving like a private key and allowing transactions between involved parties.

## IV. Experimental results

In this section, the results of the experiments conducted on Blockchain and Tangle technologies are presented.

### *A. Blockchain - Truffle, EOS*

Truffle is a testing environment for Ethereum. The platform represents an educational approach for understanding the basics of Ethereum technology. It offers the possibility of using and testing smart contracts by running JavaScript and Solidity.

In order to experiment Truffle commands, the user has to create new projects using Truffle Boxes [7], which are

different project patterns, as presented in Fig.1. Thus, the user can observe the items of the project template.

```
carmen@ub:~/truffle/metacoin$ truffle unbox metacoin
Downloading...
Unpacking...
Setting up...
Unbox successful. Sweet!

Commands:

  Compile contracts: truffle compile
  Migrate contracts: truffle migrate
  Test contracts:    truffle test
carmen@ub:~/truffle/metacoin$ ls
contracts  migrations  test  truffle-config.js  truffle.js
carmen@ub:~/truffle/metacoin$
```

Fig. 1. Unboxing a Truffle project template

Next, the Solidity test has to be ran on a terminal:

```
truffle test ./test/TestMetacoin.sol
```

The tests are ran against the contract, with additional descriptions of their purpose:

```
TestMetacoin
    √testInitialBalanceUsingDeployedContract
(118ms)
    √testInitialBalanceWithNewMetaCoin
(139ms)
  2 passing (1s)
```

Also, JavaScript tests are ran in a similar way, using:

```
truffle test ./test/metacoin.js
```

In order to have the smart contracts [8] deployed, the user has to be connected to a blockchain. The interaction is done using Truffle Develop, which displays multiple accounts together with their private keys. An alternative to Truffle Develop is using Ganache, a desktop application for launching the blockchain. This method requires an additional step, which is editing the configuration file to point to Ganache. The output can be seen in Fig. 2.

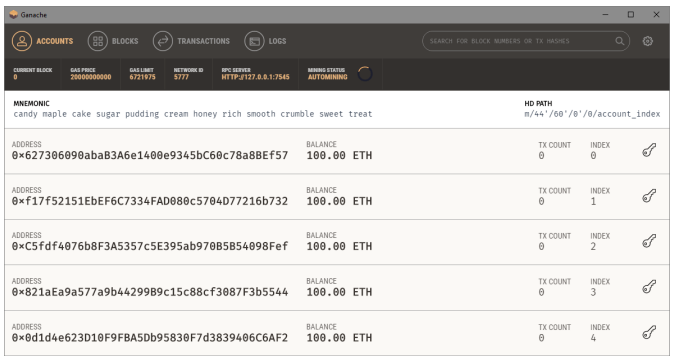


Fig. 2. Launching Ganache

The user is able to see transactions that have been processed, as well to interact with the contract and to do transfers between different accounts in order to experiment multiple scenarios [9].

EOSIO is a framework that enables applications to run decentralized within the blockchain architecture. Furthermore, it cannot be traced using crypto-mining fingerprinting method [10].

This software provides accounts, authentication, databases, asynchronous communication and applications scheduling on multiple Central Processing Units (CPUs) or clusters [11]. The resulted technology can reach millions of transactions per second, eliminating utilization tools and ensuring easy maintenance of decentralized applications in the context of blockchain administration type. EOSIO includes a set of programs, the main ones being:

- nodeos (node + EOS = nodeos): the main EOSIO node daemon can be configured using plug-ins to run a node;
- cleos (CLI + eos = cleos): a command line interface to interact with blockchain site and to manage "wallets";
- keosd (key + eos = keosd): a component that keeps the EOS secret keys in the “wallets”.

The experimentation includes creating a smart contract using the EOSIO. For doing this, Docker, a containerization solution, was firstly installed. Then, after the image was pulled, it was ran, and the cleos command gave a positive result. Then, a Docker network was created, and the server’s software was initiated, while the wallet of this server was ran. After that, the server’s functionality was checked, the result being displayed in Fig. 3., where the expected result is showed on the left side, while our result, on the right. They are the same, meaning a successful connection.

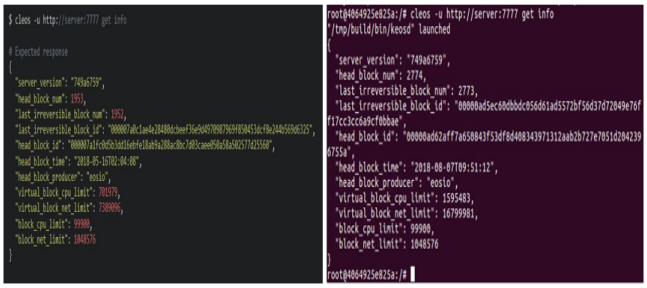


Fig. 3. Server functionalty: expected result vs practical result

## B. *Tangle - IOTA*

Using CarrIOTA, downloaded on a Windows 10 operating system, new transactions can be created. CarrIOTA represents a wallet that transfers and stores IOTA. It also includes the feature of giving different permissions to other entities like business, friends, family, on accessing the user’s wallet. In Fig. 4, CarriIOTA Bolero application is used, since it allows launching an IOTA full node easier, with no complex node setup as in the IOTA wallet case. CarrIOTA has a feature which enables automatic management of neighbors when preparing a full node setup, helping the network grow faster and improving IOTA’s performance.

In our testing, a seed was successfully generated, and new neighbors were added to this newly created node. Some port forwarding was also needed to be done in the Network Address Translation (NAT) Router. Then, the node was functional, as observing in Fig. 4 where a node having 3 neighbors runs.

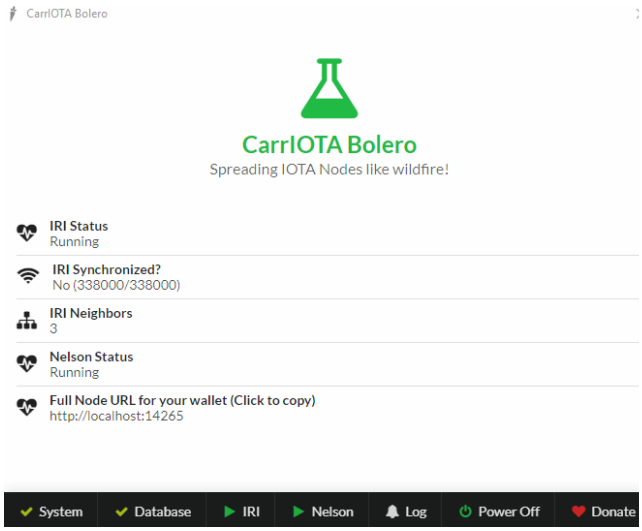


Fig. 4. Functioning Node

The answer of accessing the node is presented in Fig. 5 where the Application's Programming Interface (API's) response is given. To receive a different answer a different URL with commands should be accessed.


Fig. 5. Node Access

## V. CONCLUSIONS

Distributed Ledger Technology describes a method that uses a complex algorithms for keeping records. Cyberattacks are one of the most important problems that can occur when recordings are being accessed. Therefore, nodes are used while creating the network. This article compared Blockchain and Tangle in terms of main characteristics and results of the experiments.

Blockchain allows a procedure to be created as a chain of records which cannot be altered. On the other hand, Tangle brings into attention the concept of acrylic graph that offers some advantages in terms of security since every new transaction needs to allow other two.

In this paper there were presented results of experiments using Blockchain and Tangle technologies. Truffle is an environment that allows the user to connect to a blockchain. In addition to this, for Tangle, the CarrIOTA Bolero was installed on Windows in order to create new transactions. As future work we envision deploying a smart contract for distributed trade engine using different DLTs.

## ACKNOWLEDGMENT

This paper was partially supported by UEFISCDI Romania and MCI through projects ODSI, PARFAIT and ToR-SIM, and funded in part by European Union's Horizon 2020 research and innovation program under grant agreements No. 777996 (SealedGRID project) and No. 787002 (SAFECARE project).

## REFERENCES

[1] Mills, D.C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A.I., Brezinski, T., Fahy, L., Liao, K., Kargenian, V. and Ellithorpe, M., "Distributed ledger technology in payments, clearing, and settlement," 2016.

[2] Samman G., "Kadena: The First Real Private Blockchain," 2016 https://medium.com/@sammantic/kadena-the-first-real-private-blockchain-add7fd76bc22.

[3] McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., and Granzotto, A., "BigchainDB: a scalable blockchain database," white paper, BigChainDB, 2016.

[4] Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M., "Blockchain based decentralized management of demand response programs in smart energy grids," Sensors, 18(1), 162, 2018.

[5] Zhang, Y., & Wen, J., "The IoT electric business model: Using blockchain technology for the internet of things.", Peer-to-Peer Networking and Applications, 10(4), 983-994, 2017.

[6] Popov, S., "The tangle," cit. on, 131, 2016.

[7]"Truffle Boxes," https://truffleframework.com/boxes

[8]"Sweet Tools For Smart Contracts," https://truffleframework.com

[9]"Building & testing a frontend app with Truffle",https://truffleframework.com/tutorials/building-testing-frontend-app-truffle-3

[10] Draghicescu, D., Caranica D., Vulpe A., and Fratu, O. "Crypto-Mining Application Fingerprinting Method." In IEEE 2018 International Conference on Communications (COMM), pp. 543-546, 2018.

[11] Stankovski, V., Salado, G.F., Suciu, G., Ulisses, A., and Cees de Laat. "Developing, Provisioning and Controlling Time Critical Applications in Cloud." In Advances in Service-Oriented and Cloud Computing: Workshops of ESOCC 2017, Revised Selected Papers, vol. 824, p. 169. Springer, 2018.