Future Generation Computer Systems 112 (2020) 307–319

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# Iota Tangle: A cryptocurrency to communicate Internet-of-Things data

Wellington Fernandes Silvano *, Roderval Marcelino

*Applied Research Laboratory, Federal University of Santa Catarina, Araranguá, Santa Catarina, Brazil*

ARTICLE INFO

*Article history:*
Received 4 November 2019
Received in revised form 21 May 2020
Accepted 28 May 2020
Available online 1 June 2020

*Keywords:*
Iota Tangle
IoT
DLT
Iota
Distributed computing

ABSTRACT

The emergence of distributed ledger technologies (DLT) and design limitations of Blockchain systems for some types of applications led to the development of cryptocurrency alternatives for various purposes. Iota is a cryptocurrency with a new architecture called Tangle, which promises high scalability, no fees, and near-instant transfers, focused on the Internet-of-Things (IoT) solutions. This paper aims to present a systematic community's visions of this new technology and to provide minimum background to understand the Iota Tangle and ecosystem generated by this distributed Ledger. The first parts of this article describe the ecosystem behind Iota, theoretical mathematical foundation, and its challenges and solutions for implementation. In the second part, we presented systematic research about Iota Tangle in academic databases: IEEE, ScienceDirect, Scopus, and Research Gate. We select the articles those of high impact which can be filtered with the H5-index indicator. This criterion aims to guarantee that the papers analyzed underwent a careful selection process, evaluated by peers. The methodology used helped have a global vision of Iota, including that this innovation is not only understood as a cryptocurrency but can be considered as a "distributed communication protocol", absence of fees, low latency, and low computational cost for sending transactions. However, there exist several challenges in the vanguard of development of this ledger. It could also be identified that this technology enables many possibilities, however, it is fundamental to understand the potentials and limitations of this ecosystem to generate the best use cases.



## 1. Introduction

Iota is a cryptocurrency that promises high scalability, near-instant transfers at zero cost, focused on Internet of things solutions [1]. The Internet of Things (IoT) is a large global information system composed of massive heterogeneous and decentralized devices that can be identified, sensed, and processed based on standardized and interoperable communication protocols [2,3]. The currents centralized systems are unlikely to scale enough to support millions of microtransactions per second efficiently and enable greater automation in dynamic factory processes, automated decision making, and successful negotiation and are vulnerable to many issues of security and privacy; these issues have been limiting the adoption of IoT [4]. In many cases, IoT data are stored on different cloud servers and processed and accessed in a distributed manner. However, cloud services can expose security breaches to the Internet and are susceptible to cyber-attack [5–8]. With so many objects connected, the obstacles appear, it is not easy to monitor with security and enable billions of low-power connected devices to share collected data [9]. Decentralized system can provide privacy and scalability, without relying on a central authority or specific hardware. In this context Distributed Ledger technologies (DLT) can be important facilitators for implementing IoT economy.

The development of the Iota technology is basically related to two factors, namely, the growth of connected devices and the Blockchain. Blockchains were first proposed in 2008 is the technology behind the Bitcoin, can say that Blockchain as a type of Distributed Ledger Technology (DLT), where changes in the ledger are reflected in all computers in the network [10]. More precisely, through a consensus mechanism the information is replicated and cannot be changed by a user or a group of users [11]. Currently Blockchains have face the challenges of being "decentralized", "secure" and "scalable" at the same time. Blockchain systems can only have, two of the three properties problem is known as the "Scalability Trilemma" [12]. Important design issues in today's Blockchain systems, such as the presence of fees, high processing time, and lack of scalability, do not fit well into a heterogeneous device scenario such as those arising from the new economy that emerged with IoT [13]. Humanity is moving rapidly into the connected future, according to Gartner and Cisco, by 2020 there will be between 25 and 50 billion internet-connected devices worldwide. To allow for machines to participate autonomously in economic life by buying and selling data or resources, it has become relevant to create a system that gains scalability as the

* Corresponding author.
*E-mail addresses:* wellington.fernandes@posgrad.ufsc.br (W.F. Silvano), roderval.marcelino@ufsc.br (R. Marcelino).

https://doi.org/10.1016/j.future.2020.05.047
0167-739X/

number of networked devices increases. Selling data or resources also requires the possibility of sending very small transactions. Cryptocurrencies using Blockchain are unable to resolve these issues, and most of other active cryptocurrencies use this technology. In order to mitigate these issues, Iota created its own DLT, which is called Tangle.

This paper aims to identify the potential and challenges that Iota Tangle technology has, as well as provide the background for understanding the ecosystem, create uses cases and facilitate the follow-up study of this new and emerging field. The paper is divided into two parts: the first refers to the fundamentals of the Tangle technology and the current state of Iota solution development, presenting current problems and solutions. The second part is a literature review of high impact articles about Iota Tangle published from 2015 to July 2019 in four academic databases: IEEE, ScienceDirect, Scopus, and ResearchGate.

## 2. IOTA Tangle

In 2015, Popov presented the document that characterizes the technology behind Iota and expose its goals. The article named "Tangle" was changed to "The Tangle". It has been revised several times and will be the basis of the concepts presented in this section that underlies the technology. This paper indicates that the Iota project focuses on providing a microtransaction infrastructure for the IoT universe [1,14]. It is a more energy-efficient technology compared to Blockchain, that increases transactions speed and makes possible transactions at no cost.

While systems like Bitcoin and Ethereum use the Blockchain that has sequential blocks, with multiple transactions within a block, a type of directed acyclic graph (DAG) restricted a connection only a single path (the next Block) [4], the Iota use one other type of DAG less restricted named the Tangle [1]. In the Iota Tangle network there are no blocks, each new transaction references the previous two transactions and is not necessary to obtain immediate consensus [6,8]. Whenever a participant wants to add a new transaction to Tangle he must approve any two transactions previously attached. When a new transaction references two previous transactions, it works as a statement of "I certify that these transactions, which have not been proven before, as well as all their predecessors, and their success is tied to my success" [15]. The consensus is related to the number of transactions that approved a certain transaction. The transaction that receives additional approvals has a higher level of confidence [1]. Since network users themselves who validate the transactions, no miners necessary [15,16] (computers responsible for validating the transactions and obtain consensus, in case the Blockchain), all participants in the network play the same role, all participants issue and validate transactions and are equally responsible for the consensus. Therefore the cost of a transaction involves only the computational cost of validating two other transactions.

At the core of the logic of distributed cryptographic currencies lies the problem of surmounting the double-spending problem, which poses accounting and accountability challenges that useful cryptocurrencies have sought to overcome [17]. The double-spending problem is a potential failure in a cryptocurrency whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified. The double-spending problem raises questions about the protection of a digital currency in the same way that traditional currencies are to be protected from fraud or counterfeit, with subjacent accountability issues in the protection of a digital information. Analogously to traditional counterfeit money, the double-spending problem exerts inflationary pressure by creating a new supply of fraudulent currency that has not previously existed, thereby debasing the digital currency's value relative to the general price level. In turn, this compromises the governance and accountability associated with user trust in the currency [17,18].

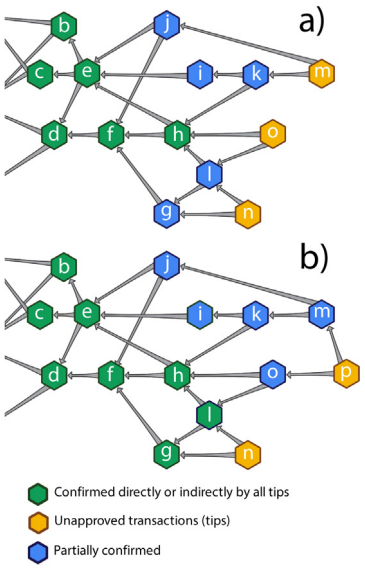



**Fig. 1.** Graph illustrating a part of Tangle. (a) State at any time t (b) State t + 1, with a new transaction p.

### 2.1. The Tangle

To understand the consensus and how Tangle addressed the double-spending problem, it is essential to know deeper the Tangle. The network in the Tangle graph is composed of nodes that are entities that issue and validate transactions in the Tangle, and each node also represent a transaction [1]. The process of attaching a transaction to Tangle goes as follows: (1) a node chooses two other transactions to approve, according to a tip selection algorithm Markov Chain Monte Carlo (MCMC); (2) the node checks if the two transactions are, or not, in conflict and disapprove conflicting transactions (double-spending); (3) in sequence, for node to emit a valid transaction, it must solve a sort of proof-of-work (PoW), this is achieved finding a nonce, such that its hash is concatenated with some data from the approved transaction [1], this computational effort is a much lighter version than the one performed by the Blockchain [19]; (4) after that, the user sends its transaction to the network, and it becomes a tip (unapproved transaction); (5) the tip waits for confirmation through direct or indirect approval until its accumulated weight reaches the predefined threshold.

Tangle transactions occur asynchronously, and the nodes usually do not see the set of all transactions. In Fig. 1(a), the node "m" does not know the history of the branches that contain the transactions "o", "n", "l", and "g", but it still validated transactions "k" and "j". Being asynchronous implies the possibility of existing conflicting transactions; it would be possible for the transaction "k" to conflict with "g" because they were not both validated together.

When transaction "p" validates "m" and "o" in Fig. 1(b), each transaction linked to them is verified, directly or indirectly, including "k" and "g"; at this time the conflict is identified and it would be needed to choose a branch, in case there is a conflict. According to Popov [1], Divya and Biradar [14] and Gal [20], the main rule used to decide between conflicting transactions is to execute the tip selection algorithm many times, identifying which of the two transactions is more likely to be indirectly approved by the chosen tip; it is chosen the branch with higher probability, while the other is abandoned.

The tip selection algorithm MCMC is useful to choose transactions for validation and has protagonism in conflict resolution,

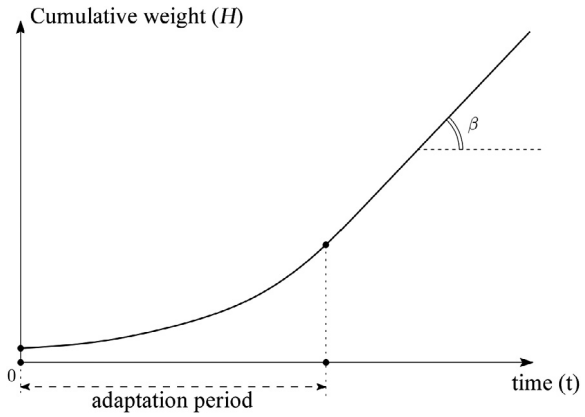



**Fig. 2.** Plot of cumulative weight vs. time for the high load regime [1].

hence is necessary to prioritize a tangle branch using a metric, in this case, the weight of the transactions. The consensus on Tangle is related to the accumulated weight. For Popov [1], the weight is proportional to the amount of work invested on validating the transaction; on the current implementation, the weight is proportional to $3^n$ for a $n$ positive integer [1]. The central idea is that a transaction with more weight is more important. The "accumulated weight" is defined as the weight of the transaction plus the sum of the weight of all transactions that directly or indirectly approve it [20]. That means that the chain with more accumulated weight tends to grow, while other branches tend to become isolated, with low certainty probability. Another consequence is that "tips" tend to be chosen for validation.

The consensus is related to the probability that the branch of a transaction cannot be abandoned. For this reason, depending on the level of importance of a transaction, it can be understood that it will be accepted as valid when its branch is chosen a specific percentage x of times, by the tip selection algorithm. A way to study the adoption of a transaction by the network precisely is using accumulated weight analysis. In a specific moment on, the accumulated weight of a transaction should grow proportionally to the number of new tips, because they would be linked to a particular transaction, directly or indirectly, increasing its weight. Popov [1] studied this point, synthesized at Eq. (1), the accumulated weight $H(t)$ of a transaction as a function of the time $h$, where $h$ is the average time that a device needs to perform calculations that are required to issue a transaction and time $t$.

$$H(t) \approx 2exp(0.352t/h) \tag{1}$$

Fig. 2 shows a plot for expression (1), which indicates the typical behavior of the accumulated weight of a transaction. It expresses the "adaptation period" of a transaction because when it reaches linear growth, it means that new tips are indirectly linked to it, having, therefore, in other words, a high probability that the transaction will not be abandoned. It is interesting to comprehend that, after an adoption period (in Fig. 2), the transaction will not be abandoned, and we can trust that transaction is valid because the new "tips" indirectly approve this particular transaction. In the Tangle, its no need to wait for this adaptation period, always transaction enters the network. The confidence level depends on the situation; for example, microtransactions can demand a 50% confidence level, while the exchange of a large number of tokens may require more than 99%. In other words, when almost all tips participate in that part of the chain [20].

Popov [1] the use that the MCMC algorithm for tip selection its based on the fact that the main Tangle chain has more power of accumulated hashing (more weight) than possible attackers. The article also makes clear that the accumulated weight must not be the only relevant parameter, but it should be followed by a factor $\alpha$ that does not allow the largest tip to be always selected [15]. Current solutions have searched for other options beyond the main chain hashing power [21].

### 2.2. The implementation

The Tangle implementation faces a series of new challenges, among them the level of network maturity, the number of indirect confirmations a transaction must perform, the size of Full nodes, and the privacy of transacted data. Problems and related solutions are presented in this session. The information presented is essential for a good understanding of the network.

#### 2.2.1. Coordinator and coordicide

To allow the network to grow to a more mature state, Iota relies on a Coordinator to provide safety against the risk of dishonest actors that may attack the network. The current consensus definition of Iota demands that a confirmed transaction should be referenced (directly or indirectly) by a transaction signed by the Coordinator known as Milestone [21], which is emitted every two minutes; all transactions approved by it are considered as 100% confidence, immediately [20]. The Coordinator also ends up facilitating the checks for double-spending. As with Blockchain, the scalability trilemma stands here, and Iota increased centralization in favor of scalability and safety with the use of the Coordinator. This is not well regarded for a cryptocurrency because, it allows Iota Foundation to choose which transactions get priority, to freeze funds, ignore transactions, and is a central point of attack. If the Coordinator stops working, network confirmations will stop [21]. Recently a paper entitled "The coordinate", published in May 2019, detailed how the Coordinator in the Tangle network may be detached. The authors detail new safety schemes for the network in the absence of the Coordinator and promise faster transactions, ordered and reliable timestamps, a new rate control algorithm, which, in theory, prevents invaders from overloading the network, among other things. In case of success, it is essential to point out that the information in this paper still holds true. New components have been predicted, but the fundamental design characteristics from Tangle remain [21].

#### 2.2.2. Snapshotting

Since a large amount of data is being exchanged, the network can grow too big, especially for allowing zero value or data-only transactions. When snapshotting, only the balances remain (addresses with an account balance $> 0$), everything else is deleted. The instant capture is like Blockchain removal, except snapshotting has the significant advantage of grouping various transactions the same address in a register, which requires fewer storage [22]. In the past, the Iota Foundation made "Global Snapshots" on irregular intervals. Today there are local snapshots which replace the global snapshots. Local snapshots of the Tangle are taken independently by Full nodes, manually or fully automatically.

#### 2.2.3. Permanodes

Some applications need to keep the entire transaction history stored, for example, a transparent audit. This is the role of Permanodes. A Permanode stores the entire Tangle data and history in a safe, permanent way [22]. Another alternative would be to keep a Full node without snapshotting under control of the person or organization that needs that data. This feature is under development.

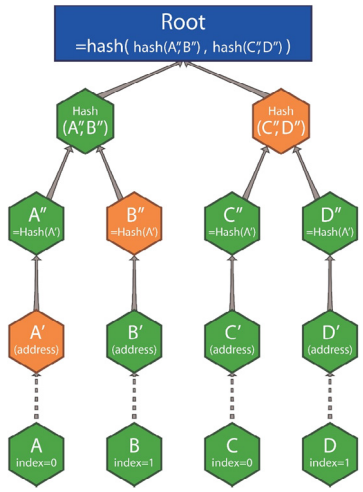



**Fig. 3.** Example of a Merkle Hash Tree with 4 leaves.

### 2.2.4. Masked Authenticated Messaging (MAM)

One frequent IoT application is the transmission of sensor data. Iota allows transactions without the exchange of tokens; therefore, an address can be used to store measured data. However, since transactions are public, how to stop an invader from falsifying measuring data or interfering with spams? Would it be possible to control the data access from other users? Masked Authenticated Messaging (MAM) was developed to solve this type of issue.

MAM acts as a data communication protocol, cryptographing, and authenticating data flows; it is a module base on the Iota protocol that provides functions to send and read message flows using Tangle. Cryptography and system authentication aims to ensure that messages will not be altered and come from a specific sender. With MAM, linked message flow is created from messages, sending each message to a new address in the form of Tangle transactions. Each message is linked to the subsequent message [23], and each transaction n has a pointer to the transaction n + 1. However, they do not know the location of the transaction n−1.

MAM uses Merkle signature scheme (MSS). This scheme is based in Merkle Hash Tree (MHT) combined with One-Time Signatures (OTS) [24]. The Merkle signature scheme (MSS) is used because it is assumed to resist quantum computer attacks and because of their short signature generation and verification times as well as their strong security guarantees. MSS comes with a standard security model proof and outperforms RSA in many aspects regarding runtimes [25]. MSS permits a method to use one public verification key to verify multiple OTS. Each message (A, B, C, D in Fig. 3) is signed with one OTS scheme, and is one leaf of MHT, presented as A′, B′, C′, D′ in Fig. 3. By applying the hash functions to shorten the addresses, the root of the Merkle tree can be obtained [26]. Each tree can produce the same number of messages as the number of leaves of MHT. Each leaf also contains the address of the next tree, that is, a pointer to the next message (Future direction of the channel) [26,27].

The MAM has three different operation modes: public, private, and restricted. On the public mode, the root of MSS is the address of a transaction in the Tangle; on the private mode, the address is the hash of the root, $H(root)$, where $H()$ is a unidirectional cryptographic hash function; on the restricted mode, the payload of each message is additionally encrypted and can only be decrypted with a key [27]. If an opponent encounters a MAM transaction in private mode, it will not be capable of decrypting the message payload using the channel ID because it is the hash of the channel key, not the key. It is very difficult for an adversary to reproduce the channel key from only the channel ID. On the restricted mode, the recipient needs to use the root to calculate the transaction address and search for the masked messages. To decrypt the masked message its necessary to use the root and a sideKey [24].

It is important to emphasize that messages send to MAM are typical transactions, with zero value, in other words, are part of the Tangle, such as others transactions. The difference is how messages are linked, each other, in the Tangle. These messages are part of the distributed ledger, and contribute to network safety, increasing the total hashing power, and benefiting from the network data integrity properties, while other transactions continue to reference them indirectly [23,24].

MAM works as a radio station, where only those with the right frequency can hear; with MAM, only those with the correct channel address have access to data [22,23]. Since the transactions are in Tangle are available to everyone, if it is necessary to protect the payload and the pointer to the next transactions, this can be realized using MAM on private or restricted mode. If one needs to share the data with only a few individuals or machines and it is also necessary to revoke access at any time, it is essential to use the restricted mode, as the message will be additionally encrypted. In this case, an additional key is required to decrypt the message.

### 2.2.5. Seeds, public key and private key

In the Iota Tangle network, a “seed” acts as a password that grants access to the user account. The seed must be randomly generated and consists of 81 trytes. Moreover, in Iota, there are the concepts of private and public key. Private keys are calculated by hashing the seed concatenated with the address index, where the index can be any positive integer [28]. Public keys are addresses, and they are calculated by hashing their associated private keys. An address contains tokens and can be used as input to a transaction (the token is spent) or output to a transaction (the address is given a token). Funds from all addresses (public keys) are summed to calculate a user’s account balance [29].

The Iota protocol uses Winternitz One-Time Signature (WOTS), a cryptographic Hash-based signatures [29] is quite promising resistant to quantum computers [30] and is faster than elliptic curve cryptography [31].

Since the Iota protocol uses WOTS, the security of a particular address decreases as the number of times it is used to send funds increases [29]. If the user often reuses an address (the same public key), it is easy for others to analyze a person’s spending. Therefore, an analysis of a transaction data can identify transaction history and balance such as what happens with Bitcoin and other cryptocurrencies [16]. It is preferable to use a new address (public key) to receive payments. Iota has a dedicated mixing service to improve anonymity, Sarfraz et al. [16] have also proposed a solution.

This issue arises because each time tokens are sent from an address, the issuer must approve moving tokens from his address. This is achieved by using a unique private key to on the transaction. However, each time signature is created, it reveals 50% of the private key associated with the address that released the tokens [29]. If the user reuses an address to sign multiple outgoing transactions, it results in the exposure of a large fraction of the corresponding private key, which makes it easy for an adversary to forge the signature to steal funds.

The current Iota protocol mitigates address already used issues by using libraries that scan Tangle transactions for worn addresses. If an address has already been used, then it cannot receive tokens. However, there are snapshots, which remove the transaction history. Thus, a spent address can receive tokens

after a snapshot, because the transaction history is cleared, and addresses that no longer contain balance are forgotten, making it impossible to scan old transactions. Solutions have been proposed to resolve this issue, for example Shafeeq et al. [29].

## 3. State of art

Four academic databases were analyzed (IEEE, ScienceDirect, Research Gate, and Scopus) from year 2015 to July 15 of 2019. The year of 2015 was the year "The Tangle" was published, defining the concepts behind Iota, seeking to draw the scientific community's attention to the new vision towards technology.

### 3.1. Article selection methodology

For article selection, the descriptors used are "Iota" and "Tangle" in the databases mentioned, picking those with at least four paragraphs about Iota/Tangle, excluding superficial mentions of the technology and unrelated subjects. Although it is difficult to find articles, because Iota is a term used in many areas, by combining "Iota" with "Tangle" in keywords, summaries or text, it was possible to filter much of the results.

The H5-index of each periodical was measured. The H5-index refers to the largest number h, such that h articles published have at least h citations each in the last five years [32]. The H-index has been studied by the scientific community and has been regarded as relevant because it is simple to measure and considers both the quantity and impact of publications. A periodical cannot have a high h-index without publishing a considerable number of articles. The benefits periodicals that have a continuous flow of articles with many citations [32].

We identified articles published in places with an H5-index greater than 20, according to Google Scholar Citations, i.e., the number of articles published in the journal or conference, over the last five years, that have at least 20 articles with 20 citations. This criterion aims to guarantee that the papers analyzed underwent a careful selection process, conducted by peers. From this criterion, 19 papers were identified for analysis; they will not be analyzed 22 because they were published or presented in places with H5-index lower than 20, mostly conferences (16), as well as articles not yet peer-reviewed (4) and two book chapters.

We identified the Impact Factor of each article to validate the quality of the selection. After papers exploratory analysis, it was seen that these articles were aimed to some applications: automotive, machine-to-machine (M2M), smart cities, e-health, and internet of things (IoT). The data of this exploratory analysis is presented in Table 1, order by H5-index. The table contains the year, title, and venue for publication, as well as the characteristics, analyzed each article: application focus and the Impact factor.

### 3.2. Papers

Most of the articles analyzed, investigate Iota with a focus on some applications, while only four articles analyze the technology for any type of application (grouped in "other"). By Grouping the papers in this way makes it easier to understand the motivations, positive, and negative aspects that the authors identify in Iota Tangle technology.

#### 3.2.1. Internet of things (IoT)

Four articles principally focused on IoT applications (Fig. 4), among these, three bibliographic reviews that present and compare different types of DLTs as having the potential to facilitate the adoption of IoT systems and a proof of concept that uses Blockchain and Tangle together.

For Wang et al. [5], Makhdoom et al. [6], Yeow et al. [7] and Jiang et al. [8], current IoT devices are vulnerable to many issues

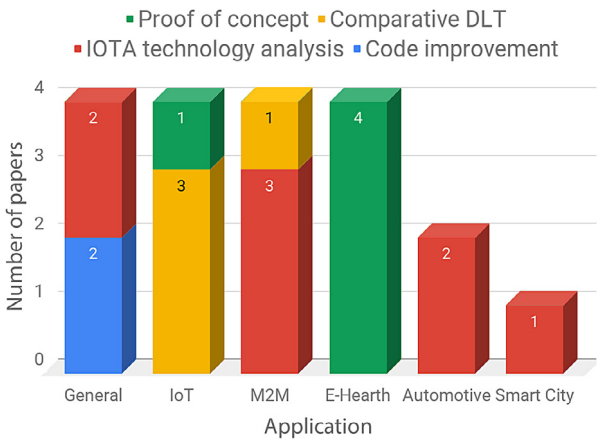



**Fig. 4.** Number of applications per approach type.

of security and privacy; these issues are limiting the adoption seriously. In many cases, IoT data are stored on different cloud servers and processed and accessed in a distributed manner. However, cloud services can open insecurity breaches to the Internet and are susceptible to cyber-attacks. Wang and his collaborators elicit problems presented in the literature, such as SQL injection, data tampering, and vulnerabilities to single node failures. For the authors, cloud services cannot guarantee data availability and integrity IoT [5]. For Yeow et al. [7] in scenarios that require low latency, devices centered in cloud are not feasible, due to staying away from the center of the network.

DLTs have, in their origin, the proposal to be distributed, incorruptible and inviolable; these characteristics motivated Wang et al. [5], Makhdoom et al. [6], Yeow et al. [7] and Jiang et al. [8] conducting his Blockchain and/or Tangle research to solve security and privacy issues for IoT. Despite the potential of DLTs, there are critical challenges in enabling devices to generate, exchange, and consume data with minimal human intervention. There are challenges inherent in the characteristics of IoT devices and those related to technology. IoT devices, such as sensors and disposable items, have limited computing power, low communication bandwidth, unpredictable network delays, varied network structure, and wide device diversity [5]. A traditional Blockchain has issues such as lack of scalability, high transaction costs [8], commit latency, large storage, computationally expensive work proof, and power requirements [6] that need be investigated to understand potentials and limitations.

The authors highlight the DAG architecture offers a great potential for IoT, especially in light of the exponential increase in data volume. The blockless structure, composed of transactions, brings speed to transactions, as transactions will have at least partial peer confirmations rapidly, Yeow et al. [7] use the term "almost instantaneously". Yet, there are no classic issues like block size limits, which causes typical delays from traditional Blockchain [7,8]. By allowing transactions to occur in parallel, Iota becomes scales as the number of transactions on the network increases [6,7]. Yeow et al. [7] credit this fact to the immediate waiver of global consensus. A comparison between DLTs by Wang et al. [5] highlights Hyperledger-Fabric and Iota, with Iota being the only public DLT with high transaction rates per second.

Yeow et al. [7], Makhdoom et al. [6], Jiang et al. [8] and Wang et al. [5], and their collaborators highlight the Iota feature for micro or nano payments due to the absence of fees. In addition to monetary transactions, Tangle also allows devices to send messages (as already mentioned), making it a perfect solution for IoT devices to communicate with each other and/or the outside

**Table 1**
Articles with H5-index equal or greater than 20 with at least 4 paragraphs describing Iota Tangle technology.

| H5-index | Year | Title | Venue | Impact factor | Application |
|---|---|---|---|---|---|
| 95 | 2019 | A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management | Sensors | 3.031 | IoT |
| 89 | 2018 | Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance | IEEE Access | 4.098 | Smart City |
| 89 | 2017 | Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues | IEEE Access | 4.098 | IoT |
| 88 | 2019 | Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies | Journal of Medical Internet Research | 4.945 | E-Health |
| 73 | 2019 | Privacy aware decentralized access control system | Future Generation Computer Systems | 5.768 | E-Health |
| 70 | 2019 | Blockchain's adoption in IoT: The challenges, and a way forward | Journal of Network and Computer Applications | 5.273 | IoT |
| 59 | 2019 | On Iota as a potential enabler for an M2M economy in manufacturing | Procedia CIRP | 2.15 | M2M |
| 58 | 2019 | Activity-aware essential tremor evaluation using deep learning method based on acceleration data | Parkinsonism | 4.36 | E-Health |
| 58 | 2019 | Equilibria in the Tangle | Computers & Industrial Engineering | 3.518 | Other |
| 57 | 2019 | Privacy aware Iota ledger: Decentralized mixing and unlinkable Iota transactions | Computer Networks | 3.03 | Other |
| 57[a] | 2018 | How to Break Iota Heart by Replaying? | IEEE Globecom Workshops | NaN | Other |
| 57[a] | 2018 | An Iota Based Distributed Sensor Node System | IEEE Globecom Workshops | NaN | M2M |
| 57[a] | 2018 | Iota Feasibility and Perspectives for Enabling Vehicular Applications | IEEE Globecom Workshops | NaN | Automotive |
| 49 | 2019 | Survey on Blockchain for Internet of Things | Computer Communications | 2.766 | IoT |
| 44 | 2018 | Iota-VPKI: A DLT-Based and Resource Efficient Vehicular Public Key Infrastructure | IEEE Technology Conference VTC | NaN | Automotive |
| 36 | 2018 | Authenticating Health Activity Data Using Distributed Ledger Technologies | Computational and Structural Biotechnology Journal | 4.72 | E-Health |
| 25 | 2019 | Curbing Address Reuse in the Iota Distributed Ledger: A Cuckoo-Filter-Based Approach | IEEE Transactions on Engineering Management | 1.867 | Other |
| 22 | 2019 | M2M Learning Environment for Electric Applications | IEEE Education Engineering (EDUCON) | NaN | M2M |
| 21 | 2019 | Distributed Ledger Technologies for M2M Communications | International Conference on Information Networking | NaN | M2M |

[a]IEEE Globecom has H5-index of 57 and before the evidence of quality IEEE Globecom Workshop was also included.

world. For Yeow et al. [7], the Iota proposal differs from the TCP/IP protocol for M2M communication, as it guarantees the authenticity and integrity of the message. By sending messages in a distributed ledger, it is possible to verify the authenticity and integrity of the message in addition to the inherent tamper-proof feature [7]. Yeow et al. [7] believe that DAG-based technologies, especially Iota, may be a response to the growing scale of edge-centric IoT (near-device networking), given the need for micropayments and low latency in a decentralized communication and payment infrastructure machine-to-machine (M2M) and people-to-people (P2P).

Since smart contracts at Iota are still a challenge, Yeow et al. [7] highlight the synergy between Iota and a Blockchain, such as Ethereum. Ethereum would be a type of central control station, while Tangle would run on all small devices. According to the authors, this solution would reflect the maximum interoperability in the IoT system — a solution cross-chain similar was developed by Jiang et al. [8].

Among the impediments to Iota being the standard for IoT device communication, the authors Makhdoom et al. [6] and Wang et al. [5] strongly emphasize the lack of smart contracts support in Iota system. Makhdoom et al. [6]. Wang et al. [5] highlight Ethereum as most appropriate platform for many applications with large numbers of IoT devices and inhomogeneous network structures. [5] identify as disadvantages of Ethereum the high computational complexity and limited capacity, however identify advantages such as supporting the Smart Contracts and being a public Blockchain.

Technologies that use DAG, such as Iota, may need a central point of control to coordinate and ensure the security of the network, which is part of the reason that Iota implements the figure of the "Coordinator" [7]. The Coordinator's existence is identified as impeditive to Iota achieving High scalability and decentralization [5,6]. Another important requirement for many IoT systems that share private data from users is data confidentiality. According to Makhdoom et al. [6] only Hyperledger-Fabric provides data confidentiality and also ensures limited privacy of user data by allowing the creation of private channels and data encryption.

According to Makhdoom et al. [6] no exist clarity about the time for approval transaction in the Tangle, for authors is important determined after how long and how many indirect approvals the transaction will be confirmed, because this is an important aspect in the management of IoT services in near real-time, such as payment of toll by smart cars, payment of fuel, rate of parking etc [6]. Since Iota is considered in the testing phase, Makhdoom et al. [6] raise some pertinent questions: Iota be only an efficient IoT micropayment system? Will it also support smart contracts like Blockchains Ethereum and Hyperledger-Fabric? [6].

Jiang et al. [8] developed a proof of concept that is presented as a cross-chain solution, which merges Iota Tangle and Hyperledge Fabric. The solution targets IoT data management. According to the authors, the need for the combined solution is because Iota does not support yet smart contracts and does not have the concept of time series, and therefore has no reliable date and time, but Iota provides high scalability and low computational cost to perform proof of work. Jiang et al. [8] and his collaborators' solution involves new actors in the network, the notaries, who provide timed transaction sequencing, and request consensus for consortium. The notary consists of multiple participants/peers

who do not trust each other using a standard consensus algorithm as proof of work (PoW). The notary is identified and signed by a public key that follows the DLT cryptographic criteria [8]. The authors believe the solution they implement is suitable for managing low-resource IoT devices and that the combination of machines and Blockchains makes these machines economically independent data exchange devices, reduces IoT operating costs, solves to security issues, and protects users privacy [8]. However, the environment was all simulated in software, and has not being deployed to real IoT devices.

*3.2.2. Machine-to-machine communication (M2M)*

There are four articles about communications between machines in distributed systems. Zivic et al. [33] brings reflections and comparisons on the use of DLTs for M2M environments. Other authors conduct a specific analysis of the Iota for M2M applications: from an extension of the conclusions of a proof of concept [4], a didactic application [9], and a sensor node system architecture [34].

Machine-to-machine communication has related the possibility of exchanges between machines without human intervention [4] and may even post-process data locally or remotely for decision-making; Interconnect and share for autonomous data, energy or resources [9]. An economy like this, devices can offer services to each other over the Internet, machines can autonomously share data in "public data markets". This offers new business models based on information products generated from large-scale data exchange. The savings generated by M2M can enable faster and cheaper access to production resources and data, allowing specialized devices to perform microtransactions with other specialized facilities when needed [4].

With so many objects connected, some obstacles appear, it is not easy to guarantee securely monitoring, storing, and managing billions of low-cost connected devices is, given the issues related to the vulnerability of such devices to cyber attacks [9]. Zivic et al. [33] pointed out that one of the essential characteristics for M2M is that transactions occur at low cost (or zero cost). For Raschendorfer et al. [4], this needs to happen quickly, reliably, efficiently, executed and paid so distributed. Current centralized systems are probably not scalable enough to support millions of microtransactions per second efficiently and enable greater automation in dynamic factory processes, automated decision making, and successful negotiation. For the authors, IoT technologies and intelligent communication devices, combined with Distributed Ledger technologies, can be the drivers for implementing a Machine-to-Machine (M2M) economy [4,9,33].

Blockchain technology in the M2M system is a challenging task, mainly due to the considerable computational load that PoW induces and the low transfer rate achieved by many applications. Also, sensor data monetization suffers inherent problems with the Blockchain protocol in scalability issues since it is not intended to transfer data [34]. In this scenario, Iota Tangle technology seems to be a promising solution [9]. Iota is already an operational project, with many developments based on it and studies to make it one of the "de facto" standards for the IoT protocols [9], incorporating quantum-proof cryptography and trying to solve the problems of Blockchain scalability [34].

Sending transactions on the Iota network does not require token sending. Tokens should only be used when there a reason to use them [9]. Iota technology allows a large number of transactions within seconds, enables different use cases, many on-demand, such as those cited by Zivic et al. [33]: "sensors that sell real-time data to computer stations"; "sensors that buy analytical capabilities from computer stations"; "consumers can buy electricity from any electricity producer"; "devices that buy storage space"; "devices that buy on-demand bandwidth without subscriptions"; "data integrity guaranteed for many devices"; "tamper-proof event log that is guaranteed for each type of infrastructure"; "e-voting and e-governance". For this reason, Iota is the primary cryptocurrency of IoT transactions between machines.

There are two main problems pointed out by the authors who research Iota, a utility for M2M transaction in IoT devices: the figure of the "Coordinator", as it gives a centralized character to the network; and the question of not guaranteeing double-spending with 100% certainty but with a certain probability. Assante and Crucco [9] point the interest of world giants such as Microsoft, Bosch, Cisco, and Samsung as evidence of the potential of Iota technology to be explored as the "support layer" for other devices.

The analysis by Raschendorfer et al. [4] consisted of an expansion of conclusions based on a proof of concept using Iota. The proof of concept of the authors is communicating with an interface that performs the management, data flow, and simulations to outsource the painting process to a robot, sending instructions and materials necessary to perform them, expecting to receive the cost of operation. The robot calculates the final price, and if the value agrees, Iota tokens are sent, waiting until the transaction is attached to the Tangle for the material to be produced. Raschendorfer et al. [4] and his collaborators conclude that there are gaps not yet filled by Iota to be ready for machine economics. The authors emphasize the lack of "smart contracts" to handle transactions. They also emphasize that the figure of the "Coordinator" eliminates the benefits related to decentralization [4].

The proof of concept of Assante and Crucco [9] is a simulation of an electric car that pays for a charging, proportional to the amount of energy consumed. For the authors, in an M2M scenario, that the car must be able to interact autonomously with the charging station, requesting a certain amount of energy, and obtaining an automatic payment for the amount using a reliable form of payment. The charging station should be able to verify the transaction in real-time, stopping charging the car immediately if the transaction cannot be performed. Developed in Python, the bench application was built on a Raspberry Pi and Debian Linux, connected to an LED and a resistor. The LED simulates an electric car that goes to the charging station. Once the connection between the car and the toll is established, a Tangle lookup is performed against the wallet address of the car, containing at first the full value of the coin. One transaction per second is performed for a predefined period, which is verified in real-time by the charging station. If the car credit is used up, the system identifies the new situation in real-time and, within the next second, stops the recharge operation, represented by one LED off [9]. For the authors, in principle, the implemented system proves Tangle's ability to be adopted to manage real-time M2M transactions since Iota tokens were used for the transactions mentioned in the PoC [9].

Lamtzidis and Gialelis [34] describes a monitoring system using distributed sensors in a delimited area. The authors idea is as follows: the sensor data, storage resources, processing power, and excess energy could be traded in an automated machine-machine (M2M) ecosystem. For the proposed system, each node is called a Super Node (SN), it is able to connect to a large number of sensors via LoraWAN, the SN receives data from the sensors, packages the data in transactions that are sent to a gateway, which processes packets before transmitting them to the Full node Iota. The system also supports peer connectivity using IEEE 802.15.4 (Zigbee). The gateway is required because long-range communications (such as LoRa) cannot efficiently transmit data packets needed to send the bundle. Authors also use the MAM channel to restrict access and encrypt data. [34]. Each SN can share its resources with any Iota compatible device. According to the authors, data monetization is one of the main aspects of

the proposed system. Although Iota Foundation has its own data market, the proposed market is different as it allows prices to change dynamically. An SN can interact with other Iota powered devices and acquire resources via Iota token exchange. These devices may be neighbors who have physical access to sources energy, network, or even a drone using contact charging technology and Iota [34]. All architectural and operational aspects are represented in sequence to demonstrate the functionality of the proposed system. Future actions include performing field system audits to evaluate proposed technologies [34].

*3.2.3. Health applications (E-health)*

This section presents four papers (Fig. 4), all of which presented proof of concept for healthcare using Iota, seeking to use DLT as a secure, consensus data layer that stores data from wearable devices and other data, as well to share patients information with a network of healthcare professionals.

Electronic devices such as smartphones, smartwatches, smart glasses have the potential to improve access, efficiency, and quality of health care [26,35]. Activity data generated outside the supervision of health professionals may provide a complete narrative to assist patient care from remote locations [24]. Pacemakers, motion sensors, smart glucometers, and activity trackers, paired with remote monitoring and telemedicine services, will enable patients to receive care and keep their health up to date [24].

Although sharing health data can offer many benefits to society, most data generated by IoT devices are currently controlled by different providers, device manufacturers, or even different health systems, making it impracticable or very difficult to share data outside their indoor environments [26]. For Shafeeq et al. [36], a decentralized access control system that can provide privacy and scalability is required [36], without dependencies on a central authority or specific hardware [35]. Share health data can provide predictive models based on population-level health data, with appropriate consent [24]. Share to patient data need to guarantee the security and privacy this information, and centralized systems are attractive targets for cyber attacks, another barrier is the lack of reliability of the collected data [24,26,35,36].

The disponibility of patient data, and support for various techniques such as deep learning, big data in conjunction with theoretical knowledge and technical experience can contribute to the study and evaluation of various clinical cases [35]. Control models to data access have been proposed for data sharing and to preserve anonymity and to gives users control over their own data using distributed ledger [24,36].

The Iota technology is promising for the future of electronic finance, however, it does have a place in all data-generating industries [24]. Iota technology is capable of sharing anonymous patient data [35] at no additional transaction fee, and is a tamperprostributed accounting protocol that addresses the scalability issues of other DLTs, helping to consolidate research and enable granular and controllable access to health data [26].

The proof of concept by Brogan et al. [24] enabled each device to be configured to transmit data through a MAM channel. According to the authors, a wearable device that is not suitable for storing the current state of the Iota tangle can still transmit data using MAM. The Proof of concept enables patient-defined access controls. That is, if a patient wants to grant access to one or more doctors, he could send the keys to the doctor's channel. It was also possible that the patient could revoke access to his data stream at any time. For this end, he could simply update the authorization key of his MAM channel and provides it to the desired subset of his healthcare providers. The authors further analyze message transmission times using MAM from two different processors, ARMv7 (Average 18.2881s) and Intel i7-7700 HQ (Average 12.5842s); the message size was of 1000 character Brogan et al. [24].

Zheng et al. [35] propose an essential tremor (ET) monitoring system, which is typically evaluated with validated scales and that provides only subjective assessment during a clinical visit, but which can be monitored via motion sensor and become useful in quantifying tremor and activity recognition using deep learning techniques, activity classification models, and tremor assessment models. With this in mind, the authors sought to identify data-based tremors from the devices of 20 subjects while they were performing tasks. The authors demonstrated the feasibility of accurately assessing tremor severity during each specific activity. In sequence to foster research on ET, the work proposed to share the blocks of data produced safely, preserving anonymity, using the distributed Iota ledger. The central idea was to "send" transactions where the "tag" (variable in Iota library) refers to the ET topic and hierarchical geographical references. In this way, researchers can share and access broader ET-related information, helping to understand individual evolution in the short and long term. Since the proposed models are based on collected data, classifiers should improve their accuracy based on sampling size [35].

The article by Zheng et al. [26] used a previously developed smartwatch Pebble human movement monitoring system for remote ET diagnostics, air quality sensors, and smartphone data to develop their proof of concept. This system allows you to measure triaxial acceleration for tremor assessment and activity recognition, location, activity name, tremor level, disease self-assessment, and other disease-related factors – such as medication, alcohol, and coffee – the information is compressed and uploaded to the remote server, sent by the smartphone which also becomes a gateway. The temperature, humidity, air quality and noise sensors sent via Raspberry Pi, also used as a gateway. The data was published to Tangle using a computer equipped with a 4 GHz 4-core Intel Core i5-4460 4 GHz CPU, 12 GB of RAM and the Ubuntu Linux 18 64-bit operating system. Memory usage was 50%. The actual waiting time was a few seconds (7.81s) and more than half a minute (55.51 s) [26]. Although the prototype of Zheng et al. [26] is functional, it is important to mention that a local server was introduced between the gateway layer and the Iota nodes to handle large amounts of raw data and simplify the testing process. In practical application, this local server can be deleted. Sensor data can be published directly to Tangle or via a gateway such as a smartphone or Raspberry Pi [26].

Shafeeq et al. [36] proposed and developed a decentralized data control policy system with Iota. The proposed scheme aims to allow the creation of data access policies, such as: "A cardiologist can read patient data if he is the patient's designated cardiologist". The proposed structure makes access restricted, where the use of an access token is mandatory to access the patient's record and electronic health. The authors developed an architecture that uses both MAM channel (for access policy publishing) and conventional Iota transactions (for the transfer of access rights) for data visualization. The hospital has the credentials of each professional, and if the request is in accordance with the patient's access policy, the medical record is released to the doctor Shafeeq et al. [36]. The experiments of Shafeeq et al. [36] were made on Windows 10 with Intel Core i5 and 4 Gb RAM. We used the official Iota Core javascript library and MAM javascript library. The average time to attach and transmit the transaction using MAM for Tangle was 17 s. The average time between requesting access and securing access in the proposed system is about 10 min, noting that the transaction rate and quality network affect the time. The solution has been tested and was confirmed to be secure in the intruder presence [36].

The current implementation of MAM has proven effective for systems that require access authentication for activity data. However, improvements that design and performance. However,

the MAM is still under development, evolving fast [26].Brogan et al. [24] suggests that a secure key exchange protocol should be integrated within the MAM module to exchange authorization keys between the parties. The authors also report that the MAM library is not optimized for different CPUs [24]. The actual waiting time for attaching a message in the Tangle can range from a few seconds to more than 1 min. Although this is faster than other block-based protocols, there is still room for improvements Zheng et al. [26]. The convergence of Iota Tangle, MAM, and IoT could significantly accelerate health data sharing.

#### 3.2.4. Automotive

The two articles that analyze Iota for vehicular applications have different focuses. While Bartolomeu et al. [37] seeks to identify general problems on communication, security, and privacy in current automobile systems and how Iota could collaborate with these systems, Tesei et al. [38] propose a new vehicular public key infrastructure that uses Iota, focused on intelligent transport systems.

The incorporation of information and communication technologies within vehicles and transportation infrastructure will revolutionize the mode which we travel today [38]. It is not difficult to imagine a world where families do not own cars and are transported by intelligent vehicles. In this scenario, car fleets can manage themselves according to their intended use, and cars can transport people to save energy and maximize the profitability of their owners, thereby providing maximum comfort and experiences to their users [37].

The future of transport and mobility will undoubtedly be realized by autonomous vehicles that including detection capabilities that can cooperate and share their resources detection and perspective with others vehicles [37]. Despite the many potential benefits, there are still critical challenges in the field of reliable, real-time communication between vehicles and transport infrastructure [38], or even within the vehicle itself [37].

Several problems have been pointed out in regard to misbehavior and cyber attacks, for example, Sybil or DDoS attacks [38]. Bartolomeu et al. [37] highlight invasions in vehicular systems found in the literature, which include: controlling a Jeep Cherokee's entertainment system from the Internet, interfering with dashboard functions, steering, brakes, and transmission; intercepting multiple sensors on a Tesla Model S from a laptop; access to the vehicle information and entertainment system of a Volkswagen Golf GTE and an Audi A3, which allows you listen to conversations onboard the vehicle through ta vehicular kit, access the address book and conversation history, and track vehicle location and history on the vehicle navigation system; remotely access a BMW via interfaces wireless, Bluetooth and cellular network.

Both Tesei et al. [38], Bartolomeu et al. [37] raise concerns about the anonymity and privacy of users. For Bartolomeu, anonymity, such as the shared information capacity without disclosing the identity of its producer, is particularly relevant when it comes to the vehicle location. Specific security mechanisms are essential for real-life deployment of intelligent transportation systems to meet challenging requirements of safety, technical, social, legal, and economic concerns [38].

An approach using a DLT such as Blockchain can mitigate most of the issues mentioned, due to intrinsic properties such as untrustworthy operation, immutability, transparency, easy verification, cryptographic security, auditability and independence of third parties [37]. However, the existence of miners in the network creates dependencies on these actors, and fluctuating price and fees of a cryptocurrency can lead to unpredictable costs in upgrade processes [38]. Blockchain growth for each node is unreasonable in the domain of the Internet of Things [38].

For Bartolomeu and his collaborators, Iota can provide a layer of security and privacy for communication protocols. The authors considered it crucial to evaluate writing transaction times and latency in Tangle. They evaluated the times to attach to Tangle, using one public node and a private node (connected to the CarrIota project), concluding that Tangle suffers from fewer transaction delays than existing public Blockchains. Tests by Bartolomeu and his collaborators show that the "tip selection" and "attach to tangle" phases are the most contributing factors to the overall time. The "transaction sending" results in minimal delays (up to 650 ms). The authors state that the latency of transactions using Iota is insignificant compared to vehicular applications and that Iota technology can provide privacy to automobile communications [37]. The article by Tesei et al. (2018) is based on a SECMACE VPKI credential management infrastructure to propose a new vehicular public key infrastructure using Iota. SECMACE supports several standards to meet the safety requirements of a vehicular network. According to the authors, despite the many potentials, SECMACE is based on a certification authority and is vulnerable to errors or violations of this central authority. In SECMACE and the authors proposition, there are actors on the web who are responsible for "vehicle registration" and issuing trusted pseudonyms for vehicle. In the proposal, Iota, can ensure confidentiality in the procedures for registration and updating of vehicle certificates [38]. During the registration phase, each vehicle requests a key, the key will be used to access the MAM channel. According to the authors, the solution is resistant to DDoS attacks [38].

#### 3.2.5. Smart City a social compliance

Ferraro et al. [19] present a social compliance model. The authors idea is to encourage human and machine behaviors to perform actions that help society through tokens exchanging. The model presented involves depositing a token and redeeming in case of "good behavior" to achieve a common goal. Besides that, the authors compared Blockchain and Tangle for their proposal. They highlight the advantages of Tangle for social compliance. Techniques for enforcing social contracts are important in any shared economy system. For the authors, charging points for electric cars, electric bicycle-sharing, and ensuring that cyclists and cars comply with transit rules have common problems and are related to the interaction of humans with machines and the need to respect certain behaviors to achieve social goals [19].

A Tangle-based model was developed to mathematically and computationally analyze Tangle behavior, including what occurs during network attacks [19]. Among the results, the authors identified that the existence of conflicts affects the network quickly, generating fewer tips available for a time, proportional to the average time between creation and disclosure of transactions to the network. After this attacks, the network stabilizes and continues its pre-attack regime. Conflicts between transactions do not happen in Tangle under the large arrival rate regime simulated by the authors [19]. From an example related to the junction of traffic at a traffic light, the authors demonstrate that small levels of non-compliance can lead to system instability, such as traffic. This example is then generalized to a generic set of interconnected activities on a road network to which the DLT Iota-based control mechanism can be applied [19].

#### 3.2.6. Others

The articles in this group have the objective of proposing improvement or analysis of technology. They are not aimed at a type specific of application, but are nevertheless intertwined with any application. There are four papers in this session. Namely, a solution that seeks to ensure anonymity [16], a proposed algorithm that avoids the reuse of addresses [29], a description

of a repetition attack, by reusing addresses [39], and finally an analysis of Tangle that seeks to identify if there exist sufficient incentives for network nodes to follow behaviors in favor of Network Health [15].

Iota has a dedicated mixing service to improve anonymity [40], but it still depends on a relying party. Consumers of the mixing service need to rely on service providers because they may be forced or encouraged to disclose this information [16]. For this reason, Sarfraz et al. [16] presents a new decentralized mixing protocol for Iota, incorporating a combination of decoding mix nets and multi-signatures. The technique requires no third parties (reliable or responsible), is completely compatible with the Iota protocol, and does not present additional mixing fees. Mixing services allow a way to transfer funds to a new address in a non-binding manner. For example, if Alice sends funds to a mixing service [40], the service will transfer funds from some randomly chosen user to Alice's new desired address. An external observer cannot distinguish transactions normal of a mixed [16]. The authors took advantage of the Iota transaction-free and M2M feature to exchange keys between network nodes for a decentralized mixer. The solution makes the mapping of payment histories difficult, improves the benefits of a centralized mixer, and prevents it from falsifying signatures due to private key part leaks [16].

Given the already mentioned problem of reusing addresses, especially after a snapshot, Shafeeq et al. [29] proposed a new solution that makes it virtually impossible to reuse address. According to the authors, the solution does not require any user interaction and does not require changes in the principles and design of Iota, and can be integrated as an extension. In the solution of Shafeeq et al. [29], the "Light node" (as an embedded system) should store a "cuckoo filter" that contains all the used addresses. Whenever a user requests a wallet to generate an address to receive funds, the "Cuckoo filter" will checked if it does not contain an address, a new public key is generated and a copy of the address is also sent to the "cuckoo filter" to avoid future reuse. Suppose a user logs in for the first time after the "snapshot", in this case the wallet generates the index 0 address and consults the "Cuckoo filter" to find out if an address has already been used to receive funds. If the return is negative, it means that an address has not used to receive funds; otherwise, it means that an address has been probably used to receive funds before. The "Light node" connect to the "Full node" and queries the address funds, that are found in the "Cuckoo Filter", which then assigns addresses of balance different of zero to the Tangle [29]. Shafeeq et al. [29] details a series of particularities and evaluation of the implementation of the algorithm and concludes that the proposed scheme avoids the reuse of addresses. The solution it also implies less time for address generation and minimal data storage, which is a prerequisite for IoT.

De Roode et al. [39] also explores the possibility of multiple transactions generated with the same address. The Iota API was modified for that the addresses to be reused. The authors describe what was necessary to modify to perform a successful replay attack then. It has been shown that the replay attack can be realized; however, the reuse address prerequisite limits the attack. Assuming the attacker did not have access to the victim's software, it would be difficult to force the victims to reuse their addresses [39].

Popov et al. [15] presents a mathematical model to study the Tangle and prove the existence of Nash equilibrium in the Tangle, even in the scenario in which part of the network nodes try to optimize their strategies for attaching transactions. A strategy that could be used would be to choose a couple of old transactions and approve them all the time, without having to do the heavier work of verifying new transactions, thus adding new information to the system, if everyone behaves this way, no new transactions will be approved, and the network will effectively stop. Are there enough incentives for participants to "behave well"? The results also show that the strategy studied outperforms in speed; the data show 25% of speed difference in the most extreme scenario. However, the cost computational this strategy is intrinsically greater than the computational cost of non-selfish strategies [15]. Moreover, even an extreme scenario, where nearly half of the transactions were issued by a selfish it, is not enough to harm the non-egotists in a significant way. The data show a deep qualitative dependence on the simulation parameter $\alpha$, mentioned in the end Section 2.1. This parameter is related to randomness; a low value implies high randomness; a higher value implies low randomness, which means that the walk will be almost deterministic. To study the effect of the factor other simulations should be performed [15].

### 3.3. General framework

We identified different motivations for choosing Iota Tangle as a research object. Researchers in M2M applications essentially motived their research due to the possibility of high transaction rates compared to other distributed ledger, as well as the zero cost to exchange data in a decentralized network. Researchers with applications in the Health sector search for the Iota Tangle technology, essential for the possibility to share patient data with health professionals, this data can be obtained from wearable devices or other sensors, always seeking to maintain patient privacy. Automotive applications research is motivated by the low security of current systems deployed in automobiles. Iota for this group of researchers provides a layer of security and privacy to protocols of communication with the car. The only solution in Smart city sought to take the possibility of exchanging data and values at zero cost, with low latency.

Makhdoom et al. [6] asked whether Iota will be an efficient IoT micropayment system only. This question can be answered by the investigation of this article. We can say that Iota is not only a cryptocurrency; it is also a distributed communication protocol that works with consensus algorithms in a semi-distributed network; this evidence is clear when looking at architectures and proof of concept in scientific papers we investigated.

Due to network and computing power available, some devices and sensors did not publish directly in the Tangle, which implies different network architectures, depending on each case. We identified that these architectures are of three types (Fig. 5):

(a) An embedded system connected to sensors reads the data and sends it to a computer (cell phone, single-board computer) through some connection (LoRaWAN, Sigfox, Zigbee, Bluetooth low energy, wireless). The computer has the function of sending data (not the entire bundle), to a remote server (which runs an Iota client or MAM client). The remote server proceeds to construct the bundle and broadcast it to the Iota node (Light or Full node) [26].

(b) An embedded system connected to sensors reads the data and sends it to a computer (cell phone, remote server, single-board computer) through some type of connection. The computer running an Iota client or MAM client, proceeds to generate the bundle and broadcast it to the Iota node [34].

(c) An embedded system (running an Iota client or MAM client) connected to sensors data reads and construct the bundle, and broadcast it to the Iota node [9].

The Architecture of item (a) better when it is necessary high data preprocessing before of creating the transaction and/or there are many sensors close geographically, and the aim is to minimize the number of computers (or single-board computer) needed. The main disadvantage is the centralization identified in the figure of

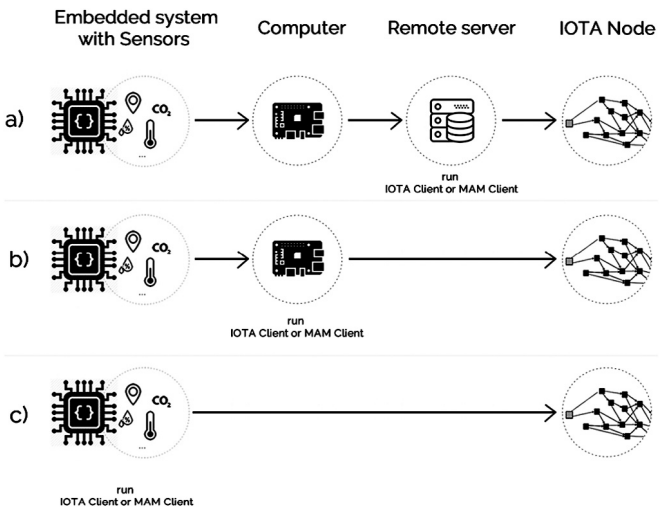



**Fig. 5.** Possible network architectures to publish sensor data to the tangle.

the remote server. Architecture (b) eliminates a point of failure, compared to the previous, consequently it is more secure. It still has a particular disadvantage of centralization, but it can be minimized by using secure and encrypted communication protocols. The Architecture (c) is ideal because the collected data goes directly to the network, and favors the decentralization of the network, and has fewer points of failure. The challenge in the architecture c) is having an embedded system capable of running an Iota Client (or MAM Client) and creating and minimal sending objects needed for an Iota transaction, for each group of sensors. Even better would it be if the embedded system also runs an Iota node.

Several authors presented similar features, this aspects mentioned by the authors are presented in Table 2 (positive aspects) and Table 3 (negative aspects).

We conclude, based on Tables 2 and 3 that, the Iota is a semi-decentralized, public cryptocurrency, capable of performing high transaction rates, since transactions occur in parallel. Iota requires no immediate consensus, the cost to confirm transactions is zero, since every user in the network must participate in consensus mechanism (no exist miners). It is possible to share and exchange data and payments without any fee, with guaranteed immutability. The lower energy consumption necessary to include a transaction in the network, in comparison to other DLTs, and the lower computational power necessary to run an Iota client, facilitate the implementation in different devices with low computational power, such as those coming with IoT. By choosing to use the Winternitz One-Time Signature (WOTS) as a signature scheme protocol, the Iota provides speed and strong resistance to attacks from a possible quantum computer. With the MAM module, it is also possible to share data streams, which can be encrypted or not. Although small, the shortest package needed to send data is large enough for a transaction with LPWAN technologies. Technologies that use DAG like Iota do not support Smart Contracts and have great difficulty in being completely decentralized. As of this writing, such technologies need a central point, as the "Coordinator".

The most investigated technical weakness is the impossibility of reusing address when using WOTS. The security of a particular address (possibility of appropriation of funds) decreases when the number of times it is used to send funds increases. It makes it easy for an adversary to forge the signature to steal funds because each time tokens are sent, it reveals 50% of the private key associated. The current Iota protocol mitigates address reuse issues by using library that prevents transactions with addresses previously used from being used again. However, this protocol may not be able to check what addressed have already been used if snapshots are used. This is because snapshotting removes the transaction history needed to check whether an address have already been used.

Another concern is with ensuring that the network is healthy. Based on the papers investigated in this research, even in scenarios where the attacker issued almost half of the transactions, it is not enough to harm of network in a significant way. There will be a certain moment, when transactions are secure; technically, it is correct to say that they have a high probability of certainty of not being abandoned.

## 4. Considerations finals

We consider some factors to be decisive for opting to model a project with Iota that have not been described in papers that analyze Iota, for some application type. We can see in Tables 2 and 3, the absence of mentions to: maintaining the transaction history, as presented in Sections 2.2.2 and 2.2.3; adaptation period of a transaction, mentioned in Section 2.1; and we also have not identified approaches that discuss incentives to run Full nodes.

Understanding that networks need "Snapshots" is crucial for projects that need to preserve historical data. There is often a confusion between Blockchain and Tangle, giving the impression that transaction data is saved permanently. However, it is necessary to find an alternative solution to saving data: maintaining a Full node without snapshot, using a cross-chain solution combined by Blockchain or save transactions in a database. We emphasize that it is necessary to further discussions how reliable this data is after a "Snapshot".

The theoretical "adaptation period" demonstrated in Section 2.1 is only valid in the absence of the "Coordinator". While the "Coordinator" is present in the network, a transaction is considered 100% valid when signed by the "Coordinator", mentioned in Section 2.2.1. Since the Tangle does is not need to wait for "adaptation period", transactions always occurs in parallel and do not require immediate consensus; however, some transactions will be abandoned. This question is not presented by authors that propose to analyze the Iota for some type of application. It is important that the authors explain how this factor may or may not be significant in their approach. The absence of this discussion makes us believe that it is not very relevant; however, this may not be true.

The need for low latency in applications and some control over data can be two of the biggest incentives for companies to run Iota Full nodes and cooperate with the network. Incentives to run Full nodes are important factors to be analyzed in the medium/long time. If the Iota becomes a standard for IoT devices, the Tangle network will bring greater decentralization, scalability, and more weight to the main chain, enabling greater security, which would make easier to remove "Coordinator" from this network. For us, believing in this technology implies believing that there exist incentives to run nodes. Otherwise, the network will always be dependent on an institution to keep the network healthy and decentralized in terms of nodes.

We suggesting the existence of more features for Full nodes as a solution to encourage institutions to run Full nodes. The feature should enable the maintenance of old chosen transactions in the network, after a local "Snapshot"; it would have a function similar to "Permanode". If this becomes viable, the ecosystem will be simpler, the old transactions would be more reliable, the hash power will be incremented, and the network would be more easily scalable.

**Table 2**
Positive aspects — Iota Tangle.

| Aspects | Associated to | Authors |
|---|---|---|
| High Transaction Rates | - Immediate consensus is not necessary;<br>- Transactions occur in parallel;<br>- There are no blocks, just transactions;<br>- There are no miners; | [5–9,35,37] |
| Public DLT | - Anyone can join the network | [5,7,33,37] |
| Micro or nano payment | - No miners;<br>- Absence of fees;<br>- every user in the network must participate of consensus mechanism; | [5–8,33] |
| Run in small and heterogeneous devices | - Low computer power necessary to run Light node;<br>- Low PoW compared to public Blockchains;<br>- Low energy consumption; | [6,7,9,24,26,35] |
| Security of transactions | -Partially decentralized;<br>- Winternitz One-Time Signature (WOTS), quantum-proof cryptography | [16,24,29,34–36,38,41] |
| Data exchange and/or sharing | - Absence of fees;<br>- It is not necessary send tokens; | [9,33–35] |
| Share data feeds, encrypted or not | - MAM modes allow to share data public, private or restricted;<br>- Merkel Signature Scheme, quantum-proof cryptography | [24,26,36–38] |

**Table 3**
Negative aspects — Iota Tangle.

| Aspects | Associated to | Authors |
|---|---|---|
| Not exist Smart Contracts | - DLTs that use DAG have intrinsic difficulties for having Smart Contracts | [4–6,8] |
| Not completely decentralized | - Central computer (coordinator) is needed;<br>- Technologies that use DAG may need a central point; | [4,6–9,33,34] |
| Low compatibility with LPWAN Technologies | - Cannot directly and efficiently send a transaction to Tangle via LPWAN | [34] |
| Dont possible realize multiple transaction with same address | - The security of wallet addresses decreases as the number of times they are used, because of WOTS | [29,36,39] |

The synthesis of the items analyzed in session 3.3, combined with the discussions proposed here, can help interested in developing and understanding the nuances of a project with Iota. In addition, researchers interested in an application will be able to go directly to the group of their interested in Section 3.3.

We understand that Iota Tangle is not only a cryptocurrency but also a distributed communication protocol that uses consensus algorithms. The proposed architecture was able to create one blockless distributed network, without miners and fees, where low-power devices can help approving transactions. By allow transactions to occur in parallel, Iota scales as the number of transactions on the network increases, if the "Coordinator" is no longer active on the network. In the current stage of technology, the biggest challenge is to remove the "Coordinator" from the network. We consider this to be the most important current research in DAG-based DLTs.

In addition research that evaluates the potentials and limitations of protocol for a specific purpose, we also recommend future research about the security of Iota protocol, due to the little number of high impact papers in this respect and the great importance of the investigation for DAG-based DLTs. We also recommend that independent researchers simulate Tangle with different tips selection algorithms, comparing with the MCMC used in Tangle. Considering the potential of MAM library, we recommend careful evaluation of code, especially seeking improvement. The Iota Foundation also has in its roadmap research related to the creation of a layer of smart contracts, which deserves much attention.

Emerging technologies involve risks inherent in its vanguard, such as Iota, however the technology already fulfills several points necessary for its maturity. The challenges encountered make it exciting to follow-up and research his approach in distributed computing. We are moving towards a connected future, and the Iota can be the cryptocurrency and protocol to ensure security; make payments machine-to-machine, machine-to-people, people-to-machine, people-to-people; and send data at no cost.

## CRediT authorship contribution statement

**Wellington Fernandes Silvano:** Conceptualization, Methodology, Investigation, Writing - original draft, Writing - review & editing. **Roderval Marcelino:** Supervision, Writing - review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

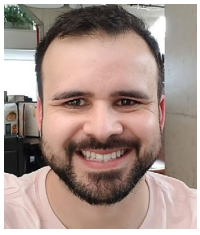
## Acknowledgments

This work is part of a research supported by Fundação de Amparo a pesquisa de Santa Catarina (FAPEU).

## References

[1] S. Popov, The tangle, 2016, pp. 1–28.
[2] Drop the phone and talk to the physical world: Programming the internet of things with erlang, in: 2012 Third International Workshop on Software Engineering for Sensor Network Applications (SESENA), 2012, pp. 8–14.
[3] C. Zhang, Y. Chen, A review of research relevant to the emerging industry trends: Industry 4.0, iot, block chain, and business analytics, J. Ind. Integr. Manag. 5 (1) (2020) 165–180.
[4] A. Raschendorfer, B. Mörzinger, E. Steinberger, P. Pelzmann, R. Oswald, M. Stadler, F. Bleicher, On IOTA as a potential enabler for an m2m economy in manufacturing, Procedia CIRP 79 (2019) 379–384, http://dx.doi.org/10.1016/j.procir.2019.02.096, 12th CIRP Conference on Intelligent Computation in Manufacturing Engineering, 18-20 July 2018, Gulf of Naples, Italy. URL: http://www.sciencedirect.com/science/article/pii/S2212827119302136.

[5] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29, http://dx.doi.org/10.1016/j.comcom.2019.01.006, URL: http://www.sciencedirect.com/science/article/pii/S0140366418306881.
[6] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: The challenges, and a way forward, J. Netw. Comput. Appl. 125 (2019) 251–279, http://dx.doi.org/10.1016/j.jnca.2018.10.019, URL: http://www.sciencedirect.com/science/article/pii/S1084804518303473.
[7] K. Yeow, A. Gani, R.W. Ahmad, J.J.P.C. Rodrigues, K. Ko, Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues, IEEE Access 6 (2018) 1513–1524, http://dx.doi.org/10.1109/ACCESS.2017.2779263.
[8] Y. Jiang, C. Wang, Y. Wang, L. Gao, A cross-chain solution to integrating multiple blockchains for iot data management, Sensors 19 (9) (2019) http://dx.doi.org/10.3390/s19092042, URL: https://www.mdpi.com/1424-8220/19/9/2042.
[9] D. Assante, R. Crucco, M2m learning environment for electric applications, in: 2019 IEEE Global Engineering Education Conference (EDUCON), 2019, pp. 1518–1522, http://dx.doi.org/10.1109/EDUCON.2019.8725151.
[10] M. Walport, Distributed ledger technology: Beyond blockchain. uk government office for science, Technical Report, Tech. Rep, 2016.
[11] B.C. Florea, Blockchain and internet of things data provider for smart applications, in: 2018 7th Mediterranean Conference on Embedded Computing (MECO), 2018, pp. 1–4, http://dx.doi.org/10.1109/MECO.2018.8406041.
[12] V. Buterin, Ethereum sharding faqs, 2018, URL: https://github.com/ethereum/wiki/wiki/Sharding.
[13] F. Marino, C. Moiso, M. Petracca, Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming iot ecosystems, Comput. Netw. (2018).
[14] M. Divya, N.B. Biradar, Iota-next generation block chain, Int. J. Eng. Comput. Sci. 7 (04) (2018) 23823–23826.
[15] S. Popov, O. Saa, P. Finardi, Equilibria in the tangle, Comput. Ind. Eng. 136 (2019) 160–172, http://dx.doi.org/10.1016/j.cie.2019.07.025, URL: http://www.sciencedirect.com/science/article/pii/S0360835219304164.
[16] U. Sarfraz, M. Alam, S. Zeadally, A. Khan, Privacy aware iota ledger: Decentralized mixing and unlinkable iota transactions, Comput. Netw. 148 (2019) 361–372, http://dx.doi.org/10.1016/j.comnet.2018.11.019, URL: http://www.sciencedirect.com/science/article/pii/S1389128618306972.
[17] U.W. Chohan, The double spending problem and cryptocurrencies, 2017, Available at SSRN 3090174.
[18] M. Rosenfeld, Analysis of hashrate-based double spending, 2014, arXiv:1402.2009.
[19] P. Ferraro, C. King, R. Shorten, Distributed ledger technology for smart cities, the sharing economy, and social compliance, IEEE Access 6 (2018) 62728–62746, http://dx.doi.org/10.1109/ACCESS.2018.2876766.
[20] A. Gal, The tangle: an illustrated introduction, 2018, URL: https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4.
[21] C.T. Iota, The coordicide, 2019, pp. 1–30.
[22] D. Sønstebø, Iota development roadmap, 2017, URL: https://blog.iota.org/iota-development-roadmap-74741f37ed01.
[23] P. Handy, Introducing masked authenticated messaging, IOTA Found. Medium blog (2017).
[24] J. Brogan, I. Baskaran, N. Ramachandran, Authenticating health activity data using distributed ledger technologies, Computational and Structural Biotechnology Journal 16 (2018) 257–266, http://dx.doi.org/10.1016/j.csbj.2018.06.004, URL: http://www.sciencedirect.com/science/article/pii/S2001037018300345.
[25] A. Hülsing, W-ots+–shorter signatures for hash-based signature schemes, in: International Conference on Cryptology in Africa, Springer, 2013, pp. 173–188.
[26] X. Zheng, S. Sun, R.R. Mukkamala, R. Vatrapu, J. Ordieres-Meré, Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies, J. Med. Internet Res. 21 (6) (2019) e13583, http://dx.doi.org/10.2196/13583, URL: https://www.jmir.org/2019/6/e13583/.
[27] A. Bmushi, Iota: Signature and validation, 2018, URL: https://medium.com/@abmushi/iota-signature-and-validation-b95b3f9ec534.
[28] S. Iota, How addresses are used in iota, 2019, URL: https://iotasupport.com/how-addresses-are-used-in-IOTA.shtml.
[29] S. Shafeeq, S. Zeadally, M. Alam, A. Khan, Curbing address reuse in the iota distributed ledger: A cuckoo-filter-based approach, IEEE Trans. Eng. Manage. (2019) 1–12, http://dx.doi.org/10.1109/TEM.2019.2922710.
[30] J. Buchmann, J. Ding, Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA October 17-19, 2008 Proceedings, Vol. 5299, Springer Science & Business Media, 2008.
[31] S. Rohde, T. Eisenbarth, E. Dahmen, J. Buchmann, C. Paar, Fast hash-based signatures on constrained devices, in: G. Grimaud, F.-X. Standaert (Eds.), Smart Card Research and Advanced Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 104–117.
[32] G. Mester, Rankings scientists, journals and countries using h-index, Interdiscip. Descr. Complex Syst.: INDECS 14 (1) (2016) 1–9.
[33] N. Zivic, C. Ruland, J. Sassmannshausen, Distributed ledger technologies for m2m communications, in: 2019 International Conference on Information Networking (ICOIN), 2019, pp. 301–306, http://dx.doi.org/10.1109/ICOIN.2019.8718115.
[34] O. Lamtzidis, J. Gialelis, An iota based distributed sensor node system, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6, http://dx.doi.org/10.1109/GLOCOMW.2018.8644153.
[35] X. Zheng, A. Vieira, S.L. Marcos, Y. Aladro, J. Ordieres-Meré, Activity-aware essential tremor evaluation using deep learning method based on acceleration data, Parkinsonism Rel. Disorders 58 (2019) 17–22, http://dx.doi.org/10.1016/j.parkreldis.2018.08.001, URL: http://www.sciencedirect.com/science/article/pii/S1353802018303316.
[36] S. Shafeeq, M. Alam, A. Khan, Privacy aware decentralized access control system, Future Gener. Comput. Syst. 101 (2019) 420–433, http://dx.doi.org/10.1016/j.future.2019.06.025, URL: http://www.sciencedirect.com/science/article/pii/S0167739X18332308.
[37] P.C. Bartolomeu, E. Vieira, J. Ferreira, Iota feasibility and perspectives for enabling vehicular applications, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–7, http://dx.doi.org/10.1109/GLOCOMW.2018.8644201.
[38] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto, P. Pagano, Iota-vpki: A DLT-based and resource efficient vehicular public key infrastructure, in: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1–6, http://dx.doi.org/10.1109/VTCFall.2018.8690769.
[39] G. De Roode, I. Ullah, P.J. Havinga, How to break iota heart by replaying?, in: 2018 IEEE Globecom Workshops (GC Wkshps), IEEE, 2018, pp. 1–7.
[40] L. Tennant, Iota mixer v1 released, 2017, URL: https://medium.com/iota-ucl/iota-mixer-91f3d39735c1.
[41] P.C. Bartolomeu, E. Vieira, J. Ferreira, Iota feasibility and perspectives for enabling vehicular applications, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–7, http://dx.doi.org/10.1109/GLOCOMW.2018.8644201.



**Wellington Fernandes Silvano (Author)** Currently study a Master degree in Information and Communication Technology in Federal University of Santa Catarina (UFSC). The research is focused in use of Distributed Ledger Technologies (DLT) for IoT applications.

Graduate in Physics at UFSC, where he participated in two cores of technology Educational Laboratory, LANTEC and NUTE. At the same time did research in Physics area. Has over two years of experience in coordinating Web projects linked to the Brazilian federal government.

**Roderval Marcelino (Co-author)** Currently is a profess or at the Federal University of Santa Catarina, has a postdoctoral degree from ULSTER University in Northern Ireland, a PhD in Engineering, has experience in Computer Science, focusing on Embedded Systems, working mainly with microprocessors, automation, renewable energy. and software. He is leader of the research group of CNPQ LPA-Applied Research Laboratory. Member and researcher of LABTEL research laboratory.