2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid) | 978-1-7281-9586-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCGrid51090.2021.00091

Secure Asset Tracking in Manufacturing through Employing IOTA Distributed Ledger Technology

Svoronos Leivadaros
Electrical & Computer Enginering Dept.
Hellenic Mediterranean University
Heraklion, Crete, Greece
leivadaros@yahoo.gr

George Kornaros
Electrical & Computer Enginering Dept.
Hellenic Mediterranean University
Heraklion, Crete, Greece
0000-0002-2371-0633

Marcello Coppola
STMicroelectronics
ST life.augmented
Grenoble, France
marcello.coppola@stm.com

***Abstract*—Today, manufacturing industry is increasingly embracing new technologies such as the Internet of Things (IoT), big data analytics, cloud computing and cybersecurity to cope with system complexity, increase information visibility, improve production performance, and gain competitive advantages in the global market. These advances are rapidly enabling a new generation of smart manufacturing, i.e., a cyber-physical system tightly integrating manufacturing enterprises in the physical world with virtual enterprises in cyberspace. To a great extent, realizing the full potential of cyber-physical systems depends on the development of new methodologies on the Internet of Manufacturing Things (IoMT) for data-enabled engineering innovations. This article presents a real implementation of IOTA Tangle architecture for data transactions extended with HMAC signing through using STM32 (F7 CPU) IoT devices. The evaluation results show promising with 32 light nodes to exceed 28 transactions per second by using 4 full nodes, thus making IOTA-based distributed ledger an effective solution for IoT-based manufacturing environments with zero-value (data) transactions.**

***Index Terms*—distributed ledger technology, IOTA, blockchain, Industrial IoT, STM32**

I. Introduction

Cybersecurity is profoundly the most critical and challenging barrier for the IoT in several application domains and especially in industry [1] [2] [3]. With respect to typical network security, IoT security is subject to several new factors and conditions that amplify potential threats, such as increased open network surface [4] [5] [6] [7], concerns on genuin vendors and suppliers firmware updating [8]. IoT devices are typically interconnected with other devices, in very variable deployment conditions, making it complex to manage device-to-device interactions and to protect them from malicious data manipulation. IoT nodes are commonly isolated hardware solutions which are subject to tampering in ways that may be unpredictable by manufacturers. The main challenge is that these nodes have typically limited computational power, which hinders the adoption of highly sophisticated security frameworks. Once IoT devices are connected with each other and with the Internet, they become an interconnected and complex system which is difficult to immunize against modern security threats. For this reason, such systems are vulnerable to several attacks (password security attacks, message spoofing/alteration, traffic analysis, Distributed Denial of Service, Sybil attack, eavesdropping, etc.). Moreover, a generic "one-size-fits-all" security model is difficult to implement. Various approaches have been proposed to address IoT security: (i) blockchain based solutions, (ii) fog computing based solutions, (iii) machine learning based solutions and (iv) edge computing based solutions [9] [10] [11].

Embracing enabling technologies in industry in cyber-physical systems[1], IoT and cloud infrastructure requires several goals, such as real-time, reliable, and secure data transmission, along with data sharing and management, interface among different nets, massive-scale data and big data collection and storage, data mining, data aggregation and information extraction. The information exchange that occur between machines and the Cloud, and the information flow between different stakeholders in smart supply chain expose smart manufacturing systems to cyber threats. Moreover, as cyber attacks on the IoT is increasing in both frequency and complexity, smart manufacturing is among the most targeted domain, making the smart manufacturing systems less secure than the traditional manufacturing systems. In order to ensure that smart manufacturing is safe, the following security requirements must be guaranteed: availability, reliability, integrity, confidentiality, authentication, message authenticity, accountability, tamper detection, through technological solutions such as blockchain.

Essentially, the blockchain is a distributed data structure, a "distributed ledger" which records transactions occurring between the members of a peer-to-peer (P2P) network. All participating peers maintain identical copies of the ledger. New entries, containing information pertaining to transactions, are added to the blockchain by means of decentralized consensus among the peers. The entries in the blockchain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys. A Merkle tree is used to store the individual transactions and the root hash of the tree is stored in the blockchain.

[1]A CPS is the integration of physical components, sensors, actuators, communication networks, and control centers, in which sensors are deployed to measure and monitor the status of physical components, actuators are deployed to ensure the desirable operations on physical components, and communication networks are used to deliver measured data and feedback comments among sensors, actuators, and control center

978-1-7281-9586-5/21/$31.00 ©2021 IEEE
DOI 10.1109/CCGrid51090.2021.00091

However, most IoT devices come with limited battery power because of cost constraints. Most popular blockchain-based systems use Proof of Work (PoW) [12] (e.g., Bitcoin and Ethereum) or Practical Byzantine Fault Tolerance (PBFT) (e.g., Hyperledger) to achieve coordination. Unfortunately, these protocols require heavy communication and/or computation. Therefore, they are not adequate for IoT devices. For a practical blockchain-based IoT system, a more lightweight technology is required. These reasons have recently led to the fusion of the Industrial Internet Consortium, which promotes best practices for trusted networking, with the Trusted IoT Alliance [13].

A. Contributions

The contributions of this work include leveraging a Directed Acyclic Graph (DAG) based DLT, i.e., developing a real IOTA-based infrastructure by using STM32 IoT devices to ensure security and privacy of IoT data in manufacturing systems (along with decentralization and scalability). By using the distributed ledger network, we have technically ensured that the data cannot be tampered with. The properties of the chaincode invocation mechanism and the historical traceability mechanism of ledgers specifically solve the problem of transparent supervision of collected sensor data in an industrial IoT system. Along with real-time transmission, real-time blockchain-based storage guarantees reliability and transparency.

With a tremendous growth to address the challenges of integrating DLTs into the IoT ecosystem [14], focusing on investigating the computation, communication and security aspects, we employ IOTA Tangle in a real implementation on smart asset tracking in manufacturing for enhanced auditability and trustworthiness. The Tangle, as a mathematical model, is a directed acyclic graph (DAG) for storing IOTA transactions [15]. We propose a solution in which the IoT devices do not store the ledger, and hence the continuous growth of the ledger size has little impact on the storage costs of IoT devices.

B. Related DLT Solutions for IoT

Distributed ledger technology is increasingly employed to foster a decentralized and private IoT and credibility automation in cyber-physical systems (CPS) in smart manufacturing [16], while factors that affect security, integrity, and traceability of this technology are of rising concern [10] [9]. Research on integrating Tangle with resource constrained devices has been presented by incorporating the IOTA Client API on STM32 embedded devices by using a Light Node application to run on two different STM32 platforms with promising results [17]. However, one caveat was that the Proof of Work, i.e., the number of trailing zeros of the hash of a transaction, called Minimum Weight Magnitude (MWM), that was conducted with MWM = 14 for the mainnet took several minutes to compute locally on the platforms; a gateway architecture is henceforth proposed to offload the PoW to a remote full node. At the same time authors propose to reduce large size of keys and signatures for a quantum-secure distributed ledger with novel smart digital signatures [18]; such solutions can be adapted to our infrastructure.

The MADIT (Mobile Agent Distributed Intelligence Tangle-based approach) is a framework that allows virtualization of computing resources in a IOTA network to allow more efficient offloading of computationally intensive processes such as the Proof of Work [19]. Additionally, mobile agents can aggregate data across IoT nodes and remove redundant information from collected data since devices that are geographically close would generate similar types of transactions. Moreover, a Proof of Concept implementation of IOTA with the Masked Authenticated Messaging protocol has recently been proposed [20]. In this work, the Masked Authenticated Messaging (MAM)[2] specification of the IOTA Network is integrated in a Raspberry Pi using the Node.js library and operating in a Linux environment. Contrary to these works our focus is on STM32 IoT nodes with a C-based RTOS IOTA implementation and evaluation framework.

II. Communications in Manufacturing

With the advent of smart manufacturing in Industry 4.0, the interconnection solutions in manufacturing are evolving and mainly involve advancements to facilitate smart interconnection and interoperability. IoT, LPWAN and/or 5G communications blended with legacy networking support intelligent heterogenous equipment management which has actually transformed various physical resources into cyber manufacturing services. Nevertheless, by mainly focusing on the communication layer as Fig. 1 shows, traceability, auditability and authentication are missing attributes from these communication technologies and protocols.

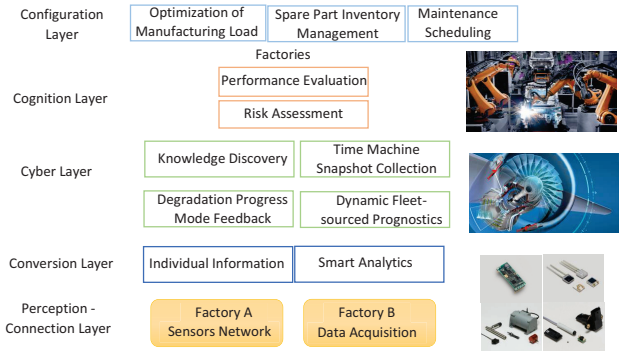

Fig. 1. Example of a layered smart manufacturing organization.

For instance, several application layer protocols for smart interconnection, which can be employed fully (or partially) in manufacturing, have been proposed and designed by big companies or associations. For example, Constrained Application Protocol (CoAP) is a specialized web transfer protocol for Machine-to-Machine (M2M) applications and typically used for resource constrained devices [21]. Message Queuing Telemetry Transport, originally developed by IBM, is

[2]https://docs.iota.org/docs/mam/1.0/overview

a publish/subscribe messaging protocol designed for M2M communications, which is usually used for gateways interconnection [22]. The Advanced Message Queuing Protocol (AMQP) is an open standard message queuing protocol used to provide message service (queuing, routing, security, reliability, etc.) in the application layer [23]. AMQP is considered a message-oriented protocol which can implement various kinds of message exchange architectures, including store and forward, publish and subscribe, message distribution, message queuing, context-based routing, and point-to-point routing. The Extensible Messaging and Presence Protocol (XMPP) is designed for chatting with XML messages and can be used for multiparty chatting, voice and video streaming, and tele-presence [24]. In XMPP, the following three roles are included, client, server and gateway, as well as bidirectional communication is supported between two parties of these three roles. Automation Markup Language (AutomationML), as one of the open standard series (IEC62714), describes the production plants and plant components with plant topology, geometry, kinematics, behavior, references and relations [25]. To provide flexible mechanisms to store different kinds of data, AutomationML defines relevant special attributes, classes, interfaces, and object identification rules. OPC Unified Architecture (OPC UA) is a standardized communication middleware for automation systems and serves as a bridge between offline-based engineering tasks and the runtime communication of the involved physical and logical resources of a CPMS [26]. Despite recent efforts for secure and trusted communications [27], these protocols still are complex to enable sensors to be seamlessly, immutable interconnected to enable automated applications in manufacturing.

LoRaWAN protocol has gained wide acceptance because of its key features such as low power consumption, bidirectional communication, secure, standardized, low cost, and long range [28] [29]. Thus, manufacturing can be "smartified" by using arrays of sensors, actuators, and control units to cross-connect domains to monitor manufacturing systems and secure valuable assets by using wireless and LoRa (or other LPWAN) networking solutions. However, to ensure the authenticity of data that IoT devices provide, cryptographic methods (e.g., of LoRaWAN) are not enough, while blockchain technology emerges addressing such issues while keeping the communication cost constant [30] [31]. Moreover, IoT devices are often lightweight clients, constrained with respect to memory, computation, communication, and power. Thus, they can only store a subset of the blockchain data and eventually generate transactions to be included into the blockchain. Despite the advantages of blockchain solutions (immutability, auditability, fault tolerance, autonomy, fairness) the integration of blockchain into the IoT platform suffers from scalability, energy efficiency and communication overheads [11]. For secure blockchains for IoT and IIoT applications IOTA foundation specifically designed the Tangle [15], which differs from the existing blockchains as it does not use any traditional blockchain at all. The main structure of IOTA is the Tangle, which is a Directed Acyclic Graph (DAG) [15]. Each time a user wants to issue a transaction, she has to verify and approve two recent transactions which then form the edges. This way, the integrity of the Tangle is ensured by the work of the users themselves rather than by a different economic set of nodes, like in the case of blockchain's miners. Furthermore, no fees are imposed by the protocol due to the lack of miners, enabling micro and data transactions, which are fundamental in IoT networks.

Its consensus encourages all participants to contribute in maintaining the ledger through referencing (i.e., approving) two unapproved transactions called tips before issuing any new transaction. For the new coming transaction, IOTA tangle leverages the MCMC random walk algorithm to select two tips. All transactions directly or indirectly approved by this new transaction then add its weight to their cumulative weights, as shown in Fig. 2. For an approved transaction, its cumulative weight gradually increases to reach a predefined threshold. Finally, the corresponding transaction is considered confirmed and permanently recorded in the ledger.

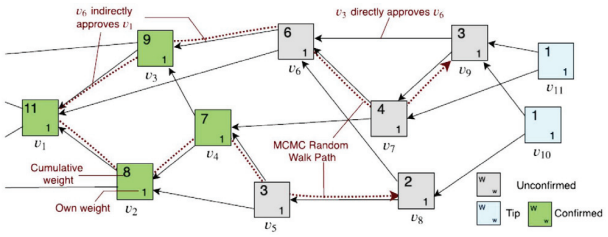

Fig. 2. IOTA tangle instance.

The process can be outlined as follows:

- The freshly issued transaction is signed with one of the private keys of the IoT device.
- This transaction is linked to two previous transactions to be part of the Tangle and later be validated. The process is called "tip selection", to select two unconfirmed nodes to be linked to this transaction using a Markov Chain Monte Carlo algorithm(MCMC). This selection is based on weight and depth of node in the graph.
- Once the two previous graph nodes are selected, the issuing device of the transaction needs to do a small proof-of-work to be able to insert his transaction in the list of pending ones.
- The transaction is broadcasted to the network to be validated and to be part of a further transaction.

III. DAG DLT Principles and Realization

A. IOTA Consensus

In traditional consensus protocols the leader node solves a given computational puzzle the fastest; this winner adds a new block to the blockchain. While the blockchain is not allowed to contain two conflicting transactions, the IOTA tangle may temporarily contain such transactions. The tangle uses a consensus protocol to decide on conflicting transactions. The fast probabilistic consensus (FPC) specifies that majority

voting is engaged so that to reach a required threshold of confidence, formally, at each step, each node chooses k random nodes C_i, queries their opinions and calculates the mean opinion.

It is important that at each round a node queries a different random set of nodes. In a decentralized system, global ordering of device or machine data, requires special consideration. If two or more machines need to agree on the order of events or data observed things get tricky and complex very quickly. This is where consensus mechanisms come into play, mechanisms to agree on the order of events so that the interpretation of them becomes consistent. All the sensor readings formed in zero-value transactions are registered in a nicely ordered data structure. IOTA ensures that transactions inside the ledger store the events of a domain in an ordered manner, without even knowing the data yet. We use IOTA's data layer to register end-devices generated data, without using the value (monetary) layer.

B. IOTA Implementation

The consensus in IOTA utilizes the Proof-of-Work (PoW) principle to enable immutability of transactions. In IOTA realization, a new transaction must select two previous unapproved transactions (called tips) to approve according to a tip selection algorithm before adding to the Tangle. Each device that creates a transaction must include a nonce value in the appropriate transaction field. This causes the hash of the whole transaction to result in a digest with a pre-defined number of 0-value trits (in a balanced trinary numerical system a Trinary Digit, or trit has values -1, 0 and 1). The number of 0-value trits that a resulting transaction hash digest should have is called the MWM [32]. For instance, if we select a MWM of 14 for a transaction, that means that the device must cycle through nonce values using a trial and error methodology and find a value that results in the hash of the transaction containing at least 14 leading 0-value trits.

In this work, we have set up a private Tangle network and configured it with a MWM of 9. Our implementation is based on the IOTA Foundation One-Command Tangle [33], a docker container which includes an IOTA Reference Implementation (IRI) of a Full Node and a Coordinator (nicknamed Compass) developed by the IOTA Foundation. An IOTA Light Node device can be configured to calculate the Proof of Work either locally or on a remote server, called Full Node. The current implementation of the Full Node released by the IOTA Foundation contains API calls that allows Light Nodes to delegate this process to the Full Node. In this work, we present an evaluation for both local PoW conducted on the STM32F746G-Disco board [34] as well as remote PoW, conducted by the Full Node, a Linux workstation featuring an Intel i7 3700K CPU.

The IOTA Light Node application is developed in the C programming language using the STM32CubeIDE and runs on the STM32F746G-Disco [34] board. The current implementation on STM32F746G-Disco board features (i) an ARM-Cortex M7 CPU clocked at 216 MHz, (ii) 1024 KB of programmable flash memory, (iii) 340 KB of RAM, (iv) 10M/100M Ethernet Port (v) 12-bit resolution ADC with support for reading the temperature of the on-board CPU, (vi) 96-bit read-only, OEM-preinstalled, STM-specific Unique Identifier, (vii) true-RNG peripheral

The application reads the temperature sensor data from the on-board CPU (ARM Cortex-M7-core) and sends it to an IOTA Full Node provider where a private Tangle is setup. The IOTA full node (IOTA Reference Implementation, called IRI) server is based on nodejs implementation. The standard node API is used to get transactions from the Tangle, get a node's neighbors, or send new transactions; this API accepts HTTP requests and responds with JSON data. Figure 3 shows the steps of the application when conducting Proof-of-Work (PoW) remotely on the Full Node. In local Proof-of-Work only step 11 changes, where PoW is calculated on the IOTA Light Node. The IOTA uses a ternary logic which has three states -1,0,1 instead of two states of a binary system.

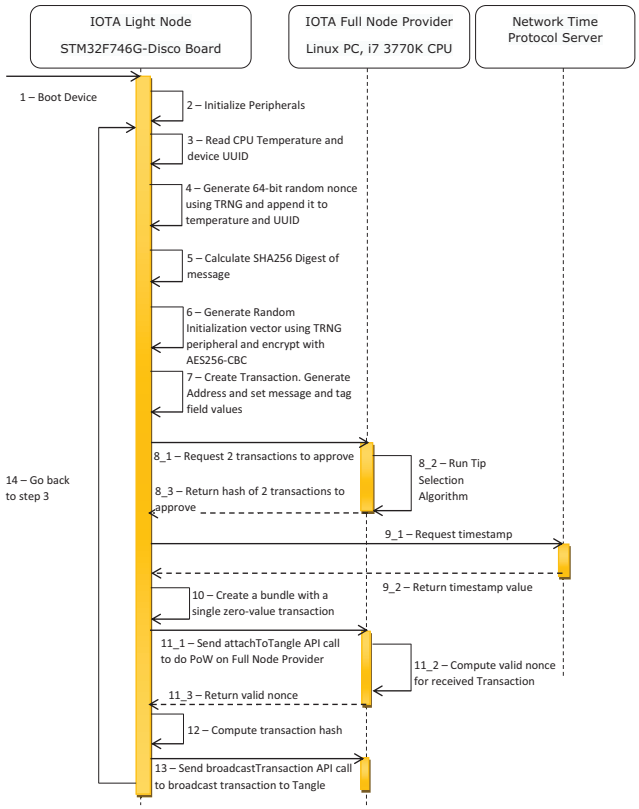

Fig. 3. IOTA Light Node transaction creation sequence flow. Remote Proof of Work is computed by the Full Node Provider. The Network Time protocol is invoked only periodically (step 9) to update the local time/counter inside the STM32F746G device.

Masked Authenticated Messaging that enables authentication of node transactions is not developed in RTOS environment, appropriate for our STM32 light node. Hence, for efficiency, to address authenticity and integrity of transactions we incorporated the X-CUBE-IOTA1 firmware package and

extended it to allow for a custom implementation of a Hashed Message Authenticated Code (HMAC-SHA256[3]) scheme. The STM32F746G-DISCO TRNG peripheral generates the random salt/nonce for the hashing and the 16 bytes of the Initialization Vector for the AES-256-CBC (NIST SP 800-38A standard) encryption. This allows for cryptographically secure random number generation based on environmental noise, which is considerably harder for malicious attackers to breach [35].

Finally, we reserved a sector of the Flash memory for the STM32 device unique indentifier. We exploit Readout Protection (RDP), a security feature that allows to protect the embedded firmware against copy, reverse engineering or dumping using debug tools or code injection in RAM (with level=2).

IV. Evaluation

In this section we investigate the IOTA realization by using the STM32F46G device with respect to the internal latency and to end-to-end performance and provide a glimpse to its scalability attributes. The latency of the application to collect the CPU temperature, to create a data transaction and to store it on the Tangle depends mainly of the selected Minimum Weight Magnitude value and of the method to compute the PoW (local or remote).

A. IOTA Transaction Performance Analysis

A breakdown of the main software functions reveals the computation intensive components for each method. These functions include: (i) the MAC (SHA256 hashing and AES256 encryption of the digest), (ii) IOTA address generation, (iii) all binary/ternary conversions, (iv) TSA, the time needed to run Tip Selection Algorithm on the Full Node, (v) the time needed to create a bundle, (vi) Proof of Work computation, (vii) the computation of the transaction hash by using the hashing function Curl-P-81, (viii) broadcasting of the final bundle (consisting of the single zero-value transaction), (ix) other operations required (memory copies, memory allocations, etc).

The Full Node platform handling the remote PoW is an Intel i7 3770K CPU-based workstation running on a Linux Debian OS version 10. This platform also stores the Tangle Ledger. Figures 4 and 5 show and analyze the main computation effort required for a transaction when employing local and remote PoW with MWM 9 and 14. As shown, an IOTA Light Node application on the STM32F746G can complete a transaction and send it to the Tangle when conducting the PoW locally and using a MWM value of 9 within 4.407 seconds, which translates to about 0.227 maximum transactions per second. However, by increasing the computation difficulty (i.e., MWM=14) makes it very challenging for local realization on a STM32F46G device, since it exhausts such a device in terms of computation and energy. However, for an industrial network which largely relies on low-bandwidth channels for communication among lightweight devices, the execution of local PoW with MWM=9 appears to be a promising option.

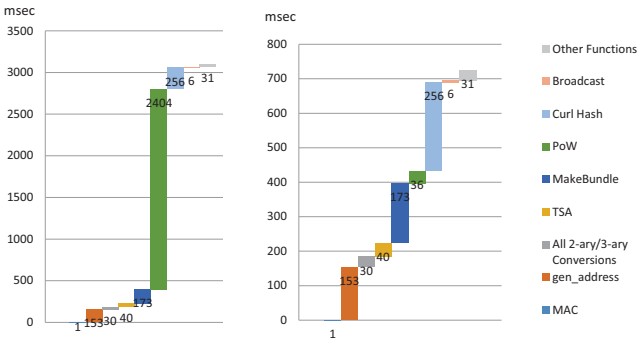

Fig. 4. Latency breakdown of the IOTA Light Node Application with MAC running on STM32F746G-Disco - Remote Proof of Work with MWM 14(left) and MWM 9 (right).

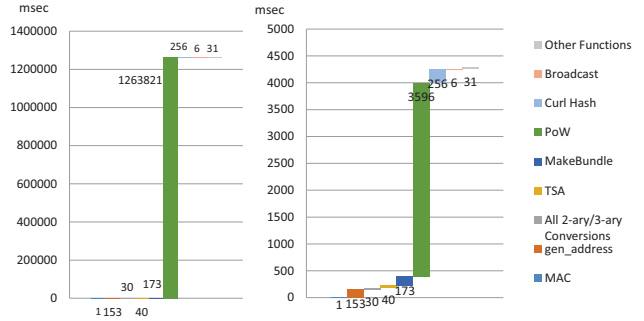

Fig. 5. Latency breakdown of the IOTA Light Node Application with MAC running on STM32F746G-Disco - Local Proof of Work with MWM 14 (left) and MWM 9 (right).

B. Scalability Evaluation

To investigate the metrics of transaction speed and scalability, we design a load testing method that consists of sending and receiving parts. As shown in figure 6, for sending component we set each sending light node or sender to intensively send transactions in every short time interval such as 1, 2 seconds (and then increasing) depending on the difficulty of proof of work, i.e., the MWM. All these transactions are broadcast to all nodes through TCP. We control the transaction sending rate by controlling the individual transaction rate and the number of senders during a test time window. Verification tests include queries to the Tangle in the form: iota.findTransactionObjects({tags:['TempSENSOR']}) to get all transactions with a tag containing the passed queryTag argument, such as the 'TempSENSOR'. The latest transaction can be queried with no more than 2 msec latency, while an older one requires almost 1 sec for 6K transactions.

In figure 6, it should be noted that the Coordinator is a special node operated by the IOTA foundation which periodically pings the tangle by executing zero-value transactions known as *milestones* which performs a checkpoint function

[3]NIST FIPS PUB 180-4 standard, also in SP 800-57 Part 1, section 5.6.2 and SP 800-131A, [online https://csrc.nist.gov/News/2019/NIST-Publishes-SP-800-131A-Rev-2]

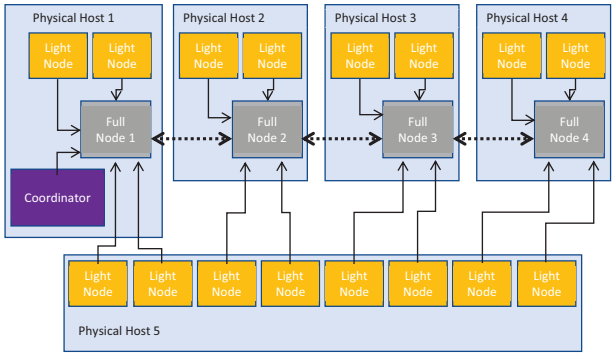

Fig. 6. Organization of multiple docker-based light and full nodes for evaluating scaling of continuous transaction generation with MWM=9.

on the Tangle to determine the state of the tangle and as well validating transactions in the process. IOTA foundation considers the Coordinator as a temporary solution.

Figure 7 shows the mean transactions per second for scaling number of light nodes and of full nodes for MWM equal to 9 for a 15 min time window. The transaction speed TPS increases almost linearly. Hence, with IOTA, as the transaction rate increases, scalability also increases i.e. the more end-devices (subscribers) and transactions the system has, the faster it gets. As shown in figure 7, the achieved throughput

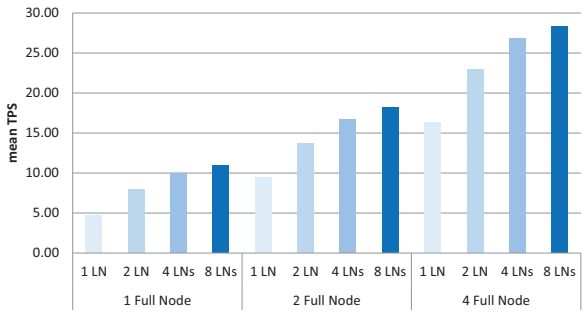

Fig. 7. Scalability results when 1-to-8 light nodes (LNs) generate transactions connected to 1-upto-4 full nodes; the physical host 5 is an i7 3770K Debian and the rest hosts are i5 Centos-based systems.

demonstrates that this realization is an effective solution in smart manufacturing with LPWAN solutions [36], since in LoRaWAN deployments the average end-to-end latency is almost 1 sec for wireline gateway connection and $<$10 sec for 3/4G connection [37].

V. Security Analysis

A *Sybil attack* is a malicious attack on a peer-to-peer network in which a person or organization attempts to take over the network by using multiple identities to control multiple accounts or nodes. For example, she can create counterfeit identities in order to have a larger weight in a voting protocol or overcome the access control mechanism. The tangle primarily ensures that the consensus result makes the right decisions when two conflicting transactions are voted on, so that to create a system that can distinguish trusted nodes from new and thus possibly malicious nodes. IOTA adopts a Sybil protection mechanism based on *mana* that is regarded as a hard to obtain resource as well as a form of a reputation, which can be assigned to trustworthy nodes. Mana is credited as part of regular transactions and nodes need not always use their account's private keys to sign. Besides, IOTA uses an autopeering mechanism to make new nodes easily join the network and avoid an attacker targeting specific nodes during the peering process. Essentially, emerging mechanisms in IOTA develops towards the philosophy in which good behaviors get rewards, while harmful ones are penalized[4].

Stability in IOTA tangle is guaranteed by the Coordinator, (or the set of trusted nodes in the future), who takes care of keeping the tangle "in-the-box" and hindering disagreement in consensus, so that no mesh forking happens. In principle, the employed method actually allows milestones to set the "full nodes" (computers that take care of validating transactions) to the validation direction and to starve old transactions that would allow the tangle to grow in the wrong direction. In addition, careful selection of parameters of MCMC walk in IOTA can subvert parasite chain attacks [38], in which an adversary secretely creates a subgraph offline and occasionally references the main graph to obtain a high weight and confidence. A model-based detection mechanism against this attack in IOTA is also developed [39].

A denial of service (DoS) attack is a method used to disrupt legitimate users access to a target network or a certain resource. This is typically done by overloading the target with a massive amount of traffic. To address such challenge, cross-chain solutions have been proposed [40], where smart contracts on the consortium blockchain prevent requesters from launching denial of service (DoS) attacks by flooding the services with many unauthorized requests. In principle, the complexity of PoW greatly lower the chance of denial of service (DoS) attacks and increase the difficulty of cheating (e.g., double spend), while at the same time, PoW leads to huge consumption of energy and limits the scalability of the system. The speed of PoW calculation becomes the bottleneck when a large number of pending blocks need to be added quickly. Although the difficulty of PoW in IOTA has already been largely reduced, it can still be infeasible for a constrained device to directly finish a PoW task. Thus, a recommended practice of using IOTA in IoT is for constrained devices to delegate the PoW calculation to a dedicated powerfull node, as in our solution. Regarding access to network servers, past works develop an effective scheme and presented two new mechanisms to find DDoS attacks by evaluating the distance values and traffic rates [41].

Last but not least, DLT solutions essentially enable immutable record-keeping, providing traceability, transparency, and at the same time, ensuring privacy within its operations, which are built upon a consensus mechanism. The authenticity

[4]https://blog.iota.org/identities-and-sybil-protection-in-iota-9c62916ff374/

of the information in the chain is established and validated by most nodes before being encrypted into the blocks. However, most of the existing research considers information from objective sources, while actually the information may originate from subjective sources. On the contrary, in our approach we use unique device ID combined in each transaction to validate the authenticity of the source information.

VI. Conclusions

In the era of smart and connected networks of manufacturing things (e.g., materials, sensors, equipment, people, products, and supply chain), mechanisms are required to ensure secure communication in IIoT environments. Smart factories which integrate many cutting-edge technologies and sophisticated machines/robots that often change operating procedures to meet ever changing requirements of market and customers, transparent and efficient tracking of various programs, software versions, simulation results, e.g. in digital twins, history of changes (within various operating procedures) etc. represent a big challenge. As distributed ledger technology has matured to receive more and more attention, its performance problems (e.g., low throughput and high latency) in IoT-based solutions in industrial domain are critical. To resolve these issues, even though improvements by new efficient consensus protocols exist, these improvements are hardly applicable in IoT environments. In this paper, we presented and evaluated a meaningful implementation with IOTA DLT technology with STM32 devices as transaction-issuers to demonstrate its performance advantages with zero-value (data) transactions. We also added an authorization level to authenticate transactions with the unique identifier of the device and HMAC signing. Future research paths include evaluating additional devices with hardware accelerators for hashing and encryption, as well as integration with various LPWAN solutions.

Acknowledgment

The research leading to these results received funding from the European Union (EU) project Horizon 2020 project AVANGARD (advanced manufacturing solutions tightly aligned with business needs) under grant agreement No. 869986.

References

[1] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on iiot and its countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 2018, pp. 124–130.

[2] A. Bahga and V. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 09, pp. 533–546, 2016.

[3] NIST, "Recommendations for iot device manufacturers: Foundational activities and core device cybersecurity capability baseline," Draft (2nd) NISTIR 8259. Washington, DC: US Department of Commerce, 2020.

[4] B. He and K.-J. Bai, "Digital twin-based sustainable intelligent manufacturing: a review," *Advances in Manufacturing*, vol. 9, pp. 1–21, 2021.

[5] W. Viriyasitavat, L. D. Xu, Z. Bi, and V. Pungpapong, "Blockchain and internet of things for modern business process in digital economy?the state of the art," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1420–1432, 2019.

[6] G. Kornaros, E. Wozniak, O. Horst, N. Koch, C. Prehofer, A. Rigo, and M. Coppola, "Secure and trusted open cps platforms," in *Solutions for Cyber-Physical Systems Ubiquity*, N. Druml, A. Genser, A. Krieg, M. Menghin, and A. Hoeller, Eds. Hershey, PA United States: IGI Global, 2018, ch. 12, pp. 301–324. [Online]. Available: doi:10.4018/978-1-5225-2845-6.ch012

[7] G. Kornaros, D. Bakoyiannis, O. Tomoutzoglou, M. Coppola, and G. Gherardi, "Trustnet: Ensuring normal-world and trusted-world can-bus networking," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–6.

[8] D. Mbakoyiannis, O. Tomoutzoglou, and G. Kornaros, "Secure over-the-air firmware updating for automotive electronic control units," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '19, 2019, pp. 174–181. [Online]. Available: https://doi.org/10.1145/3297280.3297299

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[10] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[11] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

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

[13] Industrial Internet Consortium, "The industrial internet of things: Managing and assessing trustworthiness for iiot in practice," https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf, 2019.

[14] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, "Trade-offs between distributed ledger technology characteristics," *ACM Comput. Surv.*, vol. 53, no. 2, May 2020. [Online]. Available: https://doi.org/10.1145/3379463

[15] S. Popov, "On the tangle, white papers, proofs, airplanes, and local modifiers," https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf, 2018.

[16] C. Yu, X. Jiang, S. Yu, and C. Yang, "Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation," *Robotics and Computer-Integrated Manufacturing*, vol. 64, p. 101931, 2020.

[17] D. Stucchi, R. Susella, P. Fragneto, and B. Rossi, "Secure and effective implementation of an IOTA light node using STM32," in *Proceedings of the 2nd Workshop on Blockchain-Enabled Networked Sensor*, ser. BlockSys'19, 2019, pp. 28–29.

[18] F. Shahid and A. Khan, "Smart digital signatures (SDS): A post-quantum digital signature scheme for distributed ledgers," *Future Generation Computer Systems*, vol. 111, pp. 241 – 253, 2020.

[19] T. Alsboui, L. Qin, R. Hill, and H. Al-Aqrabi, "Enabling distributed intelligence for the internet of things with iota and mobile agents," *Computing (Vienna/New York)*, vol. 102, no. 6, pp. 1345–1363, Jun. 2020.

[20] M. Bhandary, M. Parmar, and D. Ambawade, "A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 827–832.

[21] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, p. 6267, Mar. 2012.

[22] H. C. Hwang, J. Park, and J. G. Shon, "Design and implementation of a reliable message transmission system based on MQTT protocol in IoT," *Wirel. Pers. Commun.*, vol. 91, no. 4, pp. 1765–1777, Dec. 2016.

[23] R. Godfrey, D. Ingham, and R. Schloming, "OASIS Advanced Message Queuing Protocol (AMQP)," http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-messaging-v1.0.html, 2012, version 1.0, OASIS Standard.

[24] P. Saint-Andre, "Extensible messaging and presence protocol (xmpp): Core," Internet Eng. Task Force, Fremont, CA, USA, RFC 6121, 2011.

[25] S. Faltinski, O. Niggemann, N. Moriz, and A. Mankowski, "Automationml: From data exchange to system planning and simulation," in

2012 IEEE International Conference on Industrial Technology, 2012, pp. 378–383.

[26] S. Grner, J. Pfrommer, and F. Palm, "RESTful industrial communication with OPC UA," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1832–1841, 2016.

[27] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Comput. Surv.*, vol. 51, no. 6, Jan. 2019.

[28] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam, "Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges," *IEEE Access*, vol. 8, pp. 17 179–17 220, 2020.

[29] M. Coppola and G. Kornaros, "Automation for industry 4.0 by using secure lorawan edge gateways," in *Multi-Processor System-on-Chip, vol. 2.*, L. Andrade and F. Rousseau, Eds. ISTE Ltd, London, and Wiley, New York, 2021, ch. 3, pp. 49–66. [Online]. Available: https://iste.co.uk/book.php?id=1739

[30] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Delay and communication tradeoffs for blockchain systems with lightweight IoT clients," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2354–2365, 2019.

[31] R. Xie, Y. Wang, M. Tan, W. Zhu, Z. Yang, J. Wu, and G. Jeon, "Ethereum-blockchain-based technology of decentralized smart contract certificate system," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 44–50, 2020.

[32] IOTA Foundation, "Minimum weight magnitude in iota," https://docs.iota.org/docs/getting-started/0.1/network/minimum-weight-magnitude, 2020, online; accessed 09 June 2020.

[33] IOTA Foundation , "One-command tangle," https://docs.iota.org/docs/compass/1.0/tutorials/set-up-one-command, 2020, online; accessed 09 June 2020.

[34] STM, "STM32F746G-Disco Development Board," www.st.com/en/evaluation-tools/32f746gdiscovery.html, 2020, online; accessed 09 June 2020.

[35] STM , "AN4230, STM32 microcontroller random number generation validation using the NIST statistical test suite," https://www.st.com/resource/en/application_note/dm00073853-stm32-microcontroller-random-number-generation-validation-using-the-nist-statistical-test-suite-stmicroelectronics.pdf, 2020.

[36] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *ICT Express*, vol. 3, no. 1, pp. 14 – 21, 2017.

[37] A. Ptsch and F. Hammer, "Towards end-to-end latency of lorawan: Experimental analysis and iiot applicability," in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2019, pp. 1–4.

[38] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "SoK: Diving into dag-based blockchain systems," 2020. [Online]. Available: arXiv:2012.06128

[39] A. Penzkofer, B. Kusmierz, A. Capossele, W. Sanders, and O. Saa, "Parasite chain detection in the iota protocol," in *Tokenomics 2nd Conference*, 2020. [Online]. Available: arxiv.org/abs/2004.13409

[40] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A cross-chain solution to integrating multiple blockchains for iot data management," *Sensors*, vol. 19, no. 9, p. 2042, 2019.

[41] Y. You, M. Zulkernine, and A. Haque, "Detecting flooding-based ddos attacks," in *IEEE Int. Conf. Commun*, 2007, pp. 1229–1234.