Applying Distributed Ledger Technology to Facilitate IIoT Data Exchange: An Approach Based on IOTA Tangle

Xiaochen Zheng, Shengjing Sun, Joaquín Ordieres-Meré, Jinzhi Lu, and Dimitris Kiritsis

Abstract Data interoperability is a fundamental dimension in enterprise interoperability. The interoperability of data is concerned with exchanging information coming from heterogeneous sources among different partners. Under the Industry 4.0 context, Internet of Things (IoT) technology has been widely implemented in manufacturing factories which enables the concept of smart factory. The huge amount of Industrial IoT (IIoT) devices are generating large volume of data related to all aspects of the enterprise. The free exchange of these big IIoT data is crucial to enterprise interoperability. However, in practice, the overwhelming part of the industrial data remains siloed preventing the full use of the big IIoT data. Concerns about data security and privacy bring more obstacles to industrial data sharing. With the decentralized and consensus-driven characteristics, distributed ledger technologies (DLT), represented by blockchain, provide reliable solutions to improving enterprise interoperability. This paper explores the application of IOTA in IIoT data exchange. IOTA is a tangle-based distributed ledger designed specifically for the IoT applications. A prototype data exchange system is developed based on IOTA and its data communication protocol, masked authenticated messaging (MAM), to demonstrate the feasibility of the proposed approach.

Keywords Data interoperability · Industrial IoT · Distributed ledger technologies · Blockchain · IOTA tangle · Masked authenticated message

1 Introduction

For a modern enterprise, the ability to interoperate with partners from inside or outside is not only a quality and advantage for gaining competitiveness in the market but also becoming a question of survival [1]. According to the definition of IEEE [2],

X. Zheng (✉) · S. Sun · J. Ordieres-Meré
ETSII, Universidad Politécnica de Madrid, José Gutiérrez Abascal 2, 28006 Madrid, Spain
e-mail: xiaochen.zheng@epfl.ch

X. Zheng · J. Lu · D. Kiritsis
Institute of Mechanical Engineering, EPFL, 1015 Lausanne, Switzerland

B. Archimède et al. (eds.), *Enterprise Interoperability IX*, Proceedings of the I-ESA Conferences 10, https://doi.org/10.1007/978-3-030-90387-9_6

"interoperability" means the ability for two (or more) systems or components to exchange information and to use the information that has been exchanged. IDEAS defined "enterprise interoperability" as the ability of interaction between enterprises which is achieved if the interaction can, at least, take place at three levels: data, application, and business process [3]. Enterprise interoperability makes possible of two or more enterprises (of the same organization or from different organizations and irrespective of their location) with the ability of exchanging or sharing information (wherever it is and at any time) and using functionality of one another in a distributed and heterogeneous environment [4].

The interoperations among enterprises can happen from various levels such as data interoperation, service or organization interoperation, information system (IS) or IT application interoperation, processes interoperation, and business interoperation [4, 5]. They either concern the internal business processes and services of a given enterprise or cross-organizational business processes spanning partner companies or flowing across enterprise networks. The various viewpoints of enterprise interoperations are as shown in Fig. 1 which is adapted from previous studies [4, 5].

Data interoperability is the fundamental dimension for achieving higher level and enterprise interoperability. With the wide deployment of IIoT devices, huge amount of data related to different aspects of an enterprise have been generated every moment. The efficient interoperation of these IIoT data is crucial to implement the concept of smart factory. However, in practical applications, there are many barriers preventing successful data interoperability among enterprises such as different semantics and syntax to represent information, different database technologies, and strict data management policies.

Concerns about data security/privacy issues are making data protection regulations stricter. For instance, the European Union published the General Data Protection Regulation (GDPR) [6] to protect private data which will further impede data sharing. The absence of certified authenticity and audit mechanisms during data exchange may also make data owners hesitate to share data freely. Different type of attacks, such as

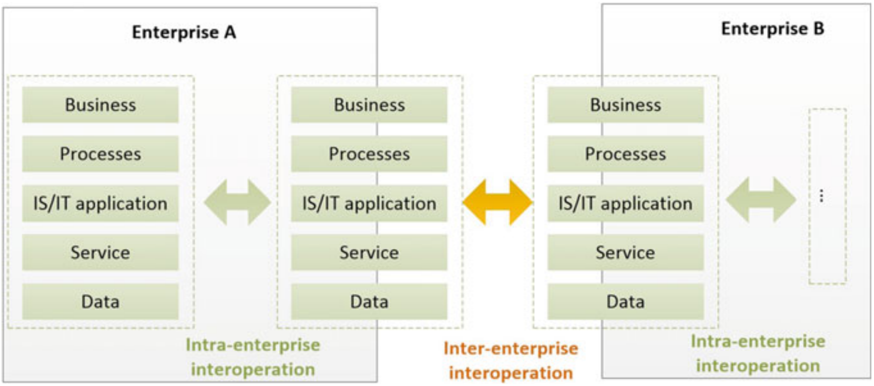


Fig. 1 Enterprise interoperation levels (based on previous studies [4, 5])

"man-in-the-middle" attacks and data tampering, can also occur when sharing data using traditional protocols and databases [7]. For industrial application scenarios, the IIoT data are usually with high frequency and require real-time exchange. Therefore, the exchange process needs to be very cheap or even totally free, which is difficult to realize using traditional technologies [8].

To address above-mentioned concerns, innovative methods are needed to establish data access policies among arbitrary parties, accommodating new participants and request types dynamically [9]. The repaid development of distributed ledger technologies (DLT) provides a possible solution to this challenge. A distributed ledger is a distributed database, maintained by a consensus protocol run by nodes in a peer-to-peer network without any central administrator [10]. Blockchain has been one of the most popular DLT in recent years due to the success of cryptocurrencies in financial field like Bitcoin [11]. Blockchain technology has been applied to variety of domains and gained mainstream attention due to some unique features, such as decentralized control, high anonymity, and distributed consensus mechanisms [12–14]. The adoption of blockchain in a data sharing system could enable better data control and makes possible of fine-grained tracking of different data usages [15].

Although many studies and projects have proved the practical value of blockchain technologies like cryptographic currencies [11] and smart contracts [16], these protocols still have various limitations that make them inadequate for IIoT data sharing.

- **Scalability** Transaction rate, i.e., the number of transactions processed per second over the whole network of a blockchain has an inherent limit, because all transactions must be attached to the longest chain causing the "blockchain bottleneck" issue [17]. For example, it has to wait up to six blocks for a transaction to be approved before reaching a high level of confidence on the Bitcoin network [15, 18]. The transaction rate of Bitcoin protocol has been lower than six transactions per second in the whole network during most of the time in the year 2019 [19]. Similarly, the Ethereum protocol processed about ten transactions per second across the entire network even after the upgrade in 2019 [20]. This low transaction rate is far away the requirements of industrial machine-to-machine data exchange scenarios.
- **Transaction Fees** The transaction fees, no matter the value of the transaction itself, is another main drawback when applying blockchain in industrial scenarios. For example, the Bitcoin protocol requires a fee that may exceed $0.30 for each transaction according to the latest statistics [21]. Currently, it is impossible to remove these fees in the blockchain platform as they provide motivations for the creators of blocks [22]. These high transaction fees make no sense for the high-frequency data exchange in IIoT environment. It is highly possible that the transaction fee is higher than the value being transferred which makes no sense.
- **Centralization** Blockchain is designed to be decentralized, but a lot of computing power is required to create blocks. In practical, large part of the mining power has been controlled by some mining pools making blockchain centralized to some extent. The latest statistic shows that the seven largest mining pools control 77.1%

of the of the network's mining power (F2Pool 17.3%, Poolin 15.1% BTC.com 13.8%, AntPool 9.7%, ViaBTC 7.4%, BTC.TOP 6.3%, SlushPool 4.3%, BitFury 3.2%) [23].

- **Vulnerable to Quantum attack** Quantum computing, although still a hypothetical construct currently, has been proved feasible. A quantum computer is supposed to be supper efficient for solving problems that depend on trial and error to find a solution [22]. Blockchains that are based on proof-of-work, such as Bitcoin, are vulnerable to quantum computing attacks. Theoretically, a quantum computer could be billions of times more efficient than a classical computer when mining the Bitcoin blocks [24], which would enable it to control over 51% of computing power of the whole network and possible to breakdown the entire network.

In order to take the advantages of Blockchain technology and meanwhile overcome the above-mentioned limitations, a new DLT is needed. In this paper, we adopt a tangle-based DLT paradigm which is designed specifically for the IoT industry, named IOTA, to facilitate the IIoT data exchange among different stakeholders.

The rest of this paper is organized as follows. Section 2 introduces the methodology we used. An application framework is developed, and some main enabling technologies are explained. A prototype system is demonstrated, and an exemplary experiment is conducted in Sect. 3. The conclusion of this paper and the future work are introduced in Sect. 4.

2 Methodology

The efficient data interoperation among different IoT environments require frequent and automatic machine-to-machine data exchange system. Conventional blockchain protocols like Bitcoin blockchain and Ethereum smart contract cannot fulfill the requirements of IIoT data interoperation scenarios due to the limitations mentioned in previous sections.

In this paper, we utilized a tangle-based DLT protocol which is specifically designed for the industrial data exchange scenarios, named IOTA. It succeeds the advantages of blockchain and at the meantime overcomes some of its fundamental limitations [25]. The tangle uses a directed acyclic graph (DAG) for storing transactions instead of sequential blocks. To issue a new transaction in the tangle, users must perform a small amount of computational work to approve two previous transactions, and this new transaction will be validated by some subsequent transactions [22]. This structure allows high scalability as more transactions joined in the tangle, the faster transactions can be approved. Moreover, financial rewards can be eliminated owing to the unique validation method enabling completely fee-free transactions with IOTA. This is extremely important for IIoT data interoperability. Furthermore, no miners exist in IOTA tangle; therefore, it is truly decentralized.

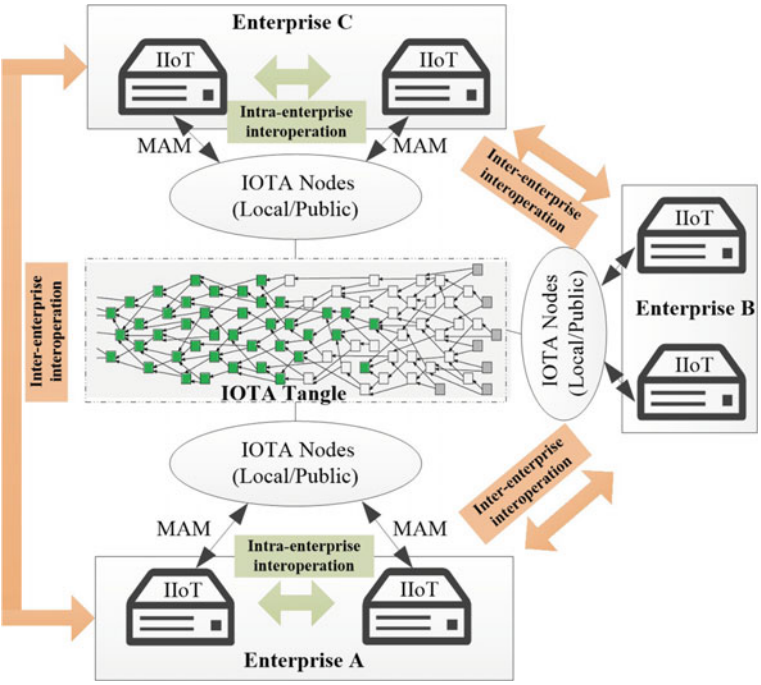

Enterprise C
IIoT
IIoT
Intra-enterprise interoperation
MAM
MAM
IOTA Nodes (Local/Public)
Inter-enterprise interoperation
Inter-enterprise interoperation
IOTA Tangle
IOTA Nodes (Local/Public)
IIoT
Enterprise B
IIoT
IOTA Nodes (Local/Public)
Inter-enterprise interoperation
MAM
MAM
Intra-enterprise interoperation
IIoT
IIoT
Enterprise A

Fig. 2 Intra-enterprise and inter-enterprise IIoT data exchange framework based on the IOTA tangle and MAM protocol

As shown in Fig. 2, a framework for intra-enterprise and inter-enterprise IIoT data interoperation is proposed based on the IOTA tangle and some relevant enabling technologies. In this framework, IIoT data are interchanged between data publishers and data subscribers. Any device with basic computing capability and access to the internet, like a computer, a smartphone, single-board computer, or any IoT device connected to a gateway, can be a data publisher or subscriber. A data publisher or subscriber can be from inside an enterprise for intra-enterprise interoperation, or from another enterprise for inter-enterprise interoperation. A data publisher can publish different kind of data to the tangle using different encryption and privacy protocols, which will be explained in the following section. The data are published in their own channels, and each channel has an address. The subscribers of a data channel will receive the new published data. The published data could be encrypted in which case an extra decryption key will be required to decrypt the received message. In the tangle, the data publishing and receiving are processed through IOTA nodes. A node can be a computer or server connected to the IOTA network. Users could configure their own local nodes or use public nodes. A user can be a data publisher or a subscriber or both at the same time.

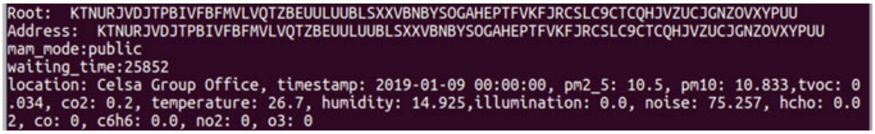
Another key-enabling tool for the proposed framework is a data communication protocol of IOTA, named masked authenticated messaging (MAM). It supports publishing and receiving an encrypted data stream over the tangle regardless of the size or cost of device [26]. MAM uses channels for data distribution which works similar to the radio broadcasting. Data publishers can create a channel with a unique address and publish a message at any time. In order to spread the message through the network and prevent spamming, the node publishing the message needs to conduct a small amount of proof-of-work. The users who are interested in this message can subscribe this channel with the address and receive the message. Merkle hash tree (MHT) is adopted as the signature scheme in the MAM protocol to encrypt the message [26]. The address of a channel is the root of this MHT which itself is created using the unique identification of the user. More details about the signature scheme have been introduced in our previous work [27].

MAM supports three privacy and encryption modes, i.e., public, restricted, and private, to control the access to a channel [26]. In public mode, the root of the MHT is used directly as the address of the MAM channel and the key to decode the message. Any user who knows the address, even randomly, will be able to decode and consume the message. In private mode, the hash of the MHT root is used as the address of the channel, while the message is encrypted using the root. In this mode, only the publisher can decode and consume the message. In restricted mode, an authorization key is added based on private mode. The address of the channel is the hash of the key and the root. In this mode, subscribers of the channel can receive the encrypted message with the channel address and decrypt it with the authorization key. The restricted mode is the most commonly used for IIoT data exchange because it enables a message publisher to revoke access to future messages from subscribers by changing the authorization key without changing the channel address.

3 Prototype and Experiment

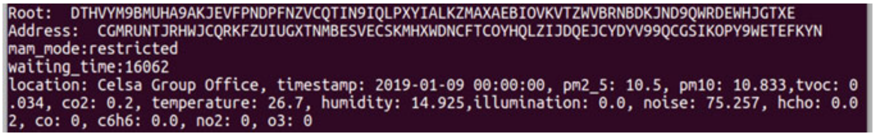
In order to verify the feasibility of the proposed framework and explore the implementation process in reality, a prototype system has been developed. The MAM-enabled data publishing and receiving functions were realized based on the JavaScript library provided by the IOTA foundation (https://github.com/iotaledger/mam.client.js) which is open available. More technical details about publishing and receiving data over the tangle using MAM are introduced in our previous work [27], and the complete JavaScript codes are available online and ready to be reused (https://github.com/zhengxiaochen/iota_mam_data_sharing).

A series of experiments have been conducted using the prototype system to publish and receive sensor data collected from different IIoT devices. For example, one of the experiments focused on the environmental quality data interoperation within a steel manufacturing factory. Figures 3 and 4 show two examples of published messages using public and restricted MAM mode, respectively. In public mode, the address of the message (second line) is the same as the MHT root (first line), as shown in Fig. 3; while in restricted mode, the message address is the hash of the MHT root, which is different from the address, as shown in Fig. 4. Data consumers must know both the



```
Root:  KTNURJVDJTPBIVFBFMVLVQTZBEUULUUBLSXXVBNBYSOGAHEPTFVKFJRCSLC9CTCQHJVZUCJGNZOVXYPUU
Address:  KTNURJVDJTPBIVFBFMVLVQTZBEUULUUBLSXXVBNBYSOGAHEPTFVKFJRCSLC9CTCQHJVZUCJGNZOVXYPUU
mam_mode:public
waiting_time:25852
location: Celsa Group Office, timestamp: 2019-01-09 00:00:00, pm2_5: 10.5, pm10: 10.833,tvoc: 0
.034, co2: 0.2, temperature: 26.7, humidity: 14.925,illumination: 0.0, noise: 75.257, hcho: 0.0
2, co: 0, c6h6: 0.0, no2: 0, o3: 0
```

Fig. 3 Sensor data published to the tangle with public MAM mode



```
Root:  DTHVYM9BMUHA9AKJEVFPNDPFNZVCQTIN9IQLPXYIALKZMAXAEBIOVKVTZWVBRNBDKJND9QWRDEWHJGTXE
Address:  CGMRUNTJRHWJCQRKFZUIUGXTNMBESVECSKMHXWDNCFTCOYHQLZIJDQEJCYDYV99QCGSIKOPY9WETEFKYN
mam_mode:restricted
waiting_time:16062
location: Celsa Group Office, timestamp: 2019-01-09 00:00:00, pm2_5: 10.5, pm10: 10.833,tvoc: 0
.034, co2: 0.2, temperature: 26.7, humidity: 14.925,illumination: 0.0, noise: 75.257, hcho: 0.0
2, co: 0, c6h6: 0.0, no2: 0, o3: 0
```

Fig. 4 Sensor data published to the tangle with restricted MAM mode

address to receive the message and the authorization key to decrypt it in restricted mode. If the publisher wants to withdraw the authorization in the future, it can change the authorization key at any time to the new published messages; by doing this, the subscribers without the new authorization key will not be able to decrypt the new message which means they will also lose the access to the future ones. This feature provides the data publisher with granular control over the shared data, which could bring great benefits to the IIoT data exchange and make IOTA distributed ledger outperform traditional block-based ledgers.

4 Discussion

This paper proposed a novel IIoT data interoperation framework utilizing the emerging distributed ledger technology. After analyzing the advantages and limitations of traditional block-based ledgers, we introduced the tangle-based IOTA distributed ledger to address the concerns of enterprise about data security/privacy and the lack of ensured authenticity/audit trails. Designed specifically for the IoT industry, IOTA could provide a scalable, lightweight, and zero-fee secure communication and transaction protocol for IIoT interoperation. A prototype system was developed under the proposed framework to demonstrate the implementation process in practice and to verify the feasibility of the proposed method. Experiment results showed that the proposed system could provide granular access controls to different sensor data by combining public and restricted MAM protocols. The proposed approach could greatly facilitate both intra-enterprise and inter-enterprise data interoperability. It also provides solutions to help handle the big IIoT data generated by numerous IoT devices in Industry 4.0 era and makes possible of the promising smart manufacturing.

Although the current implementation of IOTA is already usable, some limitations still exist. One of the main drawbacks is the presence of the coordinator in the current network, which will be removed in the future. It is introduced temporarily to secure the tangle network by issuing milestone transactions which will refer and approve all trustworthy tractions in the network. However, the existence of coordinator makes the IOTA not fully decentralized as designed and may cause a single-point failure. Another disadvantage of IOTA is that it does not support decentralized applications as the Ethereum smart contracts do. Although this drawback has no major impact on the data exchange application in this study, it limits the wide application of IOTA in other domains.

Currently, IOTA tangle and its MAM protocol are under development and are evolving rapidly. As more nodes are connected to the tangle network and continuous development efforts spent, some of the afore-mentioned limitations of IOTA will be solved and the performance of IOTA tangle is expected to improve greatly soon.

Acknowledgements The authors thank the financial support by the EU Commission within the research projects QU4LITY Digital Reality in Zero Defect Manufacturing (EU H2020 825030) and FACTLOG-Energy-aware Factory Analytics for Process Industries (EU H2020 869951).

References

1. Chen, D., & Daclin, N. (2006). Framework for enterprise interoperability. In *Proceedings of IFAC workshop EI2N: Bordeaux*.
2. Geraci, A., Katki, F., McMonegal, L., et al. (1991). *IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries*. IEEE Press.
3. IDEAS Consortium. (2003). *IDEAS project deliverables (WP1-WP7)*. Public Reports.
4. Vernadat, F. B. (2010). Technical semantic and organizational issues of enterprise interoperability and networking. *Annual Reviews in Control, 34*(1), 139–144.
5. Guglielmina, C., & Berre, A. (2005). *ATHENA, "Project A4"(slide presentation)*. ATHENA Intermediate Audit.
6. Regulation GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ), 59*(1–88), 294.
7. Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security & Privacy, 7*(1), 78–81.
8. Sønstebø, D. *IOTA data marketplace*. https://blog.iota.org/iota-data-marketplace-cb6be463ac7f. Last accessed 2019/11/05.
9. Ordieres-Meré, J., Villalba-Díez, J., & Zheng, X. (2019). Challenges and opportunities for publishing IIoT data in manufacturing as a service business. In *25th international conference on production research manufacturing innovation*. Cyber Physical Manufacturing.
10. Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating health activity data using distributed ledger technologies. *Computational and Structural Biotechnology Journal, 16*, 257–266.
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
12. Böhme, R., Christin, N., Edelman, B., et al. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238.
13. Ali, S. T. (2015). Bitcoin: Perils of an unregulated global P2P currency (transcript of discussion). In *Cambridge international workshop on security protocols*. Springer.

14. Harlev, M. A., Sun Yin, H., & Langenheldt, K. C., et al. (2018). Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning. In: *Proceedings of the 51st Hawaii international conference on system sciences*.
15. Mamoshina, P., Ojomoko, L., Yanovich, Y., et al. (2018). Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget, 9*(5), 5665.
16. Ethereum Foundation. *Decentralized autonomous organization*. https://www.ethereum.org/dao. Last accessed 2019/11/05.
17. IOTA Foundation. *Meet the Tangle*. https://www.iota.org/research/meet-the-tangle. Last accessed 2019/11/05.
18. Bitcoin Wiki. *Confirmation*. https://en.bitcoin.it/wiki/Confirmation. Last accessed 2019/11/05.
19. Transaction Rate. https://www.blockchain.com/en/charts/transactions-per-second. Last accessed 2019/11/05.
20. Ethereum transaction chart. https://etherscan.io/chart/tx. Last accessed 2019/11/05.
21. Bitcoin Avg. *Transaction fee historical chart*. https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y. Last accessed 2019/11/05.
22. Popov, S. (2018). The tangle.
23. Pool Distribution. https://btc.com/stats/pool?pool_mode=year. Last accessed 2019/11/05.
24. Brassard, G., Høyer, P., & Tapp, A. (1998). *Quantum cryptanalysis of hash and claw-free functions*. Springer.
25. IOTA Foundation. *What is IOTA?* https://www.iota.org/get-started/what-is-iota. Last accessed 2019/11/05.
26. Handy, P. *Introducing masked authenticated messaging*. https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e. Last accessed 2019/11/05.
27. Zheng, X., Sun, S., Mukkamala, R. R., et al. (2019). Accelerating health data sharing: A solution based on the Internet of Things and distributed ledger technologies. *Journal of Medical Internet Research, 21*(6), e13583.