Towards a Decentralized Digital Engineering Assets Marketplace: Empowered by Model-based Systems Engineering and Distributed Ledger Technology

Jinzi Lu\(^1\), CSEP, Xiaochen Zheng\(^1\), Zhenchao Hu\(^2\), Huisheng Zhang\(^2\), and Dimitris Kiritsis\(^1\)

\(^1\) SCI STI DK, Ecole Polytechnique Fédrale de Lausanne, Lausanne, 1015, Switzerland
\(^2\) School of Mechanical Engineering, Shanghai Jiaotong University, Shanghai, 200240, China

Model-based Systems Engineering (MBSE) has been widely utilized to formalize system artifacts and facilitate their development throughout the entire lifecycle. During complex system development, MBSE models need to be frequently exchanged across stakeholders. Concerns about data security and tampering using traditional data exchange approaches obstruct the construction of a reliable marketplace for digital assets. The emerging Distributed Ledger Technology (DLT), represented by blockchain, provides a novel solution for this purpose owing to its unique advantages such as tamper-resistant and decentralization. In this paper, we integrate MBSE approaches with DLT aiming to create a decentralized marketplace to facilitate the exchange of digital engineering assets (DEAs). We first define DEAs from perspectives of digital engineering objects, development processes and system architectures. Based on this definition, the Graph-Object-Property-Point-Role-Relationship (GOPPRR) approach is used to formalize the DEAs. Then we propose a framework of a decentralized DEAs marketplace and specify the requirements, based on which we select a Directed Acyclic Graph (DAG) structured DLT solution. As a proof-of-concept, a prototype of the proposed DEAs marketplace is developed and a case study is conducted to verify its feasibility. The experiment results demonstrate that the proposed marketplace facilitates free DEAs exchange with a high level of security, efficiency and decentralization.

Index Terms—Digital Engineering Assets, Model-based Systems Engineering, Distributed Ledger Technology, Blockchain.

I. INTRODUCTION

In the Industry 4.0 era, Internet of Things (IoT) and Cyber-Physical Systems (CPS) are constructed by multidomain physical compositions, networks, control units and computation components. These systems are considered as "system of systems" (SoS). The increasing functionalities bring new challenges for managing complex systems as every composition usually involves various stakeholders working together to develop the system from a SoS perspective\(^1\). During the entire lifecycle, co-design and collaborative design among stakeholders require frequent data exchange to gain insight to analyze, optimize and verify the system. For example, vehicle system engineers need to provide requirements to embedded system engineers in order to obtain the expected embedded systems. Thus, requirements and solutions need to be exchanged across organizations from the initial phase until the prototype is finalized. In these situations, identification of required "digital engineering assets (DEAs)" for each stakeholder is critical to the entire system development. A DEA includes documents, data and models used for information exchange. In different phases of a system lifecycle, different stakeholders may have different data and models as their digital assets. Currently it is still a challenging task to share related asset due to the lack of common understanding of expected digital asset and interoperability of heterogeneous data. The creation of an open and reliable marketplace can accelerate the DEAs exchange.

First, stakeholders exchange DEAs to realize information sharing thus to support co-design and collaborative design. It is not only difficult to identify the contents of stakeholders expected digital assets but also information represented by the digital assets must be correct, verifiable and unambiguous in different ways. In order to coordinate different stakeholders, systems engineering providing sets of standards and approaches are required to define the contents to construct DEAs\(^2\). Moreover, aiming to develop digital asset correctly, model-based systems engineering (MBSE) is proposed to define the contents of digital assets using models\(^3\). MBSE provides standardized specifications for constructing DEAs and defines formal descriptions for system artifacts of entire lifecycle.

Second, complex system development requires information exchange across organizations and lifecycle. Thus digital assets are expected by different stakeholders from different domains and hierarchies (requirement, function, behavior, etc.). However, each domain and hierarchy has specific semantics due to the fact that different domains use different mathematical theories, scopes and methods to implement their specific works\(^4\). Moreover, domain specifications often bring challenges to represent the entire systems using integrated syntax. These specific syntax and semantics lead to heterogeneous data structure which is a big challenge for data integration. Currently, meta-meta modeling approach is proposed to support data integration for DEAs\(^5\). This approach enables to construct domain-specific digital asset based on a high abstract level in order to realize the data integration during DEAs construction.

Third, the exchange of DEA among stakeholders requires an open and reliable marketplace. It is difficult to create such marketplace with traditional centralized approaches due to the concerns about data security and privacy. The stakeholders must trust each other or a third party during the DEAs ex-
change. It creates barriers when multiple partners are involved or the information need to be shared with partners from outside of the network. In recent years, the rapid development of decentralized Distributed Ledger Technologies (DLT), represented by the blockchain technology, provides an innovative tool to facilitate the concept of an open DEAs marketplace. A distributed ledger is considered as a distributed database maintained by a consensus protocol, which is run by nodes in a peer-to-peer network without any central administrator [9]. As the most popular DLT protocol, blockchain was first applied to cryptocurrency systems like Bitcoin [7]. Because of its unique features, such as decentralized control, high anonymity and distributed consensus mechanisms, blockchain has gained attention from both academia and industry. It has been applied to variety of domains such as healthcare data sharing [8], industrial IoT data exchange [9], knowledge trading [10] and energy dealing in smart grid [11] among others. The idea of using blockchain technology to empower the construction of data marketplace has also been proposed in some recent studies which mainly focused on health and industrial data [12], [13].

This study aims to propose a decentralized open DEAs marketplace empowered by MBSE and DLT methodologies to cope with the challenges during DEAs exchange. The rest of the paper is organized as follows. Related works are analyzed in Section II and the research methodology of this study is presented in Section III. The framework, key concepts and functional requirements of the proposed DEAs marketplace are presented in Section IV. Enabling technologies, i.e. MBSE approaches and DLT solutions, are investigated in Section V. A proof-of-concept prototype of the marketplace is introduced based on a case study in Section VI. Conclusions of this paper is presented in Section VII.

II. RELATED WORKS

During digital asset construction and exchange, data interoperability is one challenge to stakeholders across organizations, because of heterogeneous data structure and intellectual property [14], [15]. MBSE has been widely used to construct digital asset [16] and to support interoperability of the entire lifecycle of complex system development [17], [18]. It refers to a systems engineering approach focusing on creating and exploiting domain knowledge as the primary means of information exchange between stakeholders based on models during the entire lifecycle [19]. In Chen et al.’s survey, we find that in the lifecycle of digital asset, the existence of various data format standards is the basis to construct digital asset. MBSE approaches, such as SysML [16], can offer the defined specifications to formalize the system artifacts. Moreover, digital thread is a main approach to manage interoperability between digital twins and traceability between system development process and digital twin assets, because MBSE provides a unified descriptions of multiple domain knowledge and a specification to formalize system architecture views for the complex systems [20]. Furthermore, the unified specification enables stakeholders to develop their own models and provide them with the information in black box. This is a proper way to protect their IP and to support information exchange during system co-design [21], [22].

The utilization of DLT in data exchange or asset trading systems could enable better control and fine-grained tracking of different usages. Liu et al. [9] proposed a data collection and exchange scheme, which utilized Ethereum blockchain technology to ensure security and reliability during industrial IoT data sharing. Aiming at solving the interoperability and trust issues for IoT services, Wattana et al. [23] integrated blockchain technology with a service-oriented architecture to assure data validity, quality of services and uncertainties. Beyond the data sharing, in [10] the authors developed a consortium blockchain to facilitate knowledge management and trading based on edge computing devices and edge artificial intelligence. The architecture of a peer-to-peer (P2P) knowledge market was proposed and a pricing strategy with incentives for the market based on noncooperative game theory was also discussed in this study. The idea of creating a distributed marketplace using blockchain technology has been proposed recently to remove the centralized components. In [13], the authors used a private Ethereum blockchain to support the construction of an IoT marketplace making functionalities and storage of the marketplace distributed. In order to accelerate the IoT and other open data sharing, Gowri et al. [24] proposed a decentralized data marketplace based on blockchain to replace the existing centralized data marketplaces.

As a relatively new concept, decentralized marketplace enabled by blockchain has not been well studied and requires more research efforts. After reviewing existing studies, we found several gaps:

- Most existing marketplace solutions only focus on the exchange process of digital assets, while the interoperability of the assets remains as a challenge. We believe that data interoperability should be taken into account when designing a marketplace and MBSE could be a solution for this issue.
- There are few, if not no, studies focusing on the marketplace for supporting model-based systems development, which is usually more complex with multiple stakeholders.
- Due to the scalability limitations of most public blockchain protocols, most decentralized marketplace solutions utilize permissioned, i.e. private and consortium, blockchain protocols. These solutions are not feasible in most system development scenarios where unknown and trustless stakeholders are involved.
- Due to the high cost of blockchain transactions, most blockchain-based marketplaces are not suitable for big data exchange, while large size datasets are common during systems development.

Considering these gaps, this paper aims to propose a novel decentralized marketplace solution by combining advanced MBSE and DLT approaches.

III. RESEARCH METHODOLOGY

A. Systems thinking

Systems thinking is an approach for understanding systems by examining the interactions between the components within
the system boundary [25]. In this paper, systems thinking is adopted for designing our approach in order to provide a complete solution of the DEA marketplace based on the identified challenges and motivations.

- **Identify the scenarios of DEA marketplace**: The scenarios are defined to understand the scope (system boundary) and the related concepts about DEAs. For example, in the case study, one scenario including requirement distributions and solution receptions is defined. It demonstrates the processes that vehicle systems engineers distribute their requirements of the embedded systems and they get the solutions from the embedded system suppliers.

- **Define the entities related to the scenario**: In the scenario, the entities are captured, such as the required models for describing expected views of DEAs.

- **Define the interrelationships between entities**: Interrelationships between entities refer to relationships between entities, for example, the inclusions between views and models [26].

- **Develop an approach for constructing DEA marketplace**: Based on the entities and their interrelationships, an approach based on MBSE and DLT is proposed to construct the asset marketplace.

- **Instantiate the entities using a case study**: Based on the designed scenario, a case study is proposed for developing an approach for DEA exchange.

- **Evaluation of the case study**: Based on the case study, qualitative and quantitative analysis is conducted for evaluating the proposed approach.

## IV. DEAs marketplace concept, framework and requirements

To facilitate the development of the DEAs marketplace, it is critical to formally define concept of DEAs and specify the functional requirements of the marketplace. This section firstly presents a conceptual framework of the proposed DEAs marketplace; then formally defines the concept of DEAs; and specify the functional requirements.

### A. DEAs marketplace framework

The conceptual framework of the proposed DEAs marketplace is as shown in Fig. 1. It is composed with four basic elements including DEAs which are the “goods” to be traded, DEA providers, DEA consumers, and the decentralized marketplace. DEAs providers formalize their development processes, requirements, functions and architectures following MBSE methodology to create DEAs. DEAs (or the meta data of DEAs) are added to the marketplace through a public or private node which is connected to the marketplace network. DEAs consumers find interested DEAs through proactive searching or passive subscription. Consumers receive the DEAs directly or through certain authorization procedures depending on the trading mode.

![General architecture of the proposed DEA marketplace](image)

**Fig. 1. General architecture of the proposed DEA marketplace**

**Fig. 2. Three Dimensional DEA**

### B. Definition of DEAs

A DEA refers to a currency format in some specific case which the currency can be considered as either a medium of information exchange or an attribute that has value during the entire life cycle, such as virtual models or documents [27]. In this paper, a three dimensional DEA concept model is proposed to define the DEA from three main viewpoints: 1) DEA object; 2) product lifecycle; 3) system artifacts of products. First, the DIKW model is used, with roots in knowledge management, to classify the DEA objects from Data (D) to Information (I), Knowledge (K) and Wisdom (W) [28]. It is used to represent the interrelationships between currency used during the entire lifecycle. The details are introduced as follows:

- **Dimension of the product processes** refers to the development process including various stages, phases and work tasks.

- **Dimension of system artifacts** refers to views of system stakeholders, e.g. requirement, function and architecture.

- **Dimension of DEA objects** refers to attributes of items including data, information, knowledge and wisdom [29].
  - Data items refer to attributes of DEAs implementing simulations, design, analysis, verification & validation and optimization in the entire lifecycle. They are functional symbols, but not structure model or documents.
  - Information items refer to structural contents constructed by data, such as SysML models for describing system requirements.
Knowledge items refer to validated information which makes possible the transformation of DEAs into instructions.

- Wisdom items refer to digital assets to support decision-making based on knowledge, such as machine learning models for decision-making at one decision gate.

**Definition 1:** Token ::= refers to a collection of concepts.  
\[ DeaS_{sys} ::= \sum DeaS^{t,\text{view},\alpha}_{sys}(i) \]  
where \( DeaS_{sys} \) refers to one DEA \( i \) of \( sys \); \( t \) refers to the time stamp of the related DEA during development process; \( \alpha \) refers to the DIKW attributes of the digital asset.

**C. Functional requirements of the DEA marketplace**

Various DLT protocols and solutions have been developed in recent years with different advantages and limitations. It is critical to choose the proper solution according to the requirements of DEA exchanges, which cover the whole lifecycle of a system and may involve stakeholders from both inside and outside of an existing organization or alliance network. Based on practical industrial needs and previous studies ([10], [24]) we define the functional requirements of the proposed DEA marketplace as follows.

- **Decentralization:** Stakeholders of the marketplace are usually geographically distributed and might have no trust with each other. Therefore, the digital assets should be managed in a decentralized way without any dominant party. All stakeholders should be enabled to join the marketplace fairly and freely.

- **Nontampering:** The marketplace should be able to protect the DEAs from the malicious attacks to keep the integrity and accuracy. Besides, the trading process and records should also be protected to avoid tampering.

- **Flexible access control:** The marketplace should provide different DEA access authorization approaches for different scenarios. For example, a stakeholder’s required DEA might need to be accessible to all stakeholders to find as many potential suppliers as possible; in contrast, a supplier’s proposal DEA should be open only to the customer and relevant parties.

- **Scalability:** With the expanding of the marketplace the number of stakeholders and trading frequencies will increase rapidly. The marketplace should enable high scalability with large, even unlimited, transaction throughput and low confirmation delay.

- **Low transaction cost:** The value of a DEA varies in the marketplace. There might be several iterations during a development lifecycle. The cost of a transaction should be as low as possible. It will make no sense if the transaction fees become close or higher than the DEA per se.

- **Big data support:** A DEA might contain large size documents like product models. The marketplace should support the exchange of large files with short delays.

**V. ENABLING TECHNOLOGIES**

**A. GOPPRR approach**

This section introduces a GOPPRR approach for formalizing the DEA on the three-dimensional conceptual model in Section IV.B [28]. It is adopted to develop meta-models for constructing the MBSE models aiming to describe DEAs from system artifacts, development processes and DEA objects. The GOPPRR approach is one of the most powerful approaches to describe domain specific characteristics and meta-meta models of products [30], including Graph, Object, Point, Property, Role and Relationship:

- **Graph** is a collection of Object, Relationship and Role represented as one window (one integrated concept of a class diagram and package in UML). The graph can be a visual diagram on the top level or lower level decomposed by one Object.

- **Object** is one entity in Graphs (class concepts in UML).

- **Point** is a port in Objects.

- **Relationship** is one connection between the different Points of Objects.

- **Role** is used to define the connection rules mirrored to the relevant Relationship. For example, one Relationship has two Roles. Each is defined to connect with one Point in Objects. Then, the Relationship is connected with these Points in the Objects.

- **Property** refers to one attribute of the other five meta-meta models.

**Definition 2:** Graph\( ^a_{Gi} \) refers to the model \( a \) based on the meta-model of Graph \( Gi \); In Graph\( ^b_{Gi} \); Object\( ^b_{Obji} \) refers to the object instance \( b \) based on the meta-model of Object \( Obji \); Relationship\( ^c_{Rei} \) refers to the relationship instance \( c \) based on the meta-model of Relationship \( Rei \); Role\( ^d_{Roi} \) refers to the role instance \( d \) based on the meta-model of Role \( Roi \) in the meta-model Relationship \( Rei \); Point\( ^e_{Poi} \) refers to the point instance \( e \) based on the meta-model of Point \( Poi \) in the meta-model Object \( Obji \); Property\( ^f_{Poi} \) refers to the property instance \( f \) based on the meta-model of Property \( Poi \) in the meta-model \( z \) \( (z \subseteq \{Gi, Obji, Rei, Roi, Poi\}) \):

\[
Graph^a_{Gi} ::= (\sum Object^b_{Obji}, \sum Relationship^c_{Rei}, \sum Role^d_{Roi}(x), \sum Point^e_{Poi}(y), \sum Property^f_{Poi}(z))
\]
TABLE I

COMPARISON OF DLT CATEGORIES

| DLT category | Permissionless | Permissioned |
|--------------|---------------|--------------|
|              | Public        | Consortium   | Private     |
| Decentralization | ✓ ✓           | x            |             |
| High security   | ✓             | ✓            | ✓           |
| Free access     | ✓ ✓           | ✓            | x           |
| High throughput | Depends on protocol | ✓ ✓ |             |
| Low cost        | Depends on protocol | ✓ ✓ | ✓           |

where each Relationship \( c \) is bond to two Objects or Points in Objects through Roles in order to identify the connections among Objects and Points.

Definition 3: Token \( \Rightarrow \) refers to the realizations between MBSE models and DEAs.

\[
Graph_{c_i}^a \Rightarrow DeaS_{sys}^{t,\text{view},\alpha}(a)
\]

where model \( a \) formalizes the DEA \( i \).

B. DLT solutions

To find the most feasible DLT solution for the proposed marketplace, we firstly compared different DLT solutions on the category level. In general, as shown in Table I, DLT can be classified into public and permissioned solutions. Depending on the permission governance scheme, permissioned DLT can be further divided into private and consortium solutions. Public DLT allows any stakeholder that holds a valid pseudonym to make and verify transactions in a secured and trustless environment, and even set and connect their own nodes to the network without requesting authorization from any party. In contrast, the permissioned DLT platforms are controlled by a single entity or a number of pre-selected entities corresponding to private and consortium solutions.

In general, most public DLT solutions have high security and decentralization, but usually have relatively low scalability and high transaction cost. In comparison, permissioned DLT solved the scalability problem by reducing decentralization. As the proposed DEA marketplace should be open to all participants and have no dominant entities, permissioned solutions will not fulfill the requirements. Therefore, in this study we only focus on public DLT solutions.

We reviewed some of the popular public DLT solutions and evaluated their performances according to the aforementioned functional requirements of the DEA marketplace as shown in Table I. The results show that, according to the consensus protocols, most public DLT can be classified into three categories, i.e. blockchain-based, DAG-based and other types [31]. The most adopted consensus protocols behind blockchain-based public DLTs are the Nakamoto protocol [7] and its improved versions such as Nakamoto-GHOST [32] and Bitcoin-NG [33]. However, with the rapid increasing of the networks size, several drawbacks and vulnerabilities of Nakamoto protocol have arisen: 1) low transaction rate and poor scalability; 2) high transaction fees and inefficient energy consumption; 3) centralization risks due to mining pools; 4) vulnerable to quantum attack. For example, the whole Bitcoin network, with approximately ten thousands nodes in total, can approve less than seven transactions per second and each transaction costs around 0.3 USD according to the latest statistics (citefees2020). In terms of computing power, the top five mining pools control more than 60% of the whole networks mining power [34].

To overcome the drawbacks of the blockchain-based DLTs, several new protocols based on non-linear ledger structures have been proposed, among which Directed Acyclic Graph (DAG) has attracted much attention. Compared with blockchain-based protocols, the main advantage of DAG-based protocols is that they eliminate transaction throughput caps. Instead of sequentially storing all transactions to a linearly growing chain of blocks with fixed time intervals, in a DAG-based network every vertex can provide multiple diverging branches. Theoretically, a DAG-based protocol could allow millions of even unlimited transaction throughput, although in reality the capacity will be capped by physical communication bandwidth. These unique characteristics make DAG-based ledger structures the most favorable solutions for the construction of a open marketplace as required in this study.

IOTA Tangle is a DAG-based protocol specifically designed to support industrial IoT data exchange and machine-to-machine micro transactions [35]. To issue a new transaction in the Tangle, users must perform a small amount of computational work to validate two unapproved transactions (tips), and this new transaction will be validated by some subsequent transactions. According to this two-tip rule, every vertex in the Tangle has an out degree of two and contains a Proof-of-Work (PoW). By this way, the scalability issue can be solved as the more transactions added to the Tangle, the faster transactions can be validated. Besides, this 'pay-it-forward' system of validations can be used as the incentive mechanism for honest participation, which eliminates financial rewards and makes transactions fee-less. Moreover, there are no miners thus no mining pools in the Tangle which makes it possible to be truly decentralized.

Another advantage of IOTA Tangle is the provided second-layer data communication protocol named Masked Authenticated Messaging (MAM). It supports publishing and receiving encrypted data over the Tangle regardless of the size or cost of a device [36]. MAM distributes data using the concept of channels supported by the Tangle gossiping propagation mechanism. Any user who want to publish data can create a channel with a unique address and then attach data to this channel following the Tangle transaction two-tip approval procedure. Once approved, the other users who subscribe to this channel will be able to receive the data which might be encrypted according to the publisher’s configuration.

MAM uses Merkle Hash Tree (MHT) as the signature scheme to encrypt the message [36]. The root of a MHT is created using the unique user identification and it serves as the address of the data channel. Enabled by the MHT signature scheme, MAM allows different privacy and encryption modes to control the visibility of a channel and the access to the data i.e. public and restricted modes. Public mode uses the MHT root as both channel address and transaction identification. In this mode, any user who knows the channel address, even randomly, can decode and consume the message. Restricted
mode adopts an authorization key based on private mode. The channel address is encrypted using the hash of the MHT root and the message with authorization key. This mode allows a publisher to revoke access to future messages by changing the authorization key without changing the channel address. This encryption mechanism fulfills the flexible access control requirement of the proposed DEA marketplace.

Theoretically, there is no limitation about the size of a MAM message. When the size of a MAM message exceeds the transaction capacity, which is 2187 trytes (1.3KB), it will be automatically split into multiple transactions which will be contained in the same bundle to keep them retrievable. In the ideal scenario, i.e. when the IOTA Tangle network is mature enough to support millions or unlimited TPS, the exchange of large files will not be a problem. Currently, the IOTA Tangle is still under development with limited transaction processing capability, thus large MAM messages might cause delay in confirmation. As a temporary mitigation solution, the InterPlanetary File System (IPFS) \cite{34} is adopted in this study to handle large DEAs. IPFS is a content-addressing, peer-to-peer network for storing and sharing arbitrary data in a distributed file system. It uses a hash to access a IPFS file and the hash value changes when any change is made to the content. Therefore, a large size DEA in the marketplace can be saved in the IPFS network and only its hash is traded in the marketplace. Before saving to IPFS, the content can be encrypted to assure the privacy and security either using the encryption mechanism provided by MAM or extra encryption algorithms such as AES256-GCM \cite{38}.

In summarize, in order to address the functional requirements of the DEA marketplace, MBSE tools, e.g. GOPPRR, are used to facilitate the interoperability among stakeholders by creating formalized DEAs; IOTA Tangle and MAM protocol are adopted to enable decentralization, nontampering, high scalability, low transaction cost and flexible access control requirements; and IPFS is proposed as a temporary solution to handle large files before the mature of IOTA Tangle network.

Based on the selected enabling technologies, the overall workflow of creating and publishing DEAs is defined as shown in Algorithm 1. The receiving and consuming process is in the opposite sequence of the publishing process. Both processes are demonstrated through a case study in the following section.

### VI. Case Study

The case study is based on a common scenario during vehicle system development. An assembling vehicle company expects to purchase a solution of embedded system for a new vehicle model from external suppliers. The vehicle systems engineers first develop a requirement model, i.e. as the DEAs for the marketplace, using the GOPPRR approach. In this case, this message is expected to reach as many stakeholders as possible. Therefore, this DEA is published to the marketplace with public mode so that anyone can receive and consume the requirement model.

On the other side, the embedded system engineers from a supply agency receive the requirement model from the marketplace. Based on requirements, they develop solutions

### Table II

| Type            | DLT solutions | Protocol | Throughput (tx/s) | Confirmation time | Fault tolerance | Transaction fees |
|-----------------|---------------|----------|-------------------|-------------------|-----------------|-----------------|
| Blockchain-based| Bitcoin       | PoW      | Tens              | ≈ 60 min.         | 50% power       | ≥ 0.3 USD       |
|                 | Ethereum      | PoW      | Tens              | ≈ 6 min.          | 50% computing power | ≥ 0.1 USD      |
|                 | Litecoin      | PoW (key blocks) | Hundrededs | ≈ 10 min.         | 50% computing power | 0.003 Waves   |
|                 | IOTA          | PoW      | Tens              | ≈ 30 min.         | 50% computing power | 0.001 LTC      |
| DAG-based       | Qum           | PoS      | Thousands         | 0.5 to 10 min.    | 50% computing power | None           |
|                 | Cardano       | PoS      | Thousands         | ≈ 60 min.         | 50% stake value  | 0.001 Qum/KB    |
| Other protocols |               |          |                   |                   |                  |                 |

### Algorithm 1: Publishing DEAs to the marketplace

**Input:** Σ \( \text{Object}_{\text{obj}} \), \( \Sigma \text{Relationship}_{\text{rel}} \), \( \sum \text{Role}_{\text{role}}(x) \), \( \sum \text{Point}_{\text{point}}(y) \), \( \sum \text{Property}_{\text{property}}(z) \)

**Output:** IOTA Tangle transaction address

**Initialization:** Create MBSE models:

\[
\text{Graph}_{\text{g}} := (\sum \text{Object}_{\text{obj}} , \sum \text{Relationship}_{\text{rel}} , \sum \text{Role}_{\text{role}}(x) , \sum \text{Point}_{\text{point}}(y) , \sum \text{Property}_{\text{property}}(z))
\]

Realize the DEAs from the MBSE models:

\[
\text{Graph}_{\text{g}} \Rightarrow \text{Dea}_{\text{sys}}^{\text{e}}(x, y, a, d)
\]

1. **for** \( \text{Dea}_{\text{sys}}^{\text{e}}(a) \) **from** \( \text{Dea}_{\text{sys}}^{\text{e}}(a) \) **do**
2. **Encode** DEA to IOTA Trytes:
   \[
   \text{Dea}_{\text{sys}}^{\text{e}}(x, y, a, d) \Rightarrow \text{Trytes}_{\text{sys}}(a)
   \]
3. **Encrypt** Trytes with MAM signature scheme:
   \[
   \text{Trytes}_{\text{sys}}(a) \Rightarrow (\text{Encrypted}_{\text{sys}}(a), \text{root}_{\text{sys}}(a))
   \]
4. **Upload** Encrypted \( \text{sys} \) to IPFS
5. **return** IPFS content address \( \text{Hash}_{\text{sys}}(a) \)
6. **Encode** to IOTA Trytes:
   \[
   \text{Hash}_{\text{sys}}(a) \Rightarrow (\text{Hash}_{\text{sys}}(a), \text{root}_{\text{sys}}(a))
   \]
7. **Encrypt** with MAM signature scheme:
   \[
   \text{Trytes}_{\text{sys}}(a) \Rightarrow (\text{Encrypted}_{\text{sys}}(a), \text{root}_{\text{sys}}(a))
   \]
8. **Publish** Encrypted \( a \) to IOTA Tangle by MAM
9. **if** public mode **then**
10. **Address** \( \text{Hash}(a) = \text{root}_{\text{sys}}(a) \)
11. **else** if restricted mode **then**
12. **Address** \( \text{Hash}(a) = \text{Hash}(\text{root}_{\text{sys}}(a)) \)
13. **end if**
14. **return** IOTA transaction address \( \text{Address}_{\text{Hash}}(a) \)
15. **end for**
and build the solution models using the GOPPRR approach. In this case, the solution models are encrypted so that they are accessible only to authorized parties, i.e. the assembling vehicle company. Therefore, these DEAs (solution models) are published to the marketplace with restricted mode. The vehicle systems engineers receive the solution models from the marketplace and the corresponding encryption keys from supply agencies, so that they can access to the solutions and compare them to find the most suitable solution.

1) **DEAs marketplace prototype**

A prototype of the proposed DEA marketplace was constructed as proof-of-concept based on the IOTA Tangle API (iota.lib.js), MAM API (mam.client.js) and IPFS API (ipfs Javascript implementation). The source codes, written in Javascript, with implementation instructions for publishing and receiving DEAs files are open access on GitHub [39].

Based on this prototype, experiments were conducted covering the complete process of publishing and receiving DEAs files, i.e. the vehicle company’s requirement models and the supply agencies’ solution models. These models were developed using an MBSE tool MetaGraph [40] (http://www.zkhoneycob.com/).

2) **Experiment**

The detailed workflow of publishing and receiving the requirement models with public mode through the marketplace is shown in Figure 4. The screenshots of the output from each step based on an example is presented in Figure 5. It can be divided into the following steps.

(i) **Preparing DEAs**: The vehicle systems engineers develop requirement models, using the GOPPRR approach and export them as OWL files [41] making them ready for transferring.

(ii) **Encoding and encryption**: In order to protect the privacy of the DEAs on the IPFS network, they should be encrypted locally before uploading to IPFS. We used the encryption mechanism provided by IOTA, The original files are first encoded into trytes (Trytes1: FBFDSCUC…), which is the data encoding format of IOTA based on ternary numeral system [35]. Then the trytes data are encrypted with the MAM signature scheme, producing the encrypted data (Payload: AQKCI9D….) and a MHT root (Root1: KXEEERTEE….), which is the decryption key.

(iii) **Uploading to IPFS**: The encrypted data are uploaded to the IPFS network and a content identification (CID) hash code (Payload: QmYTHwdk…) will be generated which can be used to retrieve the uploaded content (AQQKCI9D…) from IPFS network (https://ipfs.io/ipfs/QmYTHwdk…)

(iv) **IPFS CID encryption**: Using the same encoding and encryption approach, the IPFS hash and the root of the previous encryption are encoded (IPFS_Trytes: 9CADHCCC…) and encrypted to construct the payload (IPFS_Payload: AQWC9JT…) of the IOTA transaction. A second root (Root: WKKSCCRG…) will be generated which can be used to decrypt the payload.

(v) **Publishing payload**: Using the MAM API, the payload will be published to the IOTA Tangle and one or more transactions will be generated. In public mode the second root (WKKSCCRG…) will be used as the address of the transaction. Certain tags and descriptions can also be added to the transactions to facilitate future search or subscription.

(vi) **Receiving transactions**: Once the IOTA transactions are approved, the suppliers can retrieve them through the transaction address. Certain searching service could be added to facilitate the transaction finding process.

(vii) **Payload decryption**: After received the transaction, the supplier can decrypt the payload using the address, which is the same as the root in public mode, and then decode the trytes format content to obtain the CID hash code and the root1.

(viii) **Download from IPFS**: Using the CID, the encrypted content can be downloaded from IPFS network.

(ix) **DEAs Decryption**: The downloaded content can be decrypted with root1 to get the trytes format content. After decoding, the original requirement models will be readable to the embedded systems engineers of the supplier.

After analyzing the received requirement models, the suppliers will develop corresponding solutions and prepare the solution models with the same MBSE approach. The solution models will be published to the marketplace following a similar workflow. In this case, they can use restricted mode instead of public mode. The only difference is that, the address of the transactions on IOTA Tangle is the hash of the root and an extra side key is required to decrypt the transaction payload. Therefore, the suppliers can share their side keys only to the vehicle company to authorize them with access to the solution models.

3) **Performance evaluation**

In this study, we used a public IOTA node (https://www.iotaqubic.us:443) combined with a local IPFS node to build the experiment environment. A series of experiments were conducted to evaluate the performance of the prototype. Figure 5 presents some output screenshots during publishing a requirement model which correspond to the workflow shown in Figure 4. Three groups of MBSE models were created and each of them was published to the IOTA Tangle 10 times. During each iteration, the time of three procedures were measured, i.e. local processing, attaching transactions to the Tangle and transactions been confirmed. The local processing includes data encoding, encryption and uploading to IPFS. The results are listed in Table III and the original experiment records are also open access [39].

According to the experiment results, the local processing time show positive correlation with the size of the DEAs files. This agrees with the expectation that the encoding, encrypting and uploading time increases when the data size grows. The time of attaching transactions to the Tangle is not impacted by the file size because only the encrypted CID, with fixed length, is published to IOTA Tangle. However, it is worth to note that the attaching time varies depending on the conditions of the chosen IOTA node, such as computing power, load, number of neighbours. The confirming time shows high variance which is due to the tip selection algorithm of IOTA protocol [35].
Fig. 4. DEAs Marketplace workflow

TABLE III
PERFORMANCE OF THE MARKETPLACE PROTOTYPE

| DEAs files     | Size  | Processing Time (seconds): mean (SD, min, max) | Attaching Time (seconds): mean (SD, min, max) | Confirming Time (seconds): mean (SD, min, max) |
|---------------|-------|-----------------------------------------------|---------------------------------------------|---------------------------------------------|
| Case1 models  | 2.9Mb | 0.80 (0.07, 0.72, 0.97)                       | 12.63 (10.32, 4.70, 33.94)                   | 158.90 (190.08, 46.00, 677.00)               |
| Case2 models  | 4.6Mb | 1.21 (0.12, 1.09, 1.39)                       | 16.21 (18.69, 4.40, 48.03)                   | 187.70 (175.00, 42.00, 663.00)               |
| Case3 models  | 5.6Mb | 1.37 (0.09, 1.29, 1.53)                       | 18.33 (21.74, 4.47, 52.57)                   | 172.90 (178.80, 37.00, 657.00)               |

4) Privacy and security analysis

The privacy and security analysis for the proposed marketplace is provided as follows:

- Authentication: The proposed marketplace supports two different privacy modes depending on the publisher’s needs. Data published to the marketplace in public mode are accessible to all stakeholders without restriction. In contrast, data published in restricted mode are only open to those authorized with an extra encryption key. When IPFS is used, the data uploaded to IPFS are encrypted in both modes, which keeps the data only open to the marketplace stakeholders. Even the IPFS content is compromised, the attacker will not get access to the data as they are encrypted before uploading.

- Nontampering: The tangle-based consensus protocol enables the published transactions on the marketplace with tamper-resistance characteristic. Once the transaction is approved, nobody will be capable of modifying unless the entire network is compromised. The data uploaded to IPFS network are also tamper-resistance owing to the hash function provided by IPFS. Any modification to the original data will result in a totally different identification. Besides, the encryption procedure, which also uses hash function, before uploading to IPFS adds an extra layer of protection.

- Decentralization: The proposed marketplace is based on a public tangle-based DLT protocol. This protocol was designed to be fully decentralized because no miners are required. Therefore the centralization risk caused by mining pools is eliminated.

5) Limitations

The enabling technologies, especially the adopted DLT solution, for the proposed marketplace are promising but still evolving. Some limitations remain to be addressed.

The efficiency and security of the adopted IOTA Tangle DLT protocol heavily relies on the size of the network, i.e. the number of connect nodes and participants. The nodes connected and more transactions submitted, the network will have the higher security and transaction rate. Currently, the IOTA Tangle is still in its early phase with limited number...
of nodes. To protect the network from malicious attacks a temporary mechanism called the Coordinator has been used to directly or indirectly validate the transactions. This mechanism brings the concerns of centralization and thus the single point of failure risk. This limitation is expected to be resolved in the near future by launching the Coordicide modular [42], which will remove the Coordinator and make the Tangle fully decentralized.

Pricing strategy and payment method are essential components for a mature marketplace which are not investigated in this study. The main reason is that during systems development, the price is usually offered by the DEAs providers. This is different from IoT data trading or smart energy trading etc., where the price is usually dynamically defined by the marketplace. However, certain price comparison and recommendation mechanisms will be beneficial and could be future work of this study.

VII. Conclusion

This paper proposes a decentralized open marketplace to facilitate DEAs exchange during system developments among inter-organization stakeholders. Following the systems thinking methodology, the functional requirements of the marketplace are defined based on scenario analysis. A DEAs marketplace framework is designed and its key concepts are formally defined. The GOPPRR approach is adopted to create DEAs, thus to enable the interoperability of the MBSE models. Moreover, the tangle-based DLT solution, IOTA Tangle and its MAM messaging protocol, is adopted to enable secure, non-tampering, low-cost and decentralized DEAs exchange. A proof-of-concept implementation of the marketplace is conducted based on a case study. Experiment results prove the feasibility of the proposed approach.

ACKNOWLEDGMENT

The work presented in this paper is supported by the EU H2020 project (869951) FACTLOG-Energy-aware Factory Analytics for Process Industries and EU H2020 project (825030) QU4LITY Digital Reality in Zero Defect Manufacturing and the InnoSwiss IMPULSE project on Digital Twins.

REFERENCES

[1] M. Törngren and U. Sellgren, “Complexity Challenges in Development of Cyber-Physical Systems,” in Simulation and Modeling of Systems of Systems, 2018, pp. 478–503. [Online]. Available: http://link.springer.com/10.1007/978-3-319-95226-9_27
[2] B. Beihoff, S. Friedenthal, D. Kemp, D. Nichols, C. Oster, C. Peredis, H. Stoewer, and J. Wade, “A World in Motion Systems Engineering Vision 2025,” in International Council on Systems Engineering, vol. 327, no. 5970, mar 2010, pp. 1183–1183.
[3] J. Lu, D.-j. Chen, D. Gürdür, and M. Törngren, “An Investigation of Functionalities of Future Tool-chain for Aerospace Industry,” in INCOSE International Symposium, vol. 27, no. 1, jul 2017, pp. 1408–1422. [Online]. Available: http://doi.wiley.com/10.1002/j.2334-5837.2017.00437.x
[4] M. Schluse, M. Priggemeyer, L. Atorf, and J. Rossmann, “Experimental Digital Twin Streaming Simulation-Based Systems Engineering for Industry 4.0,” IEEE Transactions on Industrial Informatics, vol. 14, no. 4, pp. 1722–1731, apr 2018. [Online]. Available: http://ieeexplore.ieee.org document/8289327

[5] J. De Lara and H. Vangheluwe, “Atom3: A tool for multi-formalism and meta-modelling,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 2306, pp. 174–188, 2002.

[6] J. Brogan, I. Baskaran, and N. Ramachandran, “Authenticating health activity data using distributed ledger technologies,” Computational and structural biotechnology journal, vol. 16, pp. 257–266, 2018.

[7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[8] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, “Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies,” Journal of medical Internet research, vol. 21, no. 6, p. e13583, 2019.

[9] C. H. Liu, Q. Lin, and S. Wen, “Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning,” IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3516–3526, 2018.

[10] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, “Making knowledge tradable in edge-a-enabled iot: A consortium blockchain-based efficient and incentive approach,” IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6367–6378, 2019.

[11] S. Wang, A. F. Taha, J. Wang, K. Kvatnernik, and A. Hahn, “Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1612–1623, 2019.

[12] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, “Blockchain-based personal health data sharing system using cloud storage,” in 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2018, pp. 1–6.

[13] L. Mikkelsen, K. Mortensen, H. Rasmussen, H.-P. Schwefel, and T. Madsen, “Realization and evaluation of marketplace functionalities using ethereum blockchain,” in 2018 International Conference on Internet of Things, Embedded Systems and Communications (INTETEC), IEEE, 2018, pp. 47–52.

[14] J. Tavcar and I. Horvath, “A Review of the Principles of Designing Smart Cyber-Physical Systems for Run-Time Adaptation: Learned Lessons and Open Issues,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 1, pp. 145–158, jan 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8329014

[15] F. Tao and Q. Qi, “New IT Driven Service-Oriented Smart Manufacturing: Framework and Characteristics,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 1, pp. 81–91, jan 2019. [Online]. Available: https://ieeexplore.ieee.org/document/7990538

[16] R. Cloutier, B. Sauser, M. Bone, and A. Taylor, “Transitioning systems thinking to model-based systems engineering: Systemtransys to SysML models,” IEEE Transactions on Systems, Man, and Cybernetics:Systems, vol. 45, no. 4, pp. 662–674, 2015.

[17] C.-H. Yang, V. Vyatkin, and C. Pang, “Model-Driven Development of Control Software for Distributed Automation: A Survey and an Approach,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 3, pp. 292–305, mar 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6555786

[18] V. Marchesini, O. Ortho, and D. Doni, “Model-Based Interoperability Engineering in Systems-of-Systems and Civil Aviation,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 4, pp. 637–648, apr 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7571227

[19] A. L. Ramos, J. V. Ferreira, and J. Barcelo, “Model-Based Systems Engineering: An Emerging Approach for Modern Systems,” IEEE Transactions on Systems, Man, and Cybernetics: Part C (Applications and Reviews), vol. 42, no. 1, pp. 101–111, jan 2012. [Online]. Available: http://ieeexplore.ieee.org/document/5772047

[20] V. Singh and K. E. Willcox, “Engineering Design with Digital Thread,” AI/AA Journal, vol. 56, no. 11, pp. 4515–4528, nov 2018. [Online]. Available: https://arc.aiaa.org/article/doi/10.2514/1J.3057255

[21] M. Schluse, M. Priggemeyer, L. Atorf, and J. Rossmann, “An investigation of MBSE practices across the contractual boundary,” Procedia Computer Science, vol. 28, no. Cser, pp. 692–701, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.procs.2014.03.083
Jinzhi Lu, CSEP, is a research scientist at EPFL. He got his Ph.D degree at KTH Royal Institute of Technology, Mechatronics Division in 2019. His research interest is MBSE tool-chain design and MBSE enterprise transitioning. He is senior member of China Council on Systems Engineering (CCOSE), China Council on Systems Engineering.

Xiaochen Zheng Ph.D. received his doctoral degree from Universidad Politécnica de Madrid. Before that he studied in Shandong University in Mechanical Engineering and obtained his bachelor and master degree. He is now working atcole Polytechnique Fédérale de Lausanne as a postdoctoral scientist. His research interests include Internet of Things, Machine learning, Wearable technology, Distributed ledger technology and their applications in industry and healthcare etc.

Zhenchao Hu is a PhD student at SJTU. He received his bachelor degree at Wuhan University in Mechanical and Electronic Engineering. His research interest remain in the data integration, prognostics health management, etc.

Huisheng Zhang was promoted as an associate professor at SJTU in 2001. In 2005-2006, he was selected to be the research scientist in the Department of Safety and Nuclear Engineering, AREVA NP in France by FFCSA. In December 2009, he was promoted as a full professor at SJTU. Prof. Zhangs research interests remain in the modeling and simulation, dynamics and control of power plant, health management system etc.

Dimitris Kiritsis is Faculty Member at the Institute of Mechanical Engineering of the School of Engineering of EPFL, Switzerland, where he is leading a research group on ICT for Sustainable Manufacturing. He serves also as Director of the doctoral Program of EPFL on Robotics, Control and Intelligent Systems (EDRS). His research interests are Closed Loop Lifecycle Management, IoT, Semantic Technologies and Data Analytics for Engineering Applications.