Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

The Symbiosis of Distributed Ledger and Machine Learning as a Relevance for Autonomy in the Internet of Things

Daniel Burkhardt
Ferdinand-Steinbeis-Institute
Stuttgart, Germany
daniel.burkhardt@steinbeis.de

Patrick Frey
Ferdinand-Steinbeis-Institute
Stuttgart, Germany
patrick.frey@steinbeis.de

Heiner Lasi
Ferdinand-Steinbeis-Institute
Stuttgart, Germany
heiner.lasi@steinbeis.de

Abstract

The Internet of Things (IoT) describes the fusion of the physical and digital world which enables assets on the edge to send data to a platform where it gets analyzed. Defined actions are then triggered to influence cross-functional edge activities. Furthermore, on the platform tier functionalities and relations need to be identified and implemented to realize assets operating autonomously and ubiquitously.

The exploration of this paper results in the identification of autonomous characteristics and shows functional components to implement autonomous assets on the edge. Distributed Ledger Technology (DLT) and its fusion with Machine Learning (ML) as an area of Artificial Intelligence (AI) provides an integral part to realize the described outline. Thus, the recognition of DLT's and ML's usage in the IoT and the evaluation of the relevance as well as the synergies build the main focus of this paper.

Keywords: Internet of Things, Autonomous Assets, Distributed Ledger, Blockchain, Artificial Intelligence, Machine Learning

1. Introduction

Heterogeneity is a characteristic of current system landscapes with incompatible data silos between enterprises evolved from a non-integrative development of systems in the 3rd Industrial Revolution [1]. Automation is the main goal of this wave of industrial advancement. Data is transferred from physical environments to centralized systems along the automation pyramid up to business domains where the created information supports business processes. The imaginary evolved silos guarantee efficiency in the respective business area but aggravate an inter-domain integration due to incompatibilities [2, 3].

IoT systems envision the enablement of ubiquitously acting Autonomous Assets (AA) supporting other AAs to realize an asset economy on the edge. Relevant components need to be identified to realize this vision. Through the merge of the Operational Technology (OT) and Information Technology (IT) different trustworthiness aspects converge [4]. On OT, systems need to be safe, efficient, and consistent whereas security, agility and flexibility are of importance for IT [5]. In order to enable AAs, IT and OT need to be combined guaranteeing trustworthiness and providing (data) interoperability throughout the end-to-end process over the edge, platform and enterprise tiers of an IoT system [6]. Furthermore, in order to enable an asset to act intelligently, a component that foster decision making in a distributed data landscape is required. Distributed Ledger Technology (DLT) enables a trustful, governed value exchange between trustless assets whereas Artificial Intelligence (AI) provides the components to make decisions in a self-sufficient, yet artificial manner. The relevant research question that builds the center of this paper and is of relevance for the described IoT vision is:

RQ: What functionalities are enabled by Distributed Ledger and Machine Learning to realize Autonomous Assets in the Internet of Things?

The named research question is approached according to the following paper structure. Section 2 forms the theoretical foundation. In the subsequent section related work is briefly provided. Based on this foundation, the paper proceeds with the presentation of the used methodologies. Results are shown in section 5 providing a functional model to enable AAs. Its implications are discussed in section 6. The conclusion summarizes the article and gives an overview of future work.

2. Theoretical Framework

2.1. Internet of Things

The IoT describes the convergence of OT and IT. OT comprises the direct monitoring and controlling of

URI: https://hdl.handle.net/10125/59900
ISBN: 978-0-9981331-2-6

devices, processes, and enterprise events to detect or cause physical changes. IT, on the other hand, covers the entire spectrum of data processing technologies based on Internet protocols [7]. The Industrial Internet Consortium (IIC) as the worldwide largest Industrial IoT (IIoT) consortium defines an IIoT system[1] as a "system that connects and integrates industrial control systems with enterprise systems, business processes and analytics" [8]. Moreover, the IIC provides an Industrial Internet Reference Architecture (IIRA) which includes different viewpoints: business, usage, functional and implementation, to support the requisite broad industry applicability. The paper proceeds with a focus on the functional components: Control, Operations, Information, Application and Business [4] and their interrelation.

The 3-Tier architecture pattern is used as a conceptual architecture of an IoT system to locate functionalities in the context of this paper. It divides an IoT system into edge, platform and enterprise tiers. The edge tier contains assets supporting the user in its physical environment. For analysis, data generated on the edge is sent to the platform tier. Additionally, control commands from the enterprise tier will be received, processed and forwarded from the platform to the edge tier. The enterprise tier provides interfaces to end-users, implements domain-specific applications and decision support systems [4].

The ubiquity and diversity of things in the IoT is steadily increasing. This also means that more data is generated on the edge. Additionally, the sensitivity and the variety of measured phenomenas increase [9]. The possibilities to store and process data span over the edge, platform[2] and DLTs [10]. However, a number of technological challenges need to be considered. On the edge tier, there are some devices with constrained resources such as energy, storage or computing power. Due to these constraints the execution of specific machine learning algorithms is difficult [9]. This also means that certain real time autonomous decisions can not be made by the device itself. In this case, the data must be transferred to an optional data storage like a platform. Because of the large amount of data and the small number of computing centers, the scalability as well as the costs for transferring the data, might be challenging [11]. Certainly, design decisions that take the named constraints into account in accordance to the aimed implementation are relevant [12].

[1]The definition of an IIoT system is used interchangeably to the definition of an IoT system in this paper

[2]The definition of "IoT platform" is given in [10]

2.2. Autonomous Assets

An autonomous learner determines its own specific objectives, defines the content and process to achieve its goals and evaluates the results of the learning progress following its unique demands for accomplishment [13]. Prognostics is an important functionality of a mission critical autonomous system in order to guarantee stability and fault tolerance [14]. Therefore, Scally et al. [14] add that the system's technology needs to be data agnostic in order to integrate data sources. Furthermore, a learning functionality is required to enable continuous improvement of the system [14].

In contrast, ubiquity defines the premise that all data of a system needs to be accessible by any asset in an adequate manner and time dependent on the asset's location. A centralized control is not sufficient to enable ubiquity. Assets need to be autonomous guaranteeing a distributed control functionality of the devices themselves [15].

Assets are non-divisible and hide their constituent parts from the external world. It is required that assets store their internal state and communicate with each other. Furthermore, assets consist of a structure, behavior and are capable of sensing [15]. Examples of assets are major applications, high impact programs, personnel, equipment or a group of systems with value to the entity that owns the asset [16].

Three architectural structures of AAs are defined. An AA can act without requiring a network infrastructure proceeding tasks independently [17]. The second structure describes the interaction of multiple assets in order to achieve a common mission. It requires a networking infrastructure, mostly based on proprietary technologies and protocols for inter-device communication. The cooperation of multiple AAs with Internet platforms is defined as the third architectural structure. Digital assets deployed on the platform act as counterparts to the AAs on the edge and enhance the functional capabilities of the respective device. Different inter-asset communications are possible. The devices can directly communicate with each other by implementing a complete TCP/IP stack. A more energy efficient variant is the communication through a gateway that solely implements the TCP/IP stack and functions as an Internet bridge for the devices. Platforms built on top of the described architecture gather device data and provide services. [17].

Coordination and multi-objective decision problem mechanisms are required in a network of multiple AAs with different capabilities and mission objectives. According to Abel and Sukkarieh [18], a coordination module that does not depend on a centralized decision

maker to provide flexibility is necessary. Therefore, a voting model is the chosen method to coordinate multiple objectives [18].
Trust between assets plays an essential role in an environment where unknown and potentially malicious assets can act [19]. Trust is defined as the subjective, probabilistic level with which an agent estimates a particular action of another agent or a group of agents [20]. Functionally, autonomous ubiquitous assets require intelligent, mobile and connectivity capabilities. Furthermore, in order to collaborate and use services independently, a value transfer functionality, in e.g. the form of digital currency, needs to be guaranteed to function self-sufficiently. Data needs to be accessible at a specific location and time as well as in a semantical uniform format providing context-awareness to enable these functionalities [21].

2.3. Distributed Ledger

A current development of platforms that enable cross-functionality and broad data analytics combining the evolved centralized, sealed systems can be observed. However, platforms lead to lock-in effects and the loss of data ownership. Solutions that prevent these aspects need to be provided.
According to Burkhardt et al. [22], the concepts of DLT, like blockchain or tangle, are based on various principles. With the use of cryptographic means, the double spending problem can be prevented in a trustless peer-to-peer (p2p) network. Asymmetric key pairs applied for digital signatures guarantee an explicit transfer of digital value items and asset authentication. Hashing and (merkle) tree structures implement user anonymity in the transparent DLT network but also enable an efficient verification of transactions as well as immutability of records. Transactions are chronologically saved in blocks, validated and redundantly attached to the linked block lists of the network participants guaranteeing information symmetry.
The Byzantine General's Problem claims that more than 2/3 of a group of peers need to be collaborative in order to reach consensus on a decision. Therefore, consensus algorithms, like Proof of Work (PoW), Proof of Stake (PoS), Hashgraph, etc., are implemented to establish agreements on the global state of the ledger.
Smart contracts implement business logic that define terms between parties and run autonomously on the DLT to enhance the protocol's functionality. To get the peers participating in the network, economic mechanisms are used to provide incentives and create intrinsic value for the participants.
According to the implementation requirements, DLT protocols are either public or private. Additionally, different procedures of a protocol can be defined as permissioned or permissionless depending on the configuration. For example, Ethereum is a public, permissionless blockchain protocol whereas Ripple is a public, permissioned protocol allowing a selected group of participants to define the state consensus. The different network configurations of a DLT protocol and the use of algorithms result in a diverse set of characteristics. For example, the immutability or finality of the DLT is different depending on the implemented consensus algorithm [22, 23].
The DLT stack consists of three layers built on top of the Internet stack: protocol, application and integration layer. On the first layer data is stored according to the implemented data structure. On top, applications enhance the protocol's functionality. Examples are Parity, RSK or wallet providers like Coinbase and Kraken as well as development tools like Remix or MetaMask using sidechains, bridges, etc. to create a connection to the first layer but also bypassing the first layer limitations. Thus, both layers are strongly interrelated in their developments [10]. The integration layer provides the user interface and enables the DLT system integration into other IT systems.
Furthermore, DLT generic platforms (DLgp) enable the entire DLT stack supporting a horizontal integration of business domains. Ethereum is a DLgp example which is a platform that forms a common data and functional basis for the creation of business logic. Thus, it provides interoperability between the developed applications. On the other hand, the development of DLT platform components (DLpc) that implement a specific property or combination to fulfill a specified purpose can be observed. BigChainDB is characterized as a DLpc functioning as a decentralized database [10].
Burkhardt et al. [10], Seebacher and Schueritz [24] identified a valuable appliance of DLT in the field of IoT to improve security, reliability, privacy and integrity. However, in order to enable a profound integration, challenges of both areas need to be identified and solved [10, 24]. In comparison to traditional transaction systems, DLT systems are located between companies avoiding redundant storage of transactions and providing data interoperability [25]. Consequently, DLT provides trustworthiness by dis-intermediation and avoidance of a central controlling party [10, 26]. Based on these capabilities, a unique digital identity representing its physical counterpart can be created with implications to audit processes and compliance procedures [27].

2.4. Machine Learning

AI is used to enable intelligent behavior of assets [28]. Various definitions of AI exist due to the missing agreement on the definition of intelligence among researchers. In the context of this paper, the definition of Luger and Stubblefield [29] is used: "AI is the branch of computer science that is concerned with the automation of intelligent behavior", whereby intelligence is described by the ability to learn, understand, and make judgments or have opinions that are based on reasons [30].

AI can be divided into the branches of machine learning (ML), natural language processing, expert systems, vision, speech, planning and robotics [31]. The usage of ML in the IoT is of focus and therefore further described. Mohri et al. [32] define ML broadly as a computational method using experience to improve performance or to make accurate predictions. Whereby, the term experience refers to past information, mostly in form of data collected and made available for analysis. The process of deploying a ML-model is demonstrated in Figure 1. The first step, *Data Collection*, includes

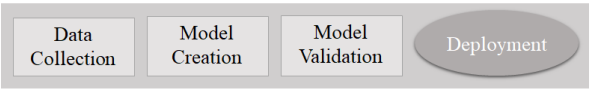

Figure 1. Machine Learning Process [28]

data acquisition and data preparation. As part of this process step, feature extraction converts raw data into information that relates to the physical state of data. After that, feature reduction reduces the number of features. This is done by selecting only a few helpful features or transforming the features to lower dimensional space [28]. The *Model Creation* process step can be grouped into the algorithm categories of supervised learning and unsupervised learning. In supervised learning, data instances are given with known labels and therefore we can apply algorithms like decision trees and neural networks. As opposed to this, in unsupervised learning, only unlabeled data instances are available. If this is the case, algorithms like K-means clustering and principle component analysis can be conducted [33, 34]. In the *Model Validation* step, techniques like re-substitution, hold-out or K-fold cross-validation determine the quality of the model. The evaluation results are used to optimize the model parameters [35].

A further branch of ML is reinforcement learning in which a learning system, without any initial information about its environment or the effects of its actions, should be trained to receive the maximum reward. To do that, the learning system has to find the best action by trying each action in turn [33, 36].

ML is used to provide new insights to optimize decision making and enable intelligent operations leading to transformational business outcomes [28]. According to Anderson et al. [28], analytical functionalities can be integrated on the information or control domain of an IoT architecture[3]. The analytics results can then be either applied on the control, application, operation or business domain with different time horizons. On the implementation viewpoint, design considerations need to be made in order to place the defined analytic functionalities on the 3-tier architecture. Design considerations are e.g. the analysis system's response time and reliability or the volume, velocity and variety of the data and the scope of analytics which are deployed[4] [28]. The described Analytical Framework is used to derive functionalities of ML in the IoT.

3. Related Work

In the following, research approaches are shown to present examples of the integration between DLT and AI. From a use case perspective, Swan [37] analyses the potential of deep learning algorithms based on enterprise blockchains. The work identifies its usage across supply chains, higher education and healthcare [37].

Smetana et al. [38] evaluate the fusion of neural networks and blockchain in the field of cyber physical systems and its application for material flow analysis and life cycle assessment. The work concludes that a network of both systems would result in a more efficient system for the named purposes. Therefore, the neural network takes over the task of information processing and modeling whereas blockchain functions as the verification unit [38]. In addition, Harlev et al. [39] use supervised ML to reduce anonymity of the Bitcoin blockchain [39]. Another convergence of AI and DLT is the application of autonomous bots on DLT networks. It speaks about the benefits of costs, peer-to-peer (p2p) data sharing by running the AI algorithms on hybrid data systems combining central servers and decentralized networks controlled by DLT. Furthermore, the article outlines the challenges due to the required decentralized processing of data while scalability problems and real-time requirements exist [40]. Generally, cryptocurrencies and smart contracts could form the basis for AI techniques and guarantee a legal and safe execution [41]. Van Loon [42] states that due to the decentralized data control, data sharing and

[3] A deeper explanation of the functional domains can be found in section 2.1 and [4]

[4] Further design considerations with a deep explanation can be found in [28]

additional security of DLT, AI can be further developed [42].

A far-reaching vision of the AI-DLT connection is developed by Swan [37]. Personal thinking chains, digital mindfiles and digital advocates could be implemented through an input-processing-output architecture. IPFS (InterPlanetary File System) is suggested as a continuously running memory enhanced by AI functionalities to mimic a thinker's memory. As the processing tier, blockchain could be an addition to deep learning algorithms in order to provide brain functionalities. This could result in e.g. a proof of intelligence consensus algorithm in which a new idea could form a stake to participate in the consensus mechanism. In summary, a friendly AI would be realized using blockchain as a governance layer for the implementation of AI techniques [37].

Marr [43] summarizes three benefits of the AI and DLT fusion. First, AI could unlock the value of the encrypted DLT data, using techniques that process encrypted data in a safe manner. Additionally, DLT could record the decision-making process of AI. Third, AI can be used to manage DLT protocols more efficiently [43].

Xain's Practical Proof of Kernel Work (PoKW) combines Proof of Work (PoW) with ML coordinated by models of optimization. In the IoT there is a high dynamic of network nodes. Therefore, the PoKW integrates ML to adapt to this dynamics in a secure, scalable and stable way [44]. Another direction of the convergence is implemented by Morpheo. The blockchain is used to record ML computations and coordinates ML prediction requests to build a ML platform on sensitive data sets [45].

How DLT and AI can be used in the IoT is another relevant question. Kouicem et al. [46] evaluate AI neural networks, on the one side, to be applied to detect Denial of Service attacks. DLT, on the other hand, provides the benefits of decentralization, pseudononymity and security of transactions in the IoT [46]. Khan and Salah [47] describe additional address space, identity, governance, authentication and authorization as further functionalities of DLT [47].

The aforementioned research shows that there is a potential in combining DLT and AI. All the shown work is in an early conceptual or implementation state. Furthermore, the usage of AI and DLT are separately analyzed in the IoT. In contrast to the provided research, this paper conceptualizes the combined application of specifically ML and DLT in the IoT. To the best of knowledge, currently, there is no research work focusing on this topic and a first step into this direction would be done by the result of this article.

4. Methodology

A Design Science Research (DSR) approach using qualitative methods in Information Systems (IS), as the problem area, was selected to apply knowledge in order to solve the practical problem defined in the research question of this paper [48, 49, 50]. DSR adheres to the engineering model of research aiming at an artifact development. Qualitative research methods can be used for the design and evaluation of the scientific innovative output [49, 51]. Developed artifacts comprise constructs, methods, models and instantiations[5] [48, 49]. The artifact construction and evaluation form two intertwined and iterative steps to gain relevant knowledge in IS [49, 50, 52]. Therefore, the design is a sequence of expert activities, whereas the evaluation provides new information to the improvement of the product and process [50]. As the result of this paper, a model describing the relation between DLT and ML enabling AAs in the IoT was created. A model, used as a representation of things, describes the relation between concepts to provide a useful practical outcome and relevance for the IS design [49]. Qualitative interviews and literature inquiry were used as research methodologies to provide input for the model creation [53]. Due to the complexity of the topic and the dynamic IS environment of DLT and ML, a descriptive evaluation is used to present the model's utility, quality, efficacy and its suitability to the problem solution [50].

Table 1. DSR research process.

Process step	Result
1.Problem identification	- Autonomous IoT asset definition & functionalities - Functionalities of DLT & ML to enable AAs - Interface identification of DLT & ML - Additional problems identified in interviews (see section 5.1)
2.Solution suggestion and objective	- ML and DLT as relevant components to implement AAs in the IoT - Identification of relevant functionalities of ML and DLT in the IoT - Definition of interfaces and identification of synergies between ML and DLT
3.Design development	DLT-ML model to visualize relevant interfaces and functionalities in the IoT (see section 5)
4.Demonstration	Acknowledgment of model by relevant stakeholders
5.Evaluation	Definition of arguments and scenarios to show utility, quality and efficacy in relation to the defined problems of step 1 (see section 6)
6.Conclusion and Communication	Summary and publication of results (see section 7)

According to Pfeffers et al. [54], the process of DSR in this paper follows the steps in Table 1. Furthermore, the table provides the results created in each step. Step 1 and 2 are elaborated in the previous sections in which the framework for the following steps is created. The main focus lies in providing transparency of the intersection between DLT and ML in the field of the IoT. This area

[5]Constructs - vocabulary and symbols, models - abstractions and representations, methods - algorithms and practices, instantiations - implementations and protoypes [50]

was further examined in six semi-structured electronic interviews with experts from the field of DLT or ML in an explanatory manner [55]. The interview type was selected because flexibility in the exploration of specific topics wanted to be guaranteed. In one of the interviews two experts were questioned together. Expert 3 was experienced in the AI field whereas expert 4 had knowledge in DLT. Following, the list of experts including their characteristics is shown.

Table 2. Interview expert list.

#	Expertise area	Expert's role	Organization size[6]	Organization type
1	DLT security	Researcher	Medium	Research institute
2	DLT & AI use cases	Head of department	Large	IT service provider and computer manufacturer
3	DLT use cases	Project manager	Large	Information and communication provider
4	AI research & development	Head of department	Large	Information and communication provider
5	DLT & AI innovation	Head of business area	Large	Car manufacturer
6	DLT & IoT development	Chief Technology Officer	Small	DLT-IoT integration
7	DLT & AI development	Project Manager	Small	DLT/AI-IoT integration

The interviews[7] were conducted from May till June 2018 via the Microsoft Skype conference tool in German. Each interview took between 45 and 60 minutes. The questionnaire was structured in 4 parts leading from the overall topic to the specific problem solution: 1) Questions about the person and knowledge level 2) Usage and potential of DLT/ML 3) Challenges in the IoT 4) Application of DLT/ML and interfaces between DLT and ML to solve IoT challenges. The interviews were recorded, transcribed and analyzed according to the content analysis method by two researchers to identify concepts and their relations [56].

5. Results

After the description of functional challenges of the IoT in this section, the model structure is displayed and filled with content from the interviews and literature.

5.1. Problem Identification

According to Burkhardt et al. [10], IoT platforms face multiple challenges along the layers of an IIoT system [10]. The identified challenges of the functional layer were expanded by items named by the experts, condensed and visualized in table[8] 3.

[6]Small<50, Medium<250, Large>250

[7]Transcripts of all interviews are available at the Ferdinand-Steinbeis-Institute

[8]No claim to the completeness of the listed IoT challenges is made

A functional *Vertical & horizontal integration* is

Table 3. IoT functional challenges [10].

1	Vertical & horizontal integration	6	Handling of millions of sensor data
2	Access to relevant data	7	Sensitive data storage
3	Define global truth	8	Context awareness
4	Asset identity, authentication and validation	9	Complex data structures
5	Asset data protection	10	Data quality

relevant to semantically analyze data from various contexts and environments. This provides *Access to relevant data* in order to enable AAs, like a Smart Home assistant. Currently, circumstances that hinders such an integration are the heterogeneity of technologies and protocols as well as the lack of standardization.
Furthermore, a challenge that was identified by the experts is the definition of a global truth between the AAs acting commonly to achieve a pre-defined goal. This requires a mechanism that synchronizes each local state.
Every asset needs to have its unique *Identity* in order to verify data generated by the respective device and it needs to provide secure *authentication*. Without a unique identity other assets are not able to *validate* if the data is actually from the sender asset. Additionally, the data has to be *protected* in the asset itself to guarantee a temper-proved data storage on the asset.
Due to the increasing ubiquity and diversity of edge devices, an increasing amount of *Sensitive data* is generated and needs to be stored according to specific regulations. In a system with different stakeholders providing their services, this is seen as a challenge by the experts. Furthermore, due to the functional heterogeneity of data semantics, *Context awareness* seems to be another demand to realize the IoT. With a variety of data types created, *Complex data structures* evolve that need to be understood in order to execute supportive analysis. This requires data to be received in the required *quality* to guarantee valuable analysis results for the respective business.

5.2. Model Design

The model of Figure 2 visualizes two areas. On the left side, features of AAs are shown. The solution of the described IoT challenges of the previous section is subject to the enablement of these functionalities. The second area is composite of DLT and ML features. Both columns provide a list of features that can be selected to realize AA features. In the following, the functional mapping between the two described areas as well as between DLT and ML is displayed using input from the conducted interviews.

Based on the definition of AAs in section 2.2

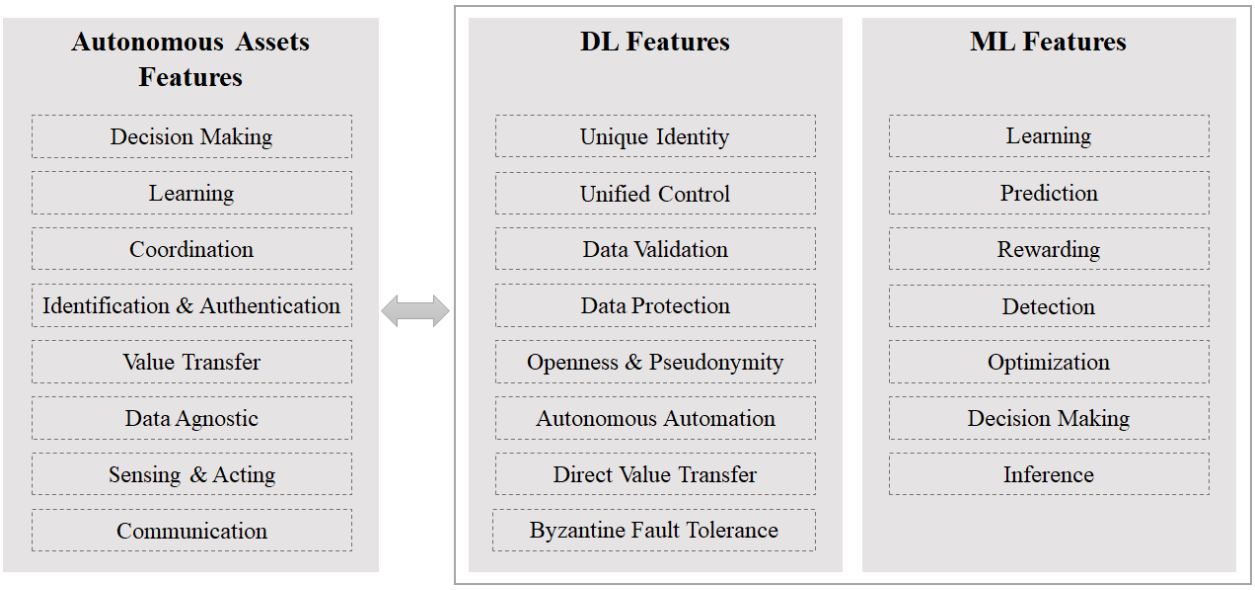

Figure 2. Functional Model

and inputs from the interview experts, eight features that are mapped to DLT and ML features were identified. *Decision making* requires various features to be realized. For example, an autonomous car decides on which direction to go by *predicting* the possible alternatives of directions. The derived prediction models are then compared based on the *detected* outcomes. The resulting direction alternative is then chosen in consideration of different requirements. Furthermore, the experts name the prediction of attacks and predictive maintenance as implementations of the feature *Prediction* to be useful for AAs. Pattern recognition, anomaly detection or correlation identification are in comparison realizations of the feature *Detection*. In a scenario in which multiple assets act with each other to make a decision, a *Unique Identity* of each asset is needed to guarantee trust between assets. The experts name this feature as a possibility for the asset's life-cycle documentation. Furthermore, in a trustful asset interaction *Unified Control* and *Data Validation* are other essential functionalities. Additionally, the experts name *Openness & Pseudonimity* as a prerequisite of the three previous DLT features to enable mutual control and data verification. In order to realize *Unified Control*, DLT provides a common decentralized open database that can be accessed by the assets to control each other, govern, provide data access and homogenize data flows. The experts define *Data Validation* in form of audits, contract verifications, contract conform data storage and prove for non-manipulated data as a further DLT feature. The second feature of AAs is *Learning* enabled by the *Learning* feature of ML and *Data Protection* feature of DLT. Based on various ML methods, *Learning*, described in section 2.4, is realized for model creation and it is used as a basis for the following listed ML features. In an environment in which different unknown assets interact, data on the asset itself needs to be protected in order to guarantee learning statements to be valuable for business. A decentralized temper resistant database using encryption technology like DLT is a requirement to secure data on the device.

Coordination functionality is required in a multi-asset scenario. *Autonomous Automation* implemented through smart contracts, autonomously running on the DLT, guarantee coordination and by the participants agreed upon execution of processes. In order to reach agreements in such an environment, *Byzantine Fault Tolerance* needs to be achieved by mechanisms of DLT. A mutual provisioning of services in the asset network requires *Rewarding* as an incentive for assets to perform actions in favor for each other. *Inference* is another necessary feature of ML to reach agreement on the coordination steps. Furthermore, the experts explain the feature of *Inference* to be used in chatbots or artificial assistants. *Optimization* of the coordination process and arrangement of assets is provided by ML to improve efficiency. An example named by the experts is the improvement of machine utilization.

Identification & Authentication is necessary to facilitate mutual trust between the assets. *Unique Identity, Data Validation* and *Unified control* are essential features of DLT for realization.

For the implementation of Machine-to-Machine (M2M)

payments, devices or resource sharing and on-demand insurances, a replacement of intermediaries by DLT is supportive. The DLT feature *Direct Value Transfer* indicates the transfer of value items between assets, like an autonomous car and a charging station.
The assets should not be locked into one environment or dependent on one centralized platform. Therefore, *Data Agnostic* is another feature of AAs enabled through the *Unified Control* of DLT. DLT generic platforms (DLgp), like Ethereum, provide a horizontal integration and data ownership which enables unknown assets to build trust and exchange value [10].
It is concluded that the implementation of *Sensing & Acting* and *Communication* requires other technologies. In summary, DLT enables through its features *Trust & Interoperability* realizing use cases across companies and M2M economy, named by the experts. Nevertheless, other technologies that, for example, guarantee a save data transfer to the DLT are of relevance for implementation. On the other hand, in order to create assets acting autonomously, *Intelligence* provided by the features of ML is required.

5.3. Model: Mapping DLT and ML

The last part of the questionnaire consisted of questions to the identification of DLT and ML interfaces. The experts described various use cases that require an interrelation of DLT and ML. In an ecosystem with various actors, ML can be seen as an independent component running algorithms based on gathered data. For another actor it is obvious which data is gathered and what is the result of the analytics but the improvement of the algorithm or functions is not transparent. Thus, DLT can be used as an integrated component of ML to make such developments comprehensible, e.g. verifiable and traceable algorithms are realized or created models, like neuronal networks, can be saved for comprehensibility on the DLT as a snapshot. With this integration even algorithms can then be rewarded.
Oppositely, ML can be integrated to adapt the consensus algorithm of a DLT protocol to its environment, e.g analytics on the algorithm can be used to improve efficiency or reinforcement algorithms might be integrated for adaption.
Furthermore, 'punctual' insurances can be realized by the combination of DLT and ML. For example, a driver in a car gets insured only when the car is moving. Features to foster *Intelligence* and *Trust & Interoperability* are therefore required. Moreover, smart contracts can be implemented that run on prediction data to execute insurance terms.
Another use case is firmware updates over the air which can be secured and distributed through DLT and ML. For example, the origin of the update can be authenticated by using DLT.
In the described ecosystem of multiple AAs, distributed ML algorithms require data to be authenticated and results to be securely verified for further usage by actors. Therefore, DLT can be used to enable a decentralized network of assets in which data can be saved in a secure and decentralized manner. Use cases, like the Airbnb scenario for cars[9] will be realizable in this way and support the vision of a shared economy.

6. Discussion

In this section, the utility of the previously designed model in accordance to a descriptive evaluation is explained. The evaluation method is used due to the novelty of the research areas of DLT, ML and IoT with the knowledge about its limitations[10]. A descriptive evaluation constructs scenarios and arguments around the artifact to show its utility, quality and efficacy [50].
On the basis of a defined use case that describes the usage of AAs, the model can be used for the subsequent design step. The model supports the identification of features relevant for the implementation of the defined AAs. Following, design scenarios can be created by selecting features of DLT and ML. The created template is seen as a preliminary step to a service or implementation design aiming at connecting the enterprise and edge layer of an IoT system. Based on this template, missing technologies can be added, interfaces can be examined or the replacement of specific features by other technologies can be discussed based on defined implementation or user requirements. Consequently, the model provides transparency of the transition between the use case design and the implementation in the IoT area. Furthermore, it can be seen as a preparation for the technology selection and adjustment with defined requirements.
The model provides the potential to be integrated on the functional level in existing reference architectures, like the IIRA. Thus, the integration expands the reference model with additional functionalities and enhances the technology selection on the implementation viewpoint. Moreover, the described re-usability can lead to a time saving and a cost reduction for the creation of new models or enhancement of existing ones.
Lastly, the development process to build the model provides knowledge that can be reused to create

[9] See turo.com as an implementation example
[10] Limitations are defined in section 7

further models of integration or to include further technologies necessary to realize AAs. For example, in order to implement the feature of *Sensing & Acting*, communication technologies are relevant that can be functionally integrated by following the process of defining features.

7. Conclusion and Outlook

In this paper a DLT-ML model was developed based on a theoretical framework and qualitative interviews in the area of the IoT. The model shows two areas - 'AA features' and 'DLT & ML features'. The AA features depict functionalities relevant for the implementation of AAs. In the second area, DLT and ML features are listed to provide Trust, Interoperability and Intelligence. The paper describes the connections between both model areas aiming at conceptualizing the enablement of autonomous IoT assets. Furthermore, the examination of interfaces between DLT and ML is of additional focus.

A limitation of this research work is the early stage of DLT and ML in practice. Especially, DLT was named by the experts to lack in a certain level of standardization. For a productive implementation this is seen as a requirement. Moreover, the early research stage of both technologies prevents an integrated implementation in practice. A statement to the model's generalization can not be made due to the limited amount of conducted interviews. Thus, the model needs to be discussed by additional research and practical experts or implementations based on the model need to be developed in order to evaluate its usability. As done in Burkhardt et al. [10] the challenges for ML in the IoT need to be identified in order to guarantee a profound integration. However, the model is seen as a first step of the combined DLT-ML integration in the IoT.

As part of future work, the model requires detailing, for example in form of feature and interface specifications. Implementations can be used to create knowledge relevant for this specification. The transfer of the model to the 3-tier architecture of the IIRA can be seen as a preparational step for the implementation of AAs. The impact of regulations on the technologies and architecture is also relevant to be observed. Finally, other technologies need to be examined functionally and integrated in the model for a profound realization of AAs in the IoT. This leads to an integrated implementation, identification of enterprise impacts and discovery of missing components.

References

[1] K. Zhou, T. Liu, and L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery, ([Piscataway, New Jersey]), pp. 2147–2152, IEEE, 2015.

[2] Capgemini, "The deciding factor: Big data & decision making," 2012.

[3] A. Rassa, "Why un-silo-ing your data will boost your company's efficiency and productivity," 2017.

[4] S. W. Lin, B. Miller, J. Durand, G. Bleakley, A. Chigani, R. Martin, B. Murphy, and M. Crawford, "The industrial internet of things volume g1: Reference architecture: Iic:pub:g1:v1.80:20170131," 2017.

[5] G. E. Digital, "An executive guide to cyber security for operational technology: Securing critical assets in a digitally connected world," 2017.

[6] S. Schrecker, H. Soroush, J. Molina, J. Caldwell, D. Meltzer, F. Hirsch, J. P. Leblanc, M. Buchheit, A. Ginter, R. Martin, H. Banavara, S. Eswarahally, K. Raman, A. King, Q. Zhang, P. MacKay, and B. Witten, "Industrial internet of things volume g4: Security framework: Iic:pub:g4:v1.0:pb:20160926," 2016.

[7] L. Lachance, "It vs. ot für das industrielle internet - zwei seiten einer medaille?," 2016.

[8] A. Karmarkar, F. Hirsch, E. Simmon, and E. Bournival, "The industrial internet of things volume g8: Vocabulary: Iic:pub:g8:v2.00:pb:20170719," 2017.

[9] R. Kranenburg van and A. Bassi, "Iot challenges," 2012.

[10] D. Burkhardt, P. Frey, S. Hiller, A. Neff, and H. Lasi, "Distributed ledger enabled iot platforms symbiosis evaluation," Springer (submitted: Apr. 2018), 2018.

[11] G. Lenz, "The data of things: How edge analytics and iot go hand in hand," 2015.

[12] Z. Javeed, "Edge analytics – the pros and cons of immediate, local insight," 2018.

[13] H. Holec, Autonomy and foreign language learning: Prepared for the Council of Europe. Council of Europe Modern Languages Project, Oxford: Pergamon Press, 1981.

[14] L. Scally, M. Bonato, and J. Crowder, "Learning agents for autonomous space asset management (laasam)," Advanced Maui Optical and Space . . ., 2011.

[15] A. Kemper, P. C. Lockemann, G. Moerkotte, H.-D. Walter, and S. M. Lang, "Autonomy over ubiquity: Coping with the complexity of a distributed world," in In Proc. Ninth Intl. Conf. on Entity Relationship Approach, 1990.

[16] R. Kissel, Glossary of key information security terms: NISTIR 7298 Revision 2. National Institute of Standards and Technology, 2013.

[17] D. Uckelmann, M. Harrison, and F. Michahelles, eds., Architecting the internet of things. Berlin and Heidelberg and New York: Springer, 2011.

[18] A. Abel and S. Sukkarieh, "The coordination of multiple autonomous systems using information theoretic political science voting models," in Proceedings 2006 IEEE/SMC International Conference on System of Systems Engineering, (New York), pp. 149–154, IEEE, 2006.

[19] K. Krukow, M. Nielsen, and V. Sassone, "Trust models in ubiquitous computing," Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, vol. 366, no. 1881, pp. 3781–3793, 2008.

[20] M. Nielsen, K. Krukow, and V. Sassone, "A bayesian model for event-based trust," Electronic Notes in

Theoretical Computer Science, vol. 172, pp. 499–521, 2007.

[21] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: A survey," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 1–27, 2018.

[22] D. Burkhardt, M. Werling, and H. Lasi, "Distributed ledger definition & demarcation," IEEE (submitted: Feb. 2018), 2018.

[23] P. Tasca and C. J. Tessone, "Taxonomy of blockchain technologies. principles of identification and classification."

[24] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in Exploring Services Science (S. Za, M. Drgoicea, and M. Cavallari, eds.), vol. 279 of Lecture Notes in Business Information Processing, pp. 12–23, Cham: Springer International Publishing, 2017.

[25] J. Kruijff and H. Weigand, "Understanding the blockchain using enterprise ontology," in Advanced Information Systems Engineering (E. Dubois and K. Pohl, eds.), vol. 10253 of Lecture Notes in Computer Science, pp. 29–43, Cham: Springer-Verlag New York Inc, 2017.

[26] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards: Prepared for the british standards institution (bsi)," 2017.

[27] M. Friedlmaier, A. Tumasjan, and I. M. Welpe, "Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures," SSRN Electronic Journal, 2016.

[28] N. Anderson, W. W. Diab, T. French, K. E. Harper, S. W. Lin, D. Nair, and W. Sobel, "The industrial internet of things volume t3: Analytics framework: Iic:pub:t3:v1.00:pb:20171023," 2017.

[29] G. F. Luger and W. A. Stubblefield, Instructor's Manual for Artificial Intelligence: Structures and Strategies for Complex Problem Solving. Redwood City, Calif.: Benjamin/Cummings Pub. Co, 2nd ed. ed., 1993.

[30] S. Legg and M. Hutter, "A collection of definitions of intelligence," Frontiers in Artificial Intelligence and Applications, 2007.

[31] M. Mills, "Artificial intelligence in law: The state of play 2016 (part 1)," 2016.

[32] M. Mohri, Rostamizadeh A., and Talwalkar A., Foundations of Machine Learning (Adaptive Computation and Machine Learning series). Adaptive computation and machine learning, Cambridge, Mass. and London: The MIT Press, 2012.

[33] M. Abu Alsheikh, S. Lin, Niyato D., and H. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," vol. Vol. 14, NO. 4, 2014.

[34] P. Dammann, "Einführung in das reinforcement learning,"

[35] K. Ajitesh, "Machine learning: Validation techniques," 2018.

[36] I. Maglogiannis, K. Karpouzis, and M. Wallace, eds., Emerging artificial intelligence applications in computer engineering: Real word AI systems with applications in eHealth, HCI, information retrieval and pervasive technologies, vol. 160 of Frontiers in artificial intelligence and applications. Amsterdam: IOS Press, 2007.

[37] M. Swan, "Blockchain for business: Next-generation enterprise artificial intelligence systems," Advances in Computers, Elsevier, 2018.

[38] S. Smetana, C. Seebold, and V. Heinz, "Neural network, blockchain, and modular complex system: The evolution of cyber-physical systems for material flow analysis and life cycle assessment," Resources, Conservation and Recycling, vol. 133, pp. 229–230, 2018.

[39] M. A. Harlev, H. S. Yin, K. C. Langenheldt, R. R. Mukkamala, and R. Vatrapu, eds., Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning, Proceedings of the Annual Hawaii International Conference on System Sciences, Hawaii International Conference on System Sciences, 2018.

[40] M. G. Ribeiro, "Decentralized artificial intelligence and autonomous bots (auto-bots) in distributed ledger/blockchain networks: Towards decentralized and localized operations using software agents (bots) in distributed ledgers/ blockchain," 2018.

[41] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," AI Matters, vol. 1, no. 2, pp. 19–21, 2014.

[42] R. van Loon, "Blockchain potential to transform artificial intelligence," 2018.

[43] B. Marr, "Artificial intelligence and blockchain: 3 major benefits of combining these two mega-trends," 2018.

[44] L. N. Lundbæk, D. J. Beutel, M. Huth, S. Jackson, L. Kirk, and S. Schwerin, "Xain: Practical proof of kernel work & distributed adaptiveness a resilient & scalable blockchain platform for dynamic low-energy networks," no. v 1.2, 2017.

[45] M. Galtier and C. Marini, "Morpheo: Traceable machine learning on hidden data."

[46] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, 2018.

[47] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2017.

[48] J. F. Nunamaker and M. Chen, "Systems development in information systems research," in Twenty-Third Annual Hawaii International Conference on System Sciences, pp. 631–640, IEEE Comput. Soc. Press, 2-5 Jan. 1990.

[49] S. T. March and G. F. Smith, "Design and natural science research on information technology," Decision Support Systems, vol. 15, no. 4, pp. 251–266, 1995.

[50] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," 2004.

[51] M. D. Myers, "Qualitative research in information systems," MIS Quarterly, vol. 21, no. 2, p. 241, 1997.

[52] M. L. Markus, A. Majchrzak, and L. Gasser, "A design theory for systems that support emergent knowledge processes," 2002.

[53] A. Hevner and S. Chatterjee, Design Research in Information Systems: Theory and Practice. Springer US, 2010.

[54] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45–77, 2007.

[55] M. D. Myers and M. Newman, "The qualitative interview in is research: Examining the craft," Information and Organization, vol. 17, no. 1, pp. 2–26, 2007.

[56] L. K. Barriball and A. While, "Collecting data using a semi-structured interview: a discussion paper," Journal of Advanced Nursing, vol. 19, no. 2, pp. 328–335, 1994.