Ontological Smart Contracts in OASIS: Ontology for Agents, Systems, and Integration of Services

Domenico Cantone, Carmelo Fabio Longo, Marianna Nicolosi Asmundo, Daniele Francesco Santamaria and Corrado Santoro

Abstract In this contribution we extend an ontology for modelling agents and their interactions, called *Ontology for Agents, Systems, and Integration of Services* (in short, OASIS), with conditionals and *ontological smart contracts* (in short, OSCs). OSCs are ontological representations of smart contracts that permit to establish responsibilities and authorizations among agents and set agreements, whereas conditionals allow one to restrict and limit agent interactions, define activation mechanisms that trigger agent actions, and define constraints and contract terms on OSCs. Conditionals and OSCs, as defined in OASIS, are applied to extend with ontological capabilities digital public ledgers such as the *blockchain* and the smart contracts implemented on it. We will also sketch the architecture of a framework based on the OASIS definition of OSCs that exploits the *Ethereum* platform and the *Interplanetary File System*.

Introduction

One of the most important features of a decentralized and publicly shared ledger is the elimination of any third-party intermediaries, since they require clients to put total and unquestioned trust on them. This is particularly true when the ledger is also responsible for managing legal contracts in a digital platform. The *blockchain* [6] has been introduced to allow parties of a network to interact in a distributed manner without the requirement of trusted entities. The blockchain is a peer-to-peer public ledger maintained by a distributed network of computational nodes. Blockchain technologies are opening new perspectives in several key aspects such as *Internet of Things* (IoT), healthcare, insurance, energy, communications, and robotics [21], in view of the wide range of benefits they provide. For example, the blockchain

Domenico Cantone, Carmelo Fabio Longo, Marianna Nicolosi Asmundo, Daniele Francesco Santamaria and Corrado Santoro, Department of Mathematics and Computer Science, Viale Andrea Doria, 6, 95125, Catania, ITALY e-mail: {domenico.cantone, fabio.longo}@unict.it, {nicolosi, santamaria, santoro}@dmi.unict.it

guarantees the ownership, transparency, traceability, public availability, continuity, and immutability of digital assets, in an efficient and trust-less environment where censorship is not achievable. One of the most popular applications of the blockchain is a self-executable contract, also called *smart contract* (SC) [18]. The SC is a way of representing contracts into lines of immutable program codes which are allowed to be self-run on a public ledger.

Smart contracts on the blockchain are equivalent to *stored procedures* of databases, and hence they have direct access to low-level mechanisms. Abstractions of smart contracts may provide several advantages. Among these, we recall that it is easier to publish contracts that integrate and operate with several types of digital and non-digital assets, when higher-level and formal representation of their constraints and agreements are provided. In addition, high-level representations of smart contracts are easy readable by human agents, thus enabling a clear understanding of the agreements and the verification of violations outside the digital borders of the application, for example, in a lawsuit context. Finally, such contracts are platform independent, and hence they can be used and shared by several types of applications and systems, for example, in cross-chain applications.

Semantic web tools and languages aim to reach full machine interoperability, to promote common data formats, and to exchange protocols on the web, share and reuse data across applications and across enterprise and community boundaries. In the semantic vision of the web, software agents are enabled to query and manipulate information on behalf of human agents by means of machine-readable data that carry explicit meaning. Thus, data can be automatically processed and integrated by agents, and can be accessed and modified at a higher level in such a way as to increase coherence and dissemination of information. In addition, with the intervention of semantic reasoners, implicit information is processed and inferred as to gain a deeper knowledge of the domain. Moreover, automated reasoning systems allow one to also verify consistency of data and query it. The definition of a specific domain is widely called *ontology* [13, 9]. The *Word Wide Web Consortium* (W3C) recommends the *Web Ontology Language 2* (OWL 2), a knowledge representation language for web ontologies relying on the Description Logic $\mathcal{SROIQ}(\mathbf{D})$[10].

In [4], we presented the *Ontology for Agents, Systems, and Integration of Services*[1] (in short, OASIS), a foundational OWL 2 ontology that defines a request-execute communication protocol for agents, and in particular for *Internet of Agents* (IoA), based on a mutual exchange of ontology fragments that allow a full transparent and high-level interoperability of agents. For example, such ontology fragments allow agents to send and retrieve information from other agents in a transparent way, request other agents the execution of operations without knowing their hardware and software specifications, acknowledge agents for the execution status of the requested actions, and so on. Moreover, OASIS models information about the assignment and the execution of operations, restrictions on requests, connections, and exchange of messages among agents.

[1] http://www.dmi.unict.it/santamaria/projects/oasis/oasis.php

In this paper, we move towards the definition of a semantic blockchain by extending OASIS so as to deal with agreements that can be established by agents and secured on the blockchain without requiring the definition of specific blockchain smart contracts. Such agreements, called *ontological smart contracts* (OSCs), are established by leveraging conditionals that are also used to abstract and formalize behavior constraints, ways of limiting, bounding, or triggering agent actions. OSCs can be secured through suitable smart contracts implemented on the blockchain and allowing storing and retrieving of RDF graphs. We will also sketch the architecture of such a system that exploits the new introduced features of OASIS and based on the *Interplanetary File System* (IPFS) [15]. The latter allows blockchain-based applications to use immutable files of large dimensions without excessively increasing the cost of transactions in terms of computation and crypto-currency. Finally, we provide an implementation on Ethereum of the designed architecture.

The paper is organized as follows. Section 1 deals with related works. Section 2 is devoted to the description of ontological smart contracts in OASIS, whereas in Section 3 we sketch the architecture of a framework based on OSCs exploiting the blockchain and the IPFS. Finally, Section 4 concludes the paper with some final considerations and hints for future work.

1 Related work

Since 2000, several results concerning how agents enter and leave different interaction systems have been presented, by exploiting both *commitment objects* [8] and *virtual institutions* [7]. Only very recently, however, researchers have focused their interest in conjoining the blockchain and ontologies [3]. One of the areas of investigation has been the development of a characterization of blockchain concepts and technologies through ontologies. A theoretical approach looking at the blockchain with an ontological approach has been introduced in [12], whereas [17] proposes a blockchain framework for *semantic web of things* (SWoT) contexts settled as a *Service-Oriented Architecture* (SOA), where nodes can exploit smart contracts for registration, discovery, and selection of annotated services and resources.

Other works aim to represent ontologies within a blockchain context. In [11], ontologies are used as a common data format for blockchain-based applications, though limited to the description of implementation aspects of the blockchain. However, some of the architectural choices presented in this paper to effectively implement OSCs through blockchain are inspired from [11].

The *Blockchain Ontology with Dynamic Extensibility* (BLONDiE) project [19] provides a comprehensive vocabulary that covers the structure of different components (wallets, transactions blocks, accounts, etc.) of blockchain platforms (Bitcoin and Ethereum) and that can be easily extended to other alternative systems.

We proposed in [4] a first version of OASIS, a behavior-oriented ontology for representing agents and their interactions. As far as we know, this represents the first attempt of using semantic web technologies for defining a transparent commu-

nication protocol among agents that abstracts from their implementation details and configurations, for integrating and uniforming agents, and as a representation system for their behaviors and interactions. In [4], we also proposed a prototype version based on two modules of a domotic assistant, called PROF-ONTO, that exploits several features of OASIS in order to enable communication of IoT devices and users in a domotic environment.

2 Ontological smart contracts in OASIS

Before introducing the classes and properties adopted by OASIS to represent smart contracts, we first present *conditionals*. In general, conditionals are used outside the context of digital contracts to put constraints on the execution of actions and to ensure that some conditions are verified before executing a task. Conditionals are OWL sentences that have the fashion of *Semantic Web Rule Language* (SWRL) rules [20] describing operations that must be triggered when certain conditions hold and exchanged among agents. In fact, unlike SWRL rules, which check the consistency of the knowledge base and infer new sentences, OWL representation of conditionals allows OASIS-oriented applications and systems to combine constraints with behaviors, thus extending the expressiveness and providing a higher-level description and representation of agents. Moreover, the introduction of conditionals in OASIS is also justified by the fact that the satisfiability of conditionals does not coincides with the satisfiability of the knowledge base. In fact, violations of conditionals may result in a litigation among agents or may lead agents to actuate alternative plans, without affecting in any way the satisfiability of the knowledge base. In the context of smart contracts, conditionals are used to characterize contract terms, which are clearly expressed provisions that give rise to an obligation and whose breach can lead to a litigation.

Fig. 1 depicts the schema of OASIS conditionals. Conditional are constituted by a consequent (head) and an antecedent (body), both formed by a conjunctive set of atoms. Atoms in their turn comprise the subject of the conditional, the object, the operator describing the action and, possibly, an operator parameter and argument.

Conditional atoms are introduced by means of the following classes:

- *ConditionalAtom*: represents a conditional atom;
- *ConditionalHeadAtom*: represents atoms of conditional consequents and is defined as a subclass of the class *ConditionalAtom*;
- *ConditionalBodyAtom*: represents atoms of conditional antecedents and is defined as a subclass of the class *ConditionalAtom*;
- *ConditionalSubject*: represents subjects of atoms of conditional consequents or of conditional antecedents;
- *ConditionalObject*: represents objects of atoms of conditional consequents or of conditional antecedents;
- *ConditionalOperator*: represents actions of atoms of conditional consequents or of conditional antecedents;

- *ConditionalParameter*: represents parameters of actions considered by conditional consequents or conditional antecedents (the class *ConditionalParameter* includes the classes *ConditionalInputParameter* and *ConditionalOutputParameter*, representing the input and output parameter, respectively);
- *ConditionalOperatorArgument*: defines operator arguments which represent a subordinate characteristic of the conditional operator (for example, "quality check" may be represented by the operator *check* with argument *quality*);
- *ConditionalEntryTemplate*: represents templates of the features that the entities involved in the conditional, which are introduced by means of the object-property *refersAsNewTo*, must satisfy.

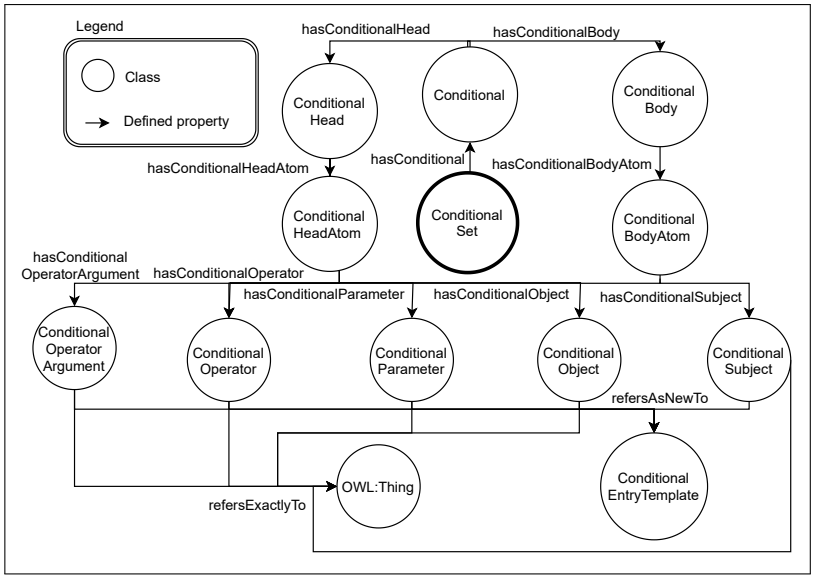

Fig. 1 Ontology schema of conditionals

Conditionals are introduced in OASIS by means of the following classes:

- *Conditional*: defines conditionals, constituted by a consequent (head) and an antecedent (body), both consisting in a conjunctive set of atoms;
- *ConditionalHead*: represents consequents (heads) of conditionals;
- *ConditionalBody*: represents antecedents (bodies) of conditionals;
- *ConditionalSet*: represents conjunctive sets of conditionals.

Conditional atoms are related to a subject (instance of the class *ConditionalSubject*), an object (instance of the class *ConditionalObject*), and an operator (instance of the class *ConditionalOperator*), by means of the object-properties *hasConditionalSubject*, *hasConditionalObject*, and *hasConditionalOperator*, respectively. Possibly,

conditional atoms are related to parameters (instances of the class *ConditionalParamenter*) and to operator arguments (instances of the class *ConditionalOperatorArgument*) by means of the object-properties *hasConditionalParameter* and *hasConditionalOperatorArgument*, respectively. Specifically, input and output parameters are introduced through the object-properties *hasConditionalInputParameter* and *hasConditionalOutputParameter*, respectively.

In OASIS there are two ways to connect conditional entries (i.e., instances of *ConditionalSubject*, *ConditionalObject*, *ConditionalOperator*, *ConditionalParamenter*, and *ConditionalOperatorArgument*) to the related entities, namely by exploiting the object-property *refersExactlyTo* and by exploiting the object-property *refersAsNewTo*.

The first way consists in directly indicating the individual involved in the conditional by means of the object-property *refersExactlyTo*, e.g., the address of a digital wallet of a specific person. In the second modality, the entry is unknown, but there is a set of desirable features that the entry must have in order to make the conditional satisfied when it is checked. For example, if a digital asset is sold to anyone who sends the correct amount of money to a digital wallet, the buyer (the conditional entry) is not known until he performs the transaction: completing a transaction is the feature required in order to consider an entity as a buyer. In such a case, the object-property *refersAsNewTo* is used to specify an instance of the class *ConditionalEntryTemplate*, which endows the set of features that must be satisfied by the conditional entry.

Instances of the classes *ConditionalHead* and *ConditionalBody* are related to instances of the classes *ConditionalHeadAtom* and *ConditionalBodyAtom*, representing conditional atoms through the object-properties *hasConditionalHeadAtom* and *hasConditionalBodyAtom*, respectively. The object-properties *hasConditionalHeadAtom* and *hasConditionalBodyAtom* are defined as subproperties of the object-property *hasConditionalAtom*.

Finally, conditionals are introduced in OASIS by way of instances of the class *ConditionalSet*. Such instances are linked through the object-property *hasConditional* to instances of the class *Conditional*, which in their turn are linked to instances of the classes *ConditionalHead* (representing the consequent) and *ConditionalBody* (representing the antecedent) by means of the object-properties *hasConditionalHead* and *hasConditionalBody*, respectively. Example of conditionals in OASIS can be found in the extended version of this paper [5].

Smart contracts benefit from the abstraction layer provided by suitable ontological models, since they are defined at a higher level, leaving the implementation details to the underneath layer constituted by blockchain-based distributed computing platforms such as *Ethereum*.[2] With this in mind, conditionals are exploited to define ontological smart contracts in OASIS according to the schema illustrated in Fig. 2.

Anytime two parties agree to take action, in order to make an exchange or payment for something of value, a contract is created (instantiated). We call such a contract actuation a *contract instance*. For example, in the case of trading agents, the contract specifies a template of the general agreements that trader and clients shall respect,

[2] https://www.ethereum.org

whereas the contract instance is the application of such a template, specifying how the two parties join the contract: the trader and the client instantiate a general brokerage contract, where the trader is responsible for selling stock on behalf of clients. In OASIS, smart contracts are introduced by the class *SmartContract*, whereas contract instances are modelled by means of the class *SmartContractInstance*. Smart contracts and smart contract instances are connected through the object-property *consistsOfSmartContractInstance*.

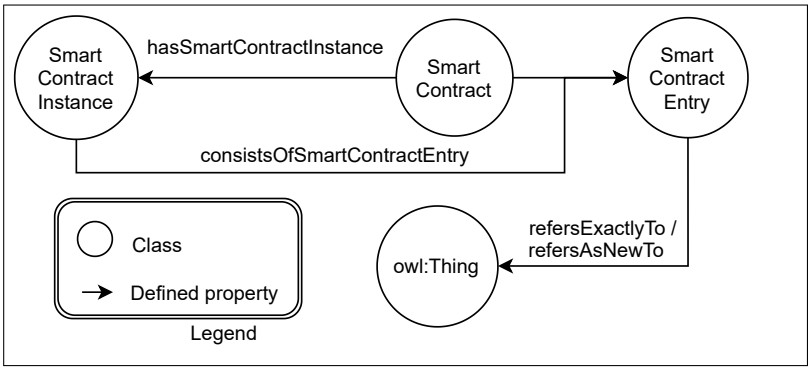

Fig. 2 Ontology schema of smart contract

Smart contracts and smart contract instances provide a set of entries mapped by instances of the class *SmartContractEntry*, the latter containing the classes *SmartContractEntryParticipant* (including individuals referring to the participants involved in the smart contract) and *SmartContractEntryValue* (including individuals referring to values involved in the smart contract). The object-property *consistsOfSmartContractEntry* links smart contracts and smart contract instances to the corresponding entries. Entries of the contract instances are connected to the corresponding contract entries by means of the object-property *refersExactlyTo*. An example of contract in the context of trading agents can be found in [5].

Conditionals are used to characterize constraints among the entries of a smart contract and to establish agreements. Agreements may be easily verified through a SPARQL query, whose result validates (or invalidates) the contract between the two parties. Ontological smart contracts model agreements among parties, whereas SPARQL query validate them: what the ontology does not guarantee is that the parties have actually agreed to the clauses of the contract, its traceability, non-repudiation, and so on, features that a blockchain framework, instead, may ensure.

3 Architectural design of a OSC-oriented application

As stated above, ontological smart contracts may enjoy from a decentralized ledger such as the blockchain. However, it is prohibitively expensive to store a lot of data on

it. For instance, at the time of this writing, about 50 US dollars are required to store the 38 pages of the PDF version of the Ethereum yellow paper, which weights about 520Kb. In fact, according to the paper itself, approximately 20,0000 gas are required for storing 256 bit/8 bytes (1 word), namely 20 Gwei for a unit of gas (1 Gwei equals 0.000000001 Ethers). In order to reduce the cost of transactions and the time required to compute them, data-oriented applications need to rely on a decentralized server to store information. The *Interplanetary File System* (IPFS) is one of the preferred solutions. Basically, IPFS allows one to store a large amount of files, whose permanent IPFS links (CID) can be included into blockchain transactions, in such a way as to put a timestamp on the data and secure it without directly including files in the chain itself. It is sufficient to upload documents on IPFS and then to store the IPFS CID on the Ethereum blockchain. The CID is a hash obtained from the file which, hence, cannot be modified. However, IPFS provides the *InterPlanetary Naming Service* that uses the peer ID to point to a specific hash. Such a hash can change whereas the peer ID cannot. It turns out that applications can gain access to mutable content in IPFS without knowing the new hash beforehand.

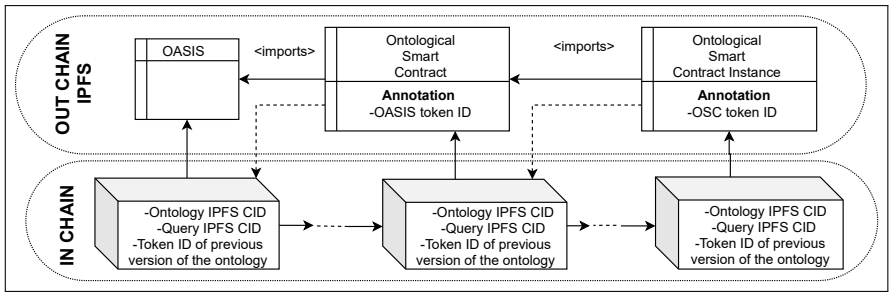

Fig. 3 Sketch of the architecture of an OASIS OSC-based application

Fig. 3 illustrates a typical application that exploits OASIS ontological smart contracts. Ontologies are secured on the blockchain by means of transactions containing only three states: the IPFS CID of the ontology, the IPFS CID of the query required to validate the ontology, and the address of the transaction that secured the previous version of both the ontology and the corresponding query. As a preliminary step, the ontology OASIS and all the ontologies required by the OSC are published on IPFS and secured through a blockchain transaction.[3] From then on, a second transaction suffices for deploying the OSC. Such a transaction secures the ontology representing the OSC, the query that validates the OSC itself, and the address of the transaction that secured, possibly, a previous version of the OSC and of the query. Analogously, any instance of the smart contract and any related ontology are secured by an additional transaction.

[3] The smart contract is compliant with the non-fungible token standard ERC721 and is available in the Ethereum main network at the address 0x36194ab80f7649572cab9ec524950df32f638b08. A Java API to publish and retrieve OSC is available at https://github.com/dfsantamaria/CLARA.

The IPFS CID of the ontology allows one to access the OSC and to ensure that the OSC and all the imported ontologies have not been modified after their publication, thus guaranteeing that all the ontologies exploited by the contract are exactly the ones on which an agreement has been reached. An additional source of guarantee is the SPARQL query that checks whether the ontological contract is voided by the instance under consideration. As in the case of the ontologies, the SPARQL query is published on IPFS and secured on the blockchain, in the same transaction as the OSC that the query checks. By accessing the secured OSC and the query that validates it, the participants have all the means to validate or invalidate the contract, with all the guarantee of the blockchain system and the versatility of ontologies. Moreover, in our architecture, ontologies may exploit suitable OWL annotation axioms, or alternatively the BLONDiE ontology, to refer to blockchain transactions that secured the imported ontologies. Finally, the ontological approach and the architecture model introduced in this paper may also be adopted in non-Turing-complete blockchains such as Bitcoin, since the effort required to the blockchain is limited to store at most two states pointing to resources located out of the blockchain, plus one state storing the token ID of the previous version of the ontology.

4 Conclusions and Future Work

We presented an extension of the *Ontology for Agents, Systems, and Integration of Services* (in short, OASIS), modelling ontological conditionals and smart contracts. Conditionals, classically applied to set restrictions on agent actions or to activate them when suitable conditions hold, are also used to define contract terms. Contract terms are applied, in their turn, to define ontological smart contracts, which establish responsibilities and authorizations among agents. Conditionals and smart contracts defined by OASIS are exploited to add an ontological level to the blockchain and smart contracts based on it. We also sketched the architecture of a system leveraging the blockchain and the Interplanetary File System (IPFS) to store and retrieve OASIS ontological smart contracts, and we implemented it through an Ethereum smart contract.

In order to extend the integration level of OASIS with blockchains, we plan to integrate and extend BLONDiE, also by considering the ontology as a meta-model extension of OASIS. We also plan to study how OASIS can be exploited by *OntologyBeanGenerator 5.0* [2] inside the JADE framework [1] to generate code for agents and artifacts and how it can be exploited by *CArtAgO* [16], a framework for building shared computational worlds. Finally, we shall extend the set of actions and parameters provided by OASIS with the synset introduced by WordNet [14], in order to make the whole infrastructure multi-language- and meaning-oriented.

References

1. Bellifemine, F.L., Caire, G., Greenwood, D.: Developing Multi-Agent Systems with JADE. Wiley (2007)
2. Briola, D., Mascardi, V., Gioseffi, M.: OntologyBeanGenerator 5.0: Extending Ontology Concepts with Methods and Exceptions. In: Proceedings of the 19th Workshop "From Objects to Agents", Palermo, Italy, June 28-29, 2018. pp. 116–123 (2018)
3. Cano-Benito, J., Cimmino, A., García-Castro, R.: Towards blockchain and semantic web. In: Abramowicz, W., Corchuelo, R. (eds.) Business Information Systems Workshops. pp. 220–231. Springer International Publishing, Cham (2019)
4. Cantone, D., Longo, C.F., Nicolosi-Asmundo, M., Santamaria, D.F., Santoro, S.: Towards an Ontology-Based Framework for a Behavior-Oriented Integration of the IoT. In: Proceedings of the 20th Workshop From Objects to Agents, 26-28 June, 2019, Parma, Italy, CEUR Workshop Proceeding Vol. 2404. pp. 119–126 (2019)
5. Cantone, D., Longo, C.F., Nicolosi-Asmundo, M., Santamaria, D.F., Santoro, C.: Ontological smart contracts in OASIS: Ontology for agents, systems, and integration of services (extended version). In: CoRR. vol. abs/2012.01410 (2021)
6. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016)
7. Esteva, M.: Electronic institutions: from specification to development. IIIA Monograph Series. PhD Thesis **19** (2003)
8. Fornara, N., Colombetti, M.: A commitment-based approach to agent communication. Applied Artificial Intelligence pp. 853–866 (2004)
9. Hofweber, T.: Logic and Ontology. Edward N. Zalta (ed.), The Stanford Encyclopaedia of Philosophy (Summer 2018 Edition) (2018)
10. Horrocks, I., Kutz, O., Sattler, U.: The even more irresistible SROIQ. In: Proc. 10th Int. Conf. on Princ. of Knowledge Representation and Reasoning, (Doherty, P. and Mylopoulos, J. and Welty, C. A., eds.). pp. 57–67. AAAI Press (2006)
11. Kim, H., Laskowski, M.: Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, Finance and Management **25**(1), 18–27 (2018)
12. de Kruijff, J., Weigand, H.: Understanding the blockchain using enterprise ontology. In: CAiSE (2017)
13. Oberle, D., Guarino, N., Staab, S.: What is an ontology? Handbook on Ontologies. Springer (2009)
14. Princeton University: WordNet, A Lexical Database for English (2010), `https://wordnet.princeton.edu`
15. Protocol Labs: The Interplanetary File Systems (IPFS), https://ipfs.io
16. Ricci, A., Piunti, M., Viroli, M., Omicini, A.: Environment Programming in CArtAgO. In: Multi-Agent Programming: Languages, Tools and Applications. pp. 259–288. Springer US, Boston, MA (2009)
17. Ruta, M., Scioscia, F., Ieva, S., Capurso, G., Pinto, A., Di Sciascio, E.: A blockchain infrastructure for the semantic web of things. In: 26th Italian Symposium on Advanced Database Systems (SEBD 2018) (2018)
18. Szabo, N.: Formalizing and securing relationships on public networks. First Monday **2**(9) (1997)
19. Ugarte Rojas, H.E.: A more pragmatic web 3.0: Linked blockchain data. In: Google Scholar (2017)
20. World Wide Web Consortium: SWRL: A Semantic Web Rule Language Combining OWL and RuleML (2004), http://www.w3.org/Submission/SWRL/
21. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: Software Architecture (ICSA), 2017 IEEE International Conference on. pp. 243–252. IEEE (2017), http://design.inf.usi.ch/sites/default/files/biblio/icsa2017-blockchain.pdf