Blockchains through ontologies: the case study of the Ethereum ERC721 standard in OASIS

Giampaolo Bella, Domenico Cantone, Cristiano Longo,
Marianna Nicolosi-Asmundo, **Daniele Francesco Santamaria**

Department of Mathematics and Computer Science, University of Catania

16 September, 2021

Introduction

- The blockchain is a peer-to-peer public ledger maintained by a distributed network of computational nodes.
- 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.
- The blockchain guarantees the ownership,transparency, traceability, public availability, continuity, and immutability of digital assets, in an efficient and trust-less environment where censorship is hardly achievable.

- Towards Semantic Blockchains.
- A formal semantic knowledge representation capturing blockchain and smart contracts
  - facilitates the understanding of blockchain concepts,
  - the interlinking with other out-of chain information,
  - enables the automatic discovery of smart contracts.
  - realizes semantic blockchains:
    - A desirable feature of token exchange systems is a precise and intelligent query mechanism capable of determining what, when, and how certain assets have been generated, exchanged or destroyed.
- 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.
- We focus on OWL 2 ontologies.

- A formal semantic knowledge representation capturing the blockchain smart contracts
  - facilitates the understanding of blockchain concepts
  - the interlinking with other out-of chain information
  - enables the automatic discovery of smart contracts
- A desirable feature of token exchange systems is a precise and intelligent query mechanism capable of determining what, when, and how certain assets have been generated, exchanged or destroyed.
- Semantic web tools and languages aim to reach full machine interoperability, to promote common data formats, to exchange protocols on the web, and to share and reuse data across applications and across enterprise and community boundaries.

- Many works aim to to provide ontologies for blockchain contexts, in particular:
  - Blockchain Ontology with Dynamic Extensibility (BLONDiE) project (Ugarte Rojas, 2017) provides a comprehensive vocabulary that covers the structure of different components of three main blockchains, Ethereum, Bitcoin, Hyperledger.
  - Ethon ontology (Pfeffer et al., 2016), providing a semantic interpretation of smart contracts as services.
- The main limitation of the approaches is the poor semantic description of smart contracts, thus hindering the discovery of unknown smart contracts and of the related operations fulfilled during their life-span.

- We extend the ontology **OASIS**, *Ontology for Agents, Systems, and Integration of Services* (Cantone et al., 2019) to semantically represent blockchain, smart contracts, and tokens through Web Ontology Language 2 (OWL 2) ontologies.
- Two steps are required:
  - Extending OASIS with conditionals and ontological smart contracts (OSCs). Conditionals allow one to restrict and limit agent interactions, define activation mechanisms that trigger agent actions, and define constraints and contract terms on OSCs. OSCs are representations of smart contracts that allow to establish responsibilities and authorizations among agents and set agreements. **(In the previous talk)**
  - Extending OASIS with definition of blockchain and the operational semantics of smart contracts, limited to the case study of the Ethereum ERC721 standard protocol for managing non-fungible tokens (NFTs). **(In this work)**

Goal

In this work:

- Ontological representation of the Ethereum blockchain.
- Ontological representation of general-purpose Ethereum smart-contracts.
- Ontological representation of Ethereum ERC721 smart-contracts.
- Ontological representation of Ethereum ERC721 tokens.
- Ontological representation of Ethereum ERC20, ERC1155 smart-contracts and tokens (**work in progress**).
- A vision of indexed blockchains where queries over semantics of transactions are allowed: e.g. "Find all the smart-contracts trading non-fungible tokens about Italian durum wheat".

OASIS

- OASIS models (web) agents and, in particular, the way they interact and operate in a collaborative environment, regardless of the framework and language adopted for their implementation.
- Agents are mainly represented by means of the mentalistic notion of agent behavior inspired by (Bresciani et al., 2004), encompassing goals and tasks that are achievable by the agent, together with actions, sensors, and actuators used to perform operations.
- OASIS is used to define actions that may be requested to other agents and their related information such as operation inputs and outputs. Such requests are submitted by exchanging suitable fragments of OASIS, whereas agents whose capabilities are compatible with the requested actions are discovered by means of SPARQL queries performed over their behaviors.

- OASIS was applied to build a TRL3 prototype of a home assistant that activates and manages applications, devices, and users interacting with each other within the environment (Cantone et al., 2019).
- OASIS is now part of the project POC4COMMERCE for the NGI ONTOCHAIN European project https://ontochain.ngi.eu/.

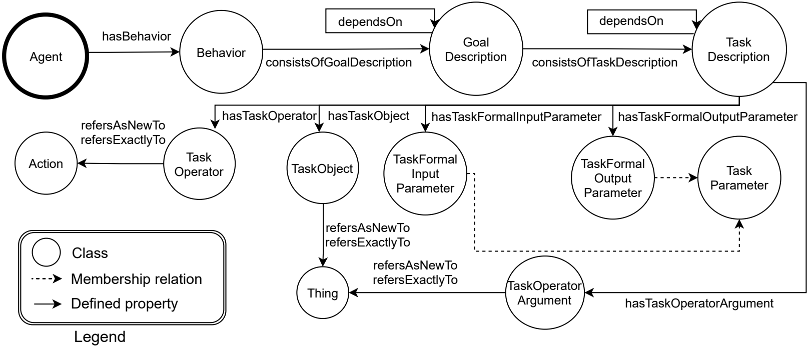
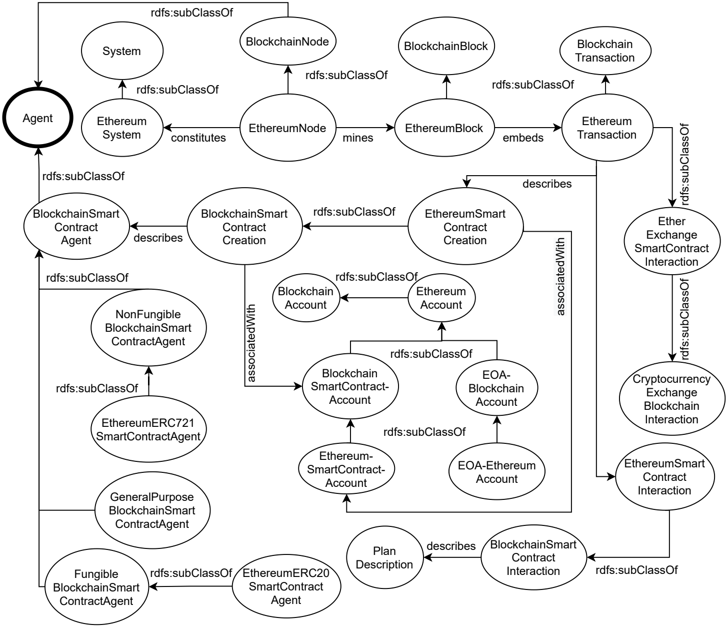


Figure 1: OASIS agent behavior schema

Agents are represented through three steps: a) behavior templates, b) concrete behavior, c) agent requests and agent actions.

Representing Ethereum



Representing Ethereum: example

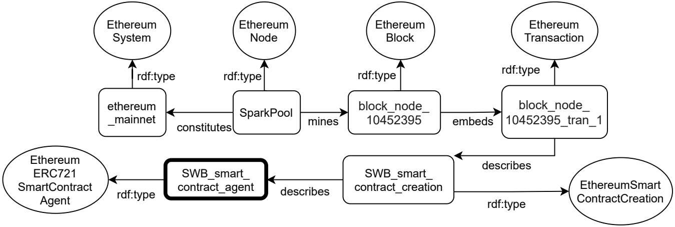


Figure 2: Ethereum representation through OASIS: example

Representing Ethereum ERC721 functions

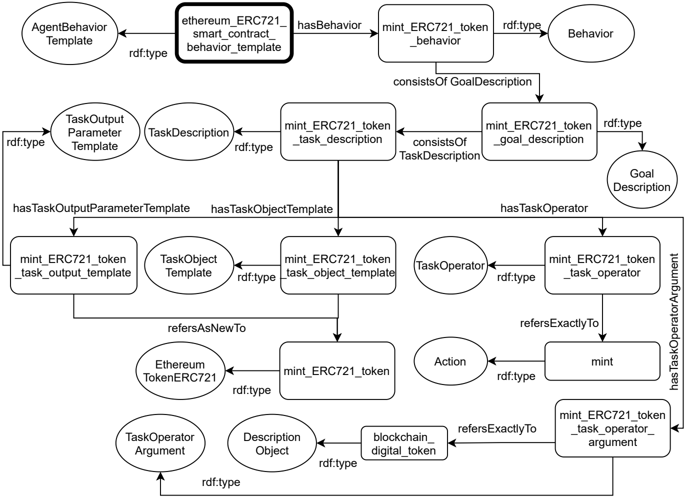

AgentBehavior Template
rdf:type
ethereum_ERC721_ smart_contract_ behavior_template
hasBehavior
mint_ERC721_token _behavior
rdf:type
Behavior
consistsOf GoalDescription
TaskOutput Parameter Template
TaskDescription
rdf:type
mint_ERC721_token _task_description
consistsOf TaskDescription
mint_ERC721_token _goal_description
rdf:type
Goal Description
rdf:type
hasTaskOutputParameterTemplate
hasTaskObjectTemplate
hasTaskOperator
mint_ERC721_token _task_output_template
TaskObject Template
rdf:type
mint_ERC721_token _task_object_template
TaskOperator
rdf:type
mint_ERC721_token _task_operator
hasTaskOperatorArgument
refersAsNewTo
refersExactlyTo
Ethereum TokenERC721
rdf:type
mint_ERC721_token
Action
rdf:type
mint
TaskOperator Argument
Description Object
rdf:type
blockchain_ digital_token
refersExactlyTo
mint_ERC721_token _task_operator_ argument
rdf:type

Figure 3: ERC721 token minting function through OASIS

Representing Ethereum ERC721 functions: example

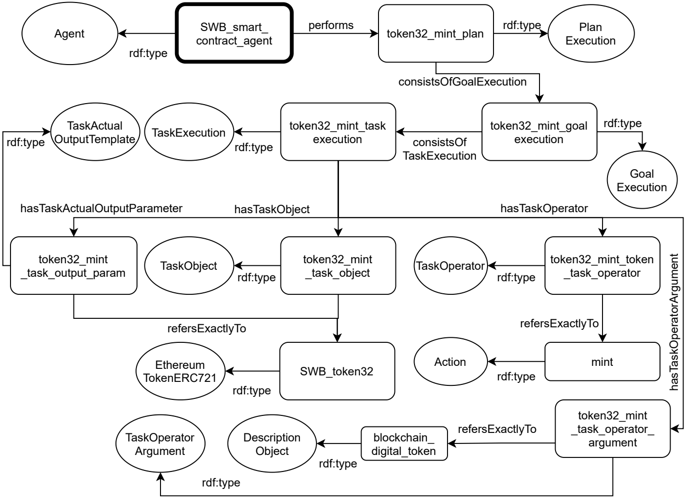


Figure 4: ERC721 token minting function example

Representing Ethereum ERC721 functions

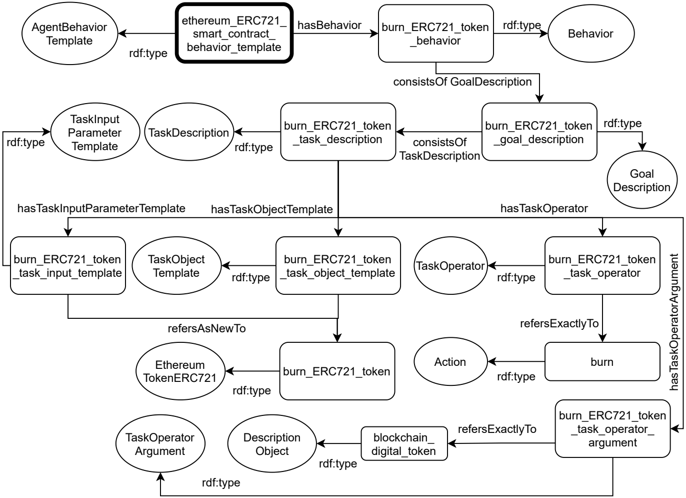
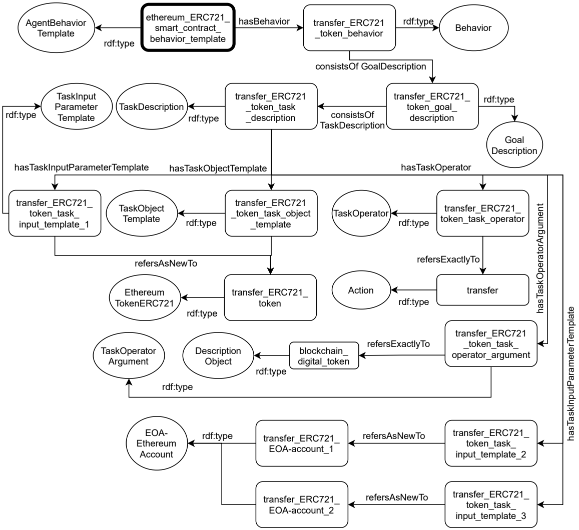

AgentBehavior Template
rdf:type
ethereum_ERC721_ smart_contract_ behavior_template
hasBehavior
burn_ERC721_token _behavior
rdf:type
Behavior
consistsOf GoalDescription
TaskInput Parameter Template
TaskDescription
rdf:type
rdf:type
burn_ERC721_token _task_description
consistsOf TaskDescription
burn_ERC721_token _goal_description
rdf:type
Goal Description
hasTaskInputParameterTemplate
hasTaskObjectTemplate
hasTaskOperator
burn_ERC721_token _task_input_template
TaskObject Template
rdf:type
burn_ERC721_token _task_object_template
TaskOperator
rdf:type
burn_ERC721_token _task_operator
hasTaskOperatorArgument
refersAsNewTo
refersExactlyTo
Ethereum TokenERC721
rdf:type
burn_ERC721_token
Action
rdf:type
burn
burn_ERC721_token _task_operator_ argument
refersExactlyTo
TaskOperator Argument
Description Object
rdf:type
blockchain_ digital_token
rdf:type

Figure 5: ERC721 token burning function through OASIS

Representing Ethereum ERC721 functions



AgentBehavior Template
rdf:type
ethereum_ERC721_ smart_contract_ behavior_template
hasBehavior
transfer_ERC721 _token_behavior
rdf:type
Behavior
consistsOf GoalDescription
rdf:type
TaskInput Parameter Template
TaskDescription
rdf:type
transfer_ERC721 _token_task _description
consistsOf TaskDescription
transfer_ERC721_ token_goal_ description
rdf:type
Goal Description
hasTaskInputParameterTemplate
hasTaskObjectTemplate
hasTaskOperator
transfer_ERC721_ token_task_ input_template_1
TaskObject Template
rdf:type
transfer_ERC721 _token_task_object _template
TaskOperator
rdf:type
transfer_ERC721_ token_task_operator
hasTaskOperatorArgument
refersAsNewTo
refersExactlyTo
Ethereum TokenERC721
rdf:type
transfer_ERC721_ token
Action
rdf:type
transfer
hasTaskInputParameterTemplate
TaskOperator Argument
Description Object
rdf:type
blockchain_ digital_token
refersExactlyTo
transfer_ERC721 _token_task_ operator_argument
rdf:type
EOA- Ethereum Account
rdf:type
transfer_ERC721_ EOA-account_1
refersAsNewTo
transfer_ERC721_ token_task_ input_template_2
transfer_ERC721_ EOA-account_2
refersAsNewTo
transfer_ERC721_ token_task_ input_template_3

Figure 6: ERC721 token transferring function through OASIS

Representing Ethereum ERC721 functions

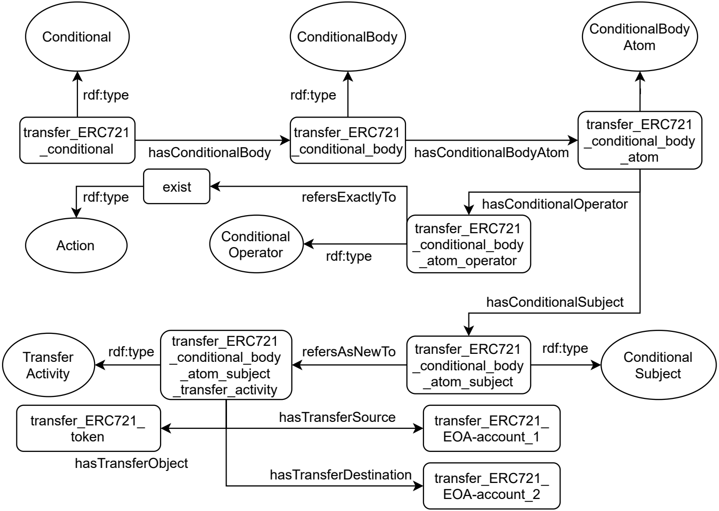


Figure 7: ERC721 token transferring function conditional

Representing Ethereum ERC721 functions

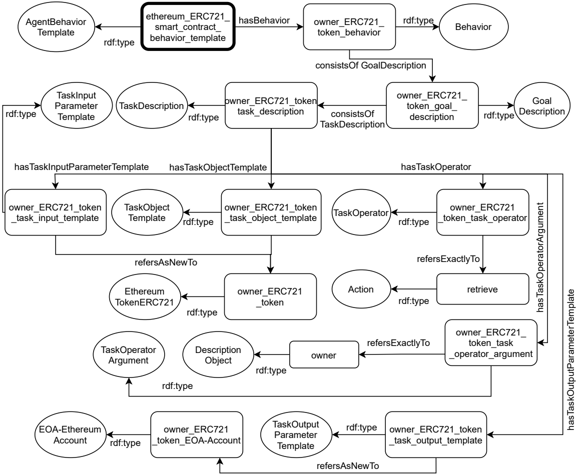

AgentBehavior Template
rdf:type
ethereum_ERC721_ smart_contract_ behavior_template
hasBehavior
owner_ERC721_ token_behavior
rdf:type
Behavior
consistsOf GoalDescription
TaskInput Parameter Template
TaskDescription
rdf:type
owner_ERC721_token task_description
consistsOf TaskDescription
owner_ERC721_ token_goal_ description
rdf:type
Goal Description
rdf:type
hasTaskInputParameterTemplate
hasTaskObjectTemplate
hasTaskOperator
owner_ERC721_token _task_input_template
TaskObject Template
rdf:type
owner_ERC721_token _task_object_template
TaskOperator
rdf:type
owner_ERC721 _token_task_operator
hasTaskOperatorArgument
refersAsNewTo
refersExactlyTo
Ethereum TokenERC721
rdf:type
owner_ERC721 _token
Action
rdf:type
retrieve
hasTaskOutputParameterTemplate
TaskOperator Argument
Description Object
rdf:type
owner
refersExactlyTo
owner_ERC721_ token_task _operator_argument
rdf:type
EOA-Ethereum Account
rdf:type
owner_ERC721 _token_EOA-Account
TaskOutput Parameter Template
rdf:type
owner_ERC721_token _task_output_template
refersAsNewTo

Figure 8: ERC721 token owner retrieving function through OASIS

Representing Ethereum ERC721 tokens

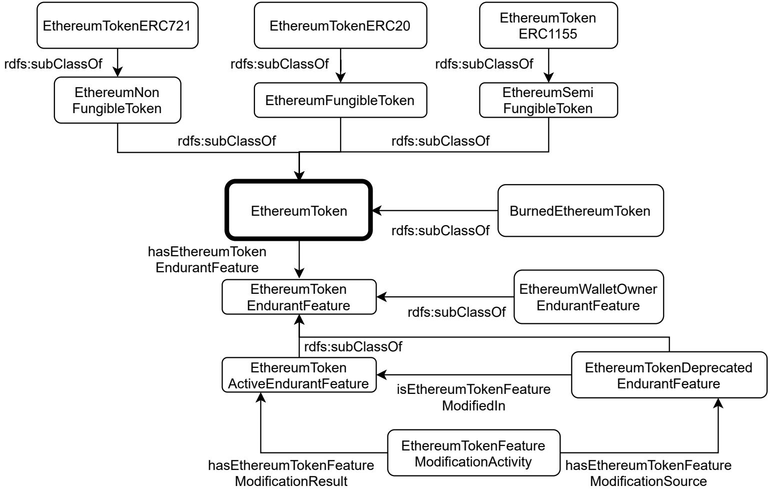

EthereumTokenERC721
EthereumTokenERC20
EthereumToken ERC1155
rdfs:subClassOf
rdfs:subClassOf
rdfs:subClassOf
EthereumNon FungibleToken
EthereumFungibleToken
EthereumSemi FungibleToken
rdfs:subClassOf
rdfs:subClassOf
EthereumToken
BurnedEthereumToken
rdfs:subClassOf
hasEthereumToken EndurantFeature
EthereumToken EndurantFeature
EthereumWalletOwner EndurantFeature
rdfs:subClassOf
rdfs:subClassOf
EthereumToken ActiveEndurantFeature
EthereumTokenDeprecated EndurantFeature
isEthereumTokenFeature ModifiedIn
EthereumTokenFeature ModificationActivity
hasEthereumTokenFeature ModificationResult
hasEthereumTokenFeature ModificationSource

Figure 9: ERC721 tokens in OASIS

References

- (Ugarte Rojas, 2017), A more pragmatic web 3.0: Linked blockchain data, in Google Scholar.
- (Pfeffer et al., 2016) Ethon - an ethereum ontology (2016), available on-line: https://ethon.consensys.net/index.html.
- (Cantone et al., 2019) Towards an Ontology-Based Framework for a Behavior-Oriented Integration of the IoT, Proc. of the 20th Workshop From Objects to Agents, 26-28 June, 2019, Parma, Italy, CEUR Vol. 2404, pp. 119–126, 2019.
- (Bresciani et al. 2004), Tropos: An agent-oriented software development methodology. Autonomous Agents Multi Agent Systems 8(3), 203–236 (2004).