Web Service for Semantic Negotiation of Smart Contracts

Umar Rashid, Allan Third, John Domingue

Knowledge Media Institute, The Open University, UK
{umar.mir, allan.third, john.domingue}@open.ac.uk

Abstract

Distributed ledger platforms based on Blockchains provide a mechanism to store and compute distributed data in a secure way. These platforms can be useful in domains (e.g. education, healthcare) where data integrity is critical. A s*mart contract* refers to the piece of code (i.e. *functions*) and data (i.e. *state*) on the blockchain that is automatically executed when specific conditions are met. However, querying and indexing smart contracts remains a challenging task. To address this issue, we propose a solution that uses a RESTful semantic web service for indexing, browsing and execution of smart contracts on Ethereum Blockchain platform. We have extended Minimal Service Model (MSM) to support semantic negotiation of smart contracts on web. Using Linked Data in combination with smart contracts ensures integrity and discoverability of data computations in distributed applications.

Keywords: Semantic Web, Blockchains, Linked Data, Semantic Negotiation

Introduction

Blockchain-based distributed ledger platforms have become popular with the advent of crypto-currencies such as Bitcoins. These platforms can be used to store as well as to compute distributed data. One of the main benefits of using Blockchain-based solution is its decentralized structure that allows execution of peer-to-peer transactions without mediation of a third party to validate those transactions. Once data is stored on Blockchains, it is shared among all peers and cannot be further edited, thus ensuring transparency and integrity of data. Such platforms can be useful in domains (e.g. finance, education, healthcare) where data integrity is critically important.

A s*mart contract* is a piece of code that automatically performs transactions on the blockchain when specific conditions are met. Smart contracts perform verifiable transactions on the blockchain without a third party interference or supervision that is visible to all peers, thus ensuring fast, transparent and secure transactions. Some proof-of-concept applications using smart contracts have been developed in domains such as land registry [3] and electronic voting [4].

As blockchain-based distributed ledgers are used for storing diverse forms of data and smart contracts, querying them becomes a challenging task. Moreover, there is need to integrate blockchain data with other services on the Web, thus making use of Linked Data tools. Researchers have started investigating how blockchain technologies can

support a more robust Semantic Web and vice versa [1]. Our earlier work [6] presented the proof-of-concept for a Linked Data index onto a distributed ledger.

In this paper, we attempt to investigate if Linked Data solutions and smart contracts can be used together to realize a Distributed Semantic Web that facilitates integrity as well discoverability of distributed data. For that purpose, we introduce a RESTful semantic web service that allows indexing, browsing and invoking smart contracts on Ethereum Blockchain [7] via a URI. We extend the Minimal Service Model (MSM) [3] with Ethereum Ontology (EthOn) [2] to support Ethereum smart contract concepts like cost (i.e. gas). In this way, we are able to be able answer queries such as 'finding a smart contract with the minimal gas payment'.

Related Work

We have borrowed concepts from EthOn and MSM to build our semantic web service for smart contracts.

EthOn

EthOn is an Ethereum ontology that describes Blockchain concepts (e.g. blocks, transactions, contracts) using W3C RDF Schema and the Web Ontology Language.

Contracts Extension

The Contracts extension of the EthOn ontology describes concepts and properties specific to smart contracts such as Functions, Events, Inputs, Outputs and Opcodes. Classes and properties in Ethon Contracts Extension are shown in Figure 1 and Figure 2 respectively.

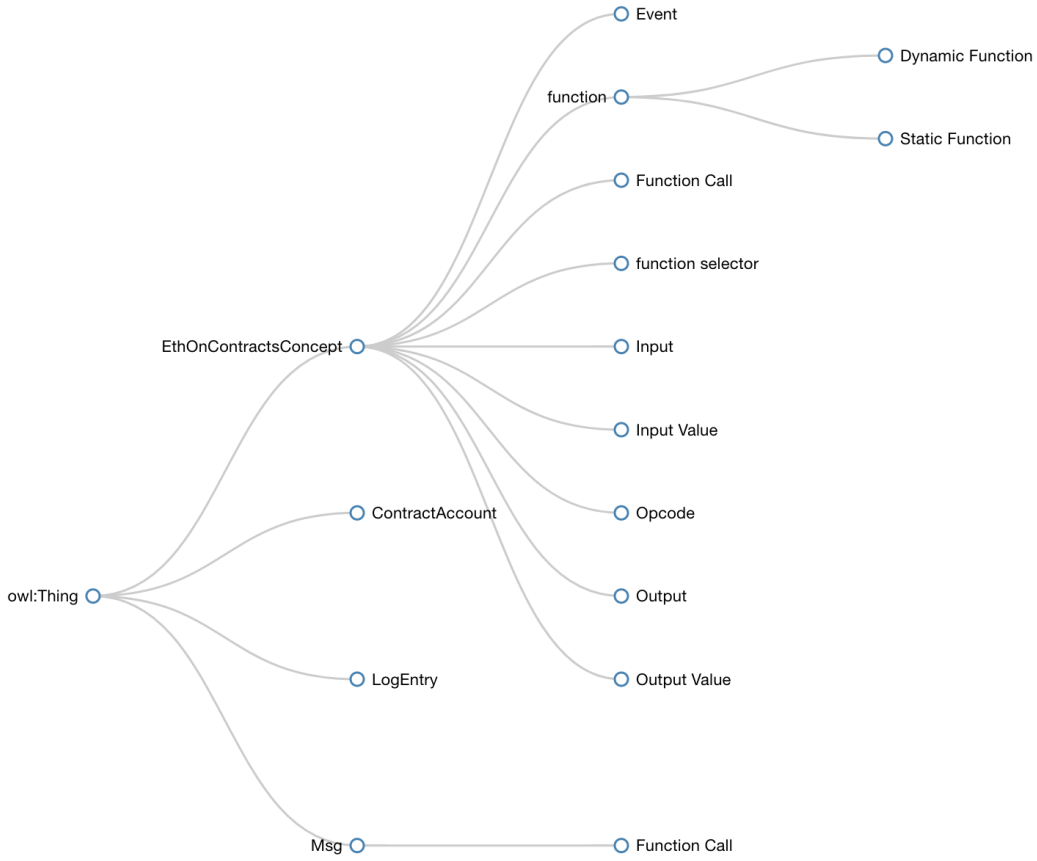

Figure 1: EthOn Classes (15)

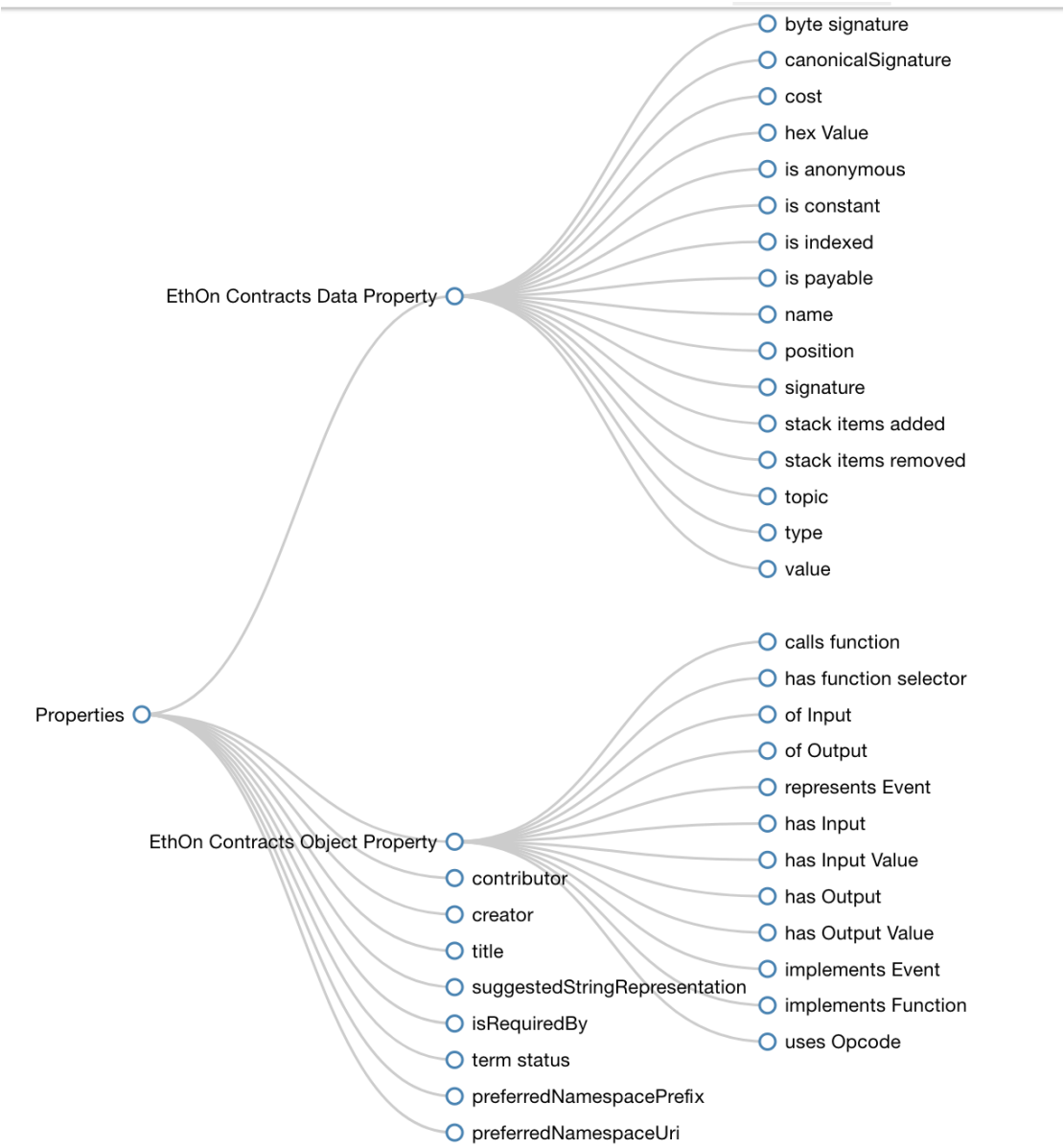

Figure 2: EthOn Properties (38)

Minimal Service Model (MSM)

The MSM [2] defines a service that has a number of Operations. Operations have input, output and fault MessageContent descriptions. MessageContent may be composed of mandatory or optional MessageParts. MessagePart provides support for finer-grained input/output discovery, as available in SAWSDL, OWL-S and WSMO.

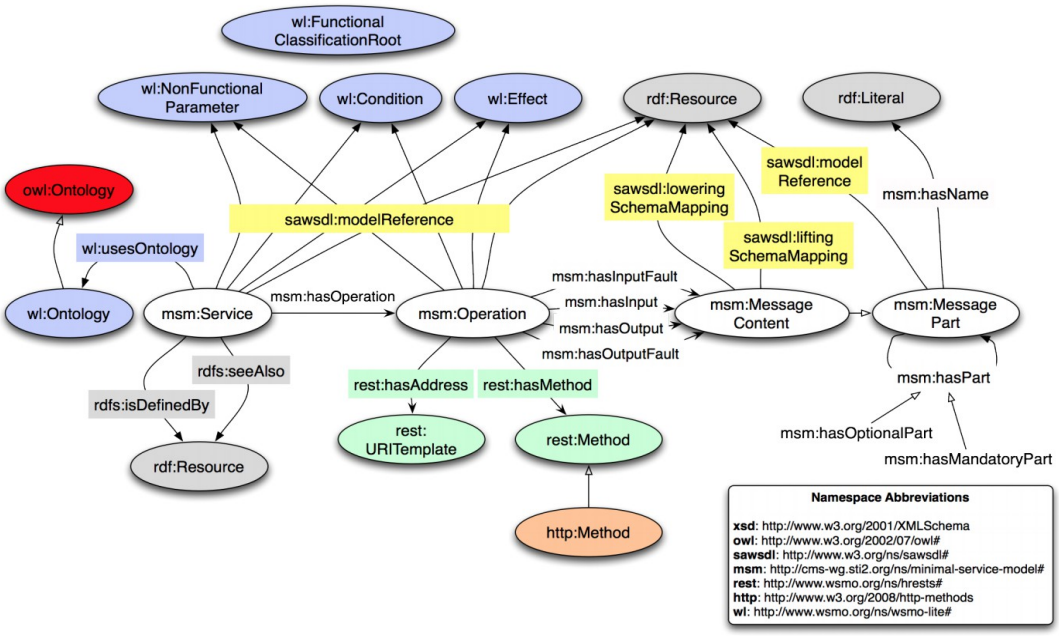

Figure 3: Minimal Service Model

Semantic Web Service for Smart Contracts

Our current work deals with storing educational data on the blockchain and using smart contracts to represent Open Badges [3], where records of students' achievements taking courses with the Open University's OpenLearn platform are stored in our private blockchain. Our aim is to index the data (including smart contracts) and transactions relating to our ongoing work with the educational Open Blockchain [5] using Ethereum.

Using Ethereum *web3* library, we monitor every block that is added to the blockchain and retrieve transactions within that block. When a transaction contains a smart contract, we retrieve the contract address using Ethereum API (i.e. *web3.eth.getTransactionReceipt)*. Then we save smart contract's address, binary, and Application Binary Interface (ABI) each as a triple in the RDF store. ABI describes the names of smart contract's methods and how to call them. We save each methods in ABI as an RDF triple based on an extension of MSM ontology as shown in Table 1.

Table 1. Extended MSM Ontology for Smart Contracts

Smart Contract Methods	**MSM**
Smart Contract ABI	msm:service
Function	msm:operation
Input	msm:messagecontent
Output	msm:messagecontent
Gas	msm:gas (from EthOn Contracts Data Property 'cost')

Using Ethereum API, a smart contract can be called using its address and ABI. However, with our web service, we are able to call a smart contract via a URI with only the contract's address as a parameter. Moreover, we are also able to execute a smart contract method via a URI.

Conclusions

We have introduced a RESTful semantic web service that allows indexing and invoking smart contracts on Ethereum Blockchain via a URI. We extended the Minimal Service Model (MSM) with Ethereum Ontology (EthOn) to support Ethereum smart contract concepts like cost (i.e. gas). In this way, we are able to answer queries such as 'finding a smart contract with the minimal gas payment'.

We have taken an initial step in connecting smart contracts with Linked Data. In future work, we plan to evaluate the performance of this approach, and compare it with other approaches to indexing smart contracts. Moreover, we would like to extend this work to blockchain platforms other than Ethereum.

References:

1. English, M., Auer, S., Domingue, J. Blockchain technologies & the Semantic Web: A framework for symbiotic development. CS Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds. (2016), pp. 47–61.
2. EthOn Ethereum Ontology http://ethon.consensys.net/
3. Goligoski, E. Motivating the learner: Mozilla's open badges program. Access to Knowledge: A Course Journal, 4(1), 2012
3. Pedrinaci, C., Domingue, J.: Toward the Next Wave of Services: Linked Services for the Web of Data. Journal of Universal Computer Science 16(13) (2010), pp. 1694–1719.
4. Rizzo, Pete. Sweden Tests Blockchain Smart Contracts for Land Registry https://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/
5. Sharples, M. and Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In European Conference on Technology Enhanced Learning, Springer, 2016, pp. 490–496.
5. SmartCitiesWorld News. Moscow introduces blockchain e-voting https://www.smartcitiesworld.net/news/news/moscow-introduces-blockchain-e-voting-2365
6. Third, A., Domingue, J.: Linked Data indexing of distributed ledgers. In: Proceedings of the 1st International Workshop on Linked Data and Distributed Ledgers at WWW 2017, pp. 1431–1436.
7. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014)