Semantic-enhanced blockchain technology for smart cities and communities

Michele Ruta, Floriano Scioscia, Saverio Ieva, Giovanna Capurso, Giuseppe Loseto, Filippo Gramegna, Agnese Pinto, Eugenio Di Sciascio
Politecnico di Bari - via E. Orabona 4, Bari (I-70125), Italy
{name.surname}@poliba.it

***Abstract*—Large-scale transactional systems still suffer from not viable trust management strategies. Given its intrinsic characteristics, blockchain technology appears as interesting from this perspective. A semantic layer built upon a basic blockchain infrastructure would join the benefits of flexible resource/service discovery and validation by consensus. This paper proposes a novel Service-oriented Architecture (SOA) based on a semantic blockchain. Registration, discovery, selection and payment operations are implemented as smart contracts, allowing decentralized execution and trust. Potential applications include material and immaterial resource marketplaces and trustless collaboration among autonomous entities, spanning many areas of interest for smart cities and communities.**

Index Terms*—Blockchain, Internet of Things, Semantic Web, Smart cities

I. Introduction

Despite the controversial reputation of *Bitcoin* (https://bitcoin.org/), the *blockchain* technology at its core is intrinsically positive. It is basically a distributed database, which records transactions occurred in a given time span in blocks, chained by means of cryptographic hashes. The reliability of such a structure comes from the fact that every transaction is trusted by consensus of the majority of entities acting in the system. Blockchain enables the execution of *smart contracts* [1], *i.e.*, software stubs which automatically process the terms of an agreement. As people, corporations and government entrust more and more critical data to information systems, trust in the digital world has become increasingly related to the confidence on given "authorities". The fact that such entities could be cracked or counterfeit poses serious security and privacy issues to the diffusion of dematerialized transactions. This is the reason why blockchain could prove to be helpful.

The benefits of Knowledge Representation –and particularly Semantic Web– technologies at resource discovery level in pervasive heterogeneous system stacks are well known [2]. This opens the way toward integrating blockchains with an ontology-based resource/service discovery, leveraging semantics of requests and resource descriptions to refine retrieval strategies. A semantic-enhanced blockchain basically amounts to a Service-Oriented Architecture (SOA) for regulating registration, discovery, selection and payment operations, implemented as distributed smart contracts validated by consensus.

This paper illustrates ongoing work on a novel framework, integrating a semantic-based resource discovery layer in a basic blockchain infrastructure. A distinguishing feature of the systems is *logic-based explanation* of discovery outcomes, grounded on non-standard inference services for semantic matchmaking [3]. The proposed system preserves fundamental blockchain features. Particularly, the effective and secure structure of the chain is capable of preventing erroneous or malicious changes on a transaction block.

More details of the proposed framework are in Section II, while Section III presents relevant application scenarios within smart cities and communities, before closing remarks.

II. Proposed approach

As discussed in [4], [1], several types of blockchain systems exist, based on the following key design decisions: network access policy (either *permission-less*, where any node can join anonymously, or *permissioned*, based on a white list of admitted and identifiable nodes); consensus algorithm (the stricter but heavier *Proof-of-Work* or the lighter *Byzantine Fault Tolerance* (BFT) variants); transaction model (the *unspent transaction outputs* (UTXO) model, suitable for simple e-currency applications, or the more general *account-based* model, which can support general-purpose smart contracts); smart contract language (an existing or purposely defined imperative programming language, or a declarative –logic-based– one, or other kinds of formalisms).

The proposed approach (whose technical details are in [4]) defines a semantic resource/service discovery layer built upon a basic blockchain framework. It allows to compare a request with multiple resource descriptions by taking into account semantics of their annotations referred to a shared ontology. The result is a score measuring the semantic distance between the request metadata and annotations of available chain resources. This logic-based metric induces a well-founded relevance ranking of resources w.r.t. the request, as well as formal *explanation* of outcomes.

Basic primitives are outlined hereafter.

A. Resource registration. Several resource domains co-exist in the same blockchain. Every domain is associated to a different ontology, which provides the reference conceptual vocabulary to annotate resources. Every ontology is uniquely identified by a Uniform Resource Identifier (URI). In order to make a resource available for discovery and usage, the owner node registers it as an *asset* on the blockchain. For greater efficiency, only the resource URI is stored on the blockchain in the registration transaction, while the semantic annotation, the URI of its reference ontology and the resource price are stored in private node memory.

B. Resource discovery. The proposal adopts a *gossip-based* (a.k.a. *epidemic*) approach to disseminate discovery requests and aggregate results. The requester randomly selects n nodes and sends a multicast request, specifying the reference ontology URI, the semantic annotation of the request in Web Ontology Language (OWL)[1], the maximum price it is willing to pay, the minimum semantic relevance threshold, and the maximum number of results to be returned. Nodes receiving the request execute semantic matchmaking of their own resources with the request through an on-board matchmaking engine [3], yielding a relevance-ranked list of results satisfying both semantic relevance and price constraints; they also select other n random nodes and forward the request. Nodes receiving forwarded requests behave in the same way, up to a search depth threshold m. Each queried node returns results to the sender, which propagates them back to the original requester following the same route of the requests.

C. Explanation. This is an optional step in a typical discovery process, invoked when a requester needs a justification of the matchmaking outcome for a specific resource. This can be useful, *e.g.*, in a request refinement process [3].

D. Resource selection. The requester selects the best resource(s) sending a unicast message to the resource owner with the resource URI and contextually a currency payment.

Resource discovery, explanation and selection transactions are recorded on the blockchain for robustness, traceability and accountability purposes.

III. Application areas for smart cities

Semantic-enhanced blockchain systems enable discovery infrastructures for general-purpose machine-to-machine trustless marketplaces with minimal or no human intervention across multiple Decentralized Autonomous Organization (DAOs). This has several applications with potentially transformation impact on relevant sectors for smart cities and communities.

– **Logistics.** Asset tracking and supply chain are among the most popular blockchain applications, due to the easy fit with existing industry standards. The simplest approaches rely on transactional ledgers for asset transfer [1]. Semantic-enhanced blockchains based on smart contracts further allow any application logic to be implemented and embedded in the blockchain, and also support discoverable, composable and verifiable multi-step business processes in multi-party SOAs [5].

– **Industry 4.0**. IoT-based manufacturing benefits from blockchain technologies [1], granting not only a decentralized collaboration infrastructure, but also a ledger for process traceability of production and quality assurance. Semantic-based blockchain evolution can provide greater composition flexibility and rigorous process formalization [4].

– **Utility markets.** Energy, water and natural gas provisioning are increasingly relying on sensor networks, low-level digital control and high-level decision support. Semantic-enhanced blockchains can strongly support visions like the *Smart Grid*, as they provide both resource-oriented discovery processes and a robust ledger for contracts and payments, which are needed in large-scale peer-to-peer decentralized marketplaces.

– **Public sector.** Many public services to the citizenry can be made faster, cheaper and less error prone through process and data dematerialization. Blockchain technology can assist in the interfacing of the information systems of several independent branches and levels of the public administration. Furthermore, it plays the role of verifiable registry in property transfers as well as authentication and notary services. Semantic-based querying capabilities make information and functionalities more accessible to both citizens and decision-makers.

– **Financial services.** Traditional banks and finance institutions, private and public alike, are experimenting with blockchain technology to reduce operating costs of financial transactions management. Semantic-based approaches enable a marketplace of financial services, where atomic building blocks can be automatically discovered, compared and composed in order to provide the most suitable personalized solutions.

IV. Conclusion and future work

This paper described an ongoing work on a semantic-based blockchain enhancement, imbuing classical infrastructures with advanced resource/service discovery. Significant impacts are expected on several domains of smart cities and communities. Early results [4] supported the feasibility of the proposal: performance results were satisfactory up to medium-scale networks, but further optimization is needed, in order to improve and re-evaluate scalability in larger deployments. Further functional evolution and case studies are also under investigation.

References

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[2] F. Scioscia and M. Ruta, "Building a Semantic Web of Things: issues and perspectives in information compression," in *Proceedings of the 3rd IEEE International Conference on Semantic Computing (ICSC 2009)*. IEEE Computer Society, 2009, pp. 589–594.

[3] M. Ruta, F. Scioscia, E. Di Sciascio, F. Gramegna, and G. Loseto, "Mini-me: the mini matchmaking engine," in *OWL Reasoner Evaluation Workshop (ORE 2012)*, ser. CEUR Workshop Proceedings, E. J.-R. Ian Horrocks, Mikalai Yatskevich, Ed., vol. 858. CEUR-WS, 2012, pp. 52–63.

[4] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic Blockchain to improve scalability in the Internet of Things," *Open Journal of Internet of Things*, vol. Proceedings of Very Large Internet of Things Workshop @ VLDB 2017, 2017, in press.

[5] A. Norta, "Creation of smart-contracting collaborations for decentralized autonomous organizations," in *International Conference on Business Informatics Research*. Springer, 2015, pp. 3–17.

[1] OWL 2 Web Ontology Language Document Overview (2nd Ed.), W3C Recommendation, 2012-12-11, https://www.w3.org/TR/owl2-overview/