Enhancing Blockchain Smart-Contracts with Proof-of-Location

Sara Migliorini
Dept. of Computer Science, University of Verona, Italy
sara.migliorini@univr.it
https://orcid.org/0000-0002-1825-0097

Abstract

Proof of Location has been recently revised in conjunction with blockchain technology in order to achieve a distributed and decentralized consensus about the position of events or agents in space and eventually in time. This concept acquires a particular importance in the context blockchain smart contracts, with the aim to describe constraints related to spatial properties of the involved parties. This statement of interest is about the way spatial data types and relations can be effectively included in smart contracts and how such information can be subsequently verified and analyzed in an efficient way.

Keywords and phrases Blockchain, smart contracts, proof of location

A blockchain is a open, distributed ledger that maintains a continuously growing list of blocks. Such blocks typically store a set of ordered transactions between parties in a verifiable and permanent way. Each block is added to the blockchain only when a (distributed) consensus is obtained from the network majority in a decentralized manner, namely without the presence of a trusted central authority. Data on blocks cannot be retroactively modified without altering all the subsequent blocks, namely again without the consensus of the network majority. The main innovation coming with the blockchain technology is that it a high Byzantine-fault-tolerant proof mechanism of all transactions in the network.

The blockchain technology was firstly introduced in 2008 as the decentralized, trustless, public ledger of the digital cryptocurrency Bitcoin [3]. Since than, many other applications of this technology have been developed, from cryptocurrencies to smart contracts. A smart contract is a piece of software that describes a real-world contract, namely it stores rules for negotiating the terms of an agreement, and is able to automatically verify its fulfillment, and to execute the agreed terms or actions. The blockchain technology has been applied for the first time in the context of smart contracts with the Ethereum project [1].

Smart contracts typically interact with the real world and location information can be an important aspect in their correct specification. For instance, a smart contract may force that a performed activity is valid only if it is executed by an agent which is verifiably at a certain location, or that two or more agents can fulfill the contract only when they are nearby to each other. For this reason, the term *Proof of Location* (PoL) has been revived in the last year in conjunction with the blockchain technology. The goal of PoL is to have consensus on whether an event or agent is verifiably at a certain point in space and eventually in time. In the context of blockchain, such certificate can be built through a distributed, trustless and decentralized consensus mechanism.

For ensuring interoperability between smart contracts, they need a shared language to reference and query physical locations. Unfortunately, currently there are no standards for embedding locations, addresses or other more general geo-spatial concepts into smart contracts. At now three active projects are starting to introduce PoL on blockchain: FOAM [2],

Platin [5] and XYO [4]. The aim of these projects is to provide a location layer for smart contracts which is based on a protocol through which nodes can provide to customers proofs of their presence at certain locations in time. They are moving the first steps towards the integration between the geo-spatial domain and the blockchain technology.

The representation of spatial information inside a blockchain introduces new challenges for the geo-spatial community, relatively to both the definition of standards for the efficient and correct representation and verification/query of locations, and to the subsequent analysis of the spatial data encoded inside smart contracts. As regards to the first aspect, spatial constraints on smart contracts cannot be limited only to the verification that a location (expressed as a point) is contained inside a given region or it corresponds to another location. Therefore, we are interested in exploring how other spatial data types and spatial relations can be integrated into smart contracts, and how they can be efficiently verified using the techniques already developed by the geo-spatial community. Such relations cannot be only proximity or distance relations, but they may also include topological ones. Moreover, in some cases the spatial constraints contained inside a smart contract can abstract from the specific location occupied by agents and concentrate only on their relative positions or on the existence of other spatial relation between them. For instance, we could require that all agents are within the same room, or they are at least at a given distance from each other independently from their location. The verification of PoL cannot neglect another important aspect which regards the accuracy and intrinsic uncertainty characterizing spatial information, and this can become even more important when different type of devices are used to determine the position of an object, for instance as in the Platin project.

Relatively to the second aspects, the statistical analysis of data contained in a blockchain is becoming an interesting task, and this can be particularly true if we consider also spatio-temporal information. This activity can involve the integration of data inside a blockchain with other datasets, potentially including huge amount of data. Therefore, this analysis can involve the use of spatially-enabled big data systems, such as SpatialHadoop or GeoSPARK. We are interested in studying how such systems have to be extended and adapted in order to correctly interpret the spatio-temporal data contained inside a spatially-enabled blockchain.

References

1 V. Buterin. A next-generation smart contract and decentralized application platform, 2014. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed June 2018.

2 Foamspace Corp. FOAM Whitepaper, 2018. https://foam.space/publicAssets/FOAM_Whitepaper.pdf. Accessed June 2018.

3 S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. http://bitcoin.org/bitcoin.pdf. Accessed June 2018.

4 A. Trouw, M. Levin, and S. Scheper. The XY Oracle Network: The Proof-of-Origin Based Crypographic Location Network, 2018. https://docs.xyo.network/XYO-White-Paper.pdf. Accessed June 2018.

5 L. Wolberger, A. Mason, and S. Capkun. Platin, Proof of Location Blockchain, White Paper, 2018. https://www.dropbox.com/s/l8zai9irf6on6su/Platin%20Whitepaper%202018-03-27sm.pdf?dl=0. Accessed June 2018.