Distributed Access Control Through Blockchain Technology

by Damiano Di Francesco Maesa, Laura Ricci (Università di Pisa) and Paolo Mori (IIT-CNR)

We defined a distributed access control system on top of blockchain technology. The underlying idea is to properly represent the access rights of the subjects in the blockchain in order to easily allow their enforcement at access request time. By leveraging blockchain advantages we can add new desired properties, such as auditability, to the access control system. To prove the feasibility and validate the proposed approach we developed a proof of concept implementation and performed some relevant experiments.

A blockchain is a distributed, always available, irreversible, and tamper-resistant public database where the control over data and its evolution is distributed among a variable set of peers. Blockchain technology does not require the existence of trust relationships among the system's users. „ onsequently, it employs a distributed consensus algorithm to allow the users to agree on immutable and auditable append-only operation without requiring interaction with a trusted third party. We are interested in the auditability of the data stored in the blockchain, since the blockchain can be used as a publicly verifiable proof that the data existed at the time it was saved in it.

Access control systems are meant to regulate the access to critical or valuable resources. Several access control models, i.e., ways of defining the policies expressing the rights of subjects to access resources, have been defined, and here we focus on attribute-based access control (ABA„) policies. An ABA„ policy combines a set of rules expressing conditions over a set of attributes paired to the subject, to the resource or to the environment. The rules must be satisfied accordingly in order for the access right to be granted. A well-known policy language to express ABA„ policies is the eXtensible Access „ ontrol Markup Language (XA„ ML), defined by the OASIS consortium.

Our proposal exploits blockchain technology as the base framework on top of which we build an ABA„ system. The first step for defining our distributed blockchain-based access control system is to store the access control policies in the blockchain. Depending on the underlying blockchain, different technical solutions can be adopted. If the blockchain allows for arbitrary data storage, then we can save the policy directly on it. On the contrary, if the underlying blockchain has strict space constraints, e.g., Bitcoin [1], we should adopt more complex solutions, such as storing links to the policies in the chain while the complete policies are stored elsewhere (e.g., in distributed hash tables (DHT)). This is possible as long as the storage system remains tamper-proof and guarantees data availability, and the linking to the policies is unique and tamper-proof as well. Another option is the one provided by the Ethereum blockchain [2], which allows smart contracts to be represented and run. In this case, these smart contracts can be exploited to properly encode the policies themselves in executable format.

The next step of our approach is to define the policy enforcement architecture, i.e., to define the set of components required to perform, at access request time, the policy evaluation against the current access context. If the policy is not stored in the blockchain in executable format, the architecture of the enforcement system is similar to the XA„ ML reference one [1].

As an example, in [3] we described a preliminary prototype of a blockchain-based access control system which exploits the Bitcoin blockchain and XA„ ML policies. In this case, since Bitcoin was not designed to store arbitrary data, we defined a customised strategy to compress the XA„ ML policies and we exploited the OP_RETURN script op code and MULTISIG transactions to store them in the chain. The attributes required at access request time to perform the policy evaluation can be retrieved from traditional attribute providers (e.g., Lightweight Directory Access Protocol (LDAP)

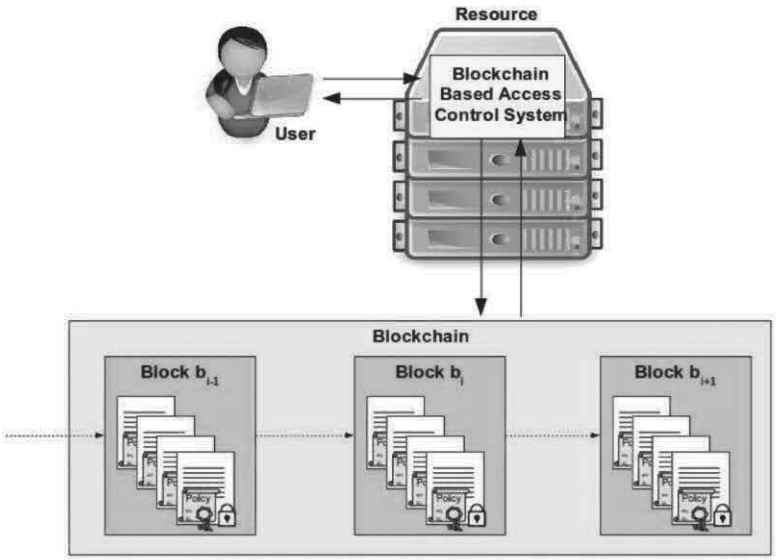

Figure 1: Architecture of the blockchain based access control framework.

services). However, we envisage that attributes could be stored and managed exploiting the blockchain as well. If the policy is stored in the blockchain in executable format, i.e., through smart contracts, most of the policy enforcement architecture is embedded in the blockchain itself. Such smart contracts represent self-evaluating policies that can be queried directly and transparently at access request time. The attributes required for the evaluation of the policy are encoded in the blockchain as smart contract as well. We have developed a proof-of-concept implementation of this approach on the Ethereum blockchain, demonstrating the feasibility of our proposal.

The evaluation of a blockchain-based access control policy could be performed by a party which is not trusted by the resource owner or by subject of the request who, instead, would like to be guaranteed against malicious or erroneous policy evaluations. For instance, the party that evaluates the policy and enforces the result could maliciously force the system to deny an access although the policy would have granted it.

Blockchain technology can be exploited to address this problem as well, In fact, having the policies and the attributes publicly available through the blockchain, allows any user to know at any time the policies that are applicable to its access request and the related access context. This allows distributed auditability, detecting parties that fraudulently alter the rights granted by the enforceable policies.

References:
[1] S. Nakamoto: "Bitcoin: A peer-to-peer electronic cash system", http://bitcoin.org/bitcoin.pdf (2008).
[2] G. Wood: "Ethereum: A secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper 151 (2014).
[3] D. Di Francesco Maesa, P. Mori, L. Ricci : "Blockchain Based Access „ ontrol", Proc. of the 17th IFIP International „ onference on Distributed Applications and Interoperable Systems (2017).

Please contact:
Damiano Di Francesco Maesa,
Dipartimento di Informatica,
Università di Pisa, Italy
damiano.difrancescomaesa@for.unipi.it

Blockchain Ensures Transparency in Personal Data Usage: Being Ready for the New EU General Data Protection Regulation

by Uwe Roth (Luxembourg Institute of Science and Technology, LIST)

The new EU General Data Protection Regulation (GDPR) [1][L1], which will come into effect in 2018, demands transparency as one of the main principles for the collection, processing, storing and transfer of personal data. Transparency ensures that individuals can enforce their legal rights: to withdraw consent for their personal data to be processed or to request that their data are erased. At the Luxembourg Institute of Science and Technology we filed a patent, based on blockchain technology, that guarantees transparency in the context of files that are exchanged in a shared data pool. It guarantees that access by partners to specific files can be traced without a central entity.

„ losed consortia who provide and exchange personal data between their partners need to understand the impact that the new General Data Protection Regulation (GDPR) of the European Union will have on their processes. In fact, it demands that the data controller must provide to an individual, upon request, information about the transfer of their personal data to third parties, third countries or international organisations.

The legal counterpart and single point of contact for a person that provided their personal data will not be the consortium as a whole, but a single data controller partner who has collected the private data and published it in the data pool. This contractual partner needs to ensure that the processing of personal data is legal, and may be sued if it fails to fulfil its legal obligations.

In the absence of a central logging facility that acts as a trusted third party, and without sophisticated access to appropriate management solutions, it can be virtually impossible to trace which partner organisations have accessed individual data sets. It can, therefore, be extremely difficult to provide relevant information to an individual who requests that their data be deleted. As a consequence, the processing of personal data inside a consortium might, in the future, be criminalised or result in a fine.

In 2016, The Luxembourg Institute of Science and Technology, LIST [L2], filed a patent application that addresses these new demands with a solution based on the latest file-distribution, blockchain and encryption technologies. In a purely decentralised peer-to-peer environment of equal partners, without requiring any centralised instance or further authorisation steps, the solution empowers the provider of data to trace the access to the data by partners in the distributed and shared data pool. This trace of access is without any doubt and cannot be denied.

The solution is based on a file distribution network of encrypted files. It creates redundancy to increase availability and to improve download speed (Figure 1). The blockchain network is used to log the access to the files which will allow every access of the data by any