Achieving Service Accountability Through Blockchain and Digital Identity

Fabrizio Angiulli, Fabio Fassetti, Angelo Furfaro(✉), Antonio Piccolo, and Domenico Saccà

DIMES - University of Calabria, P. Bucci, 41C, 87036 Rende, CS, Italy
{f.angiulli,f.fassetti,a.furfaro,a.piccolo}@dimes.unical.it, sacca@unical.it

Abstract. This paper proposes a platform for achieving accountability across distributed business processes involving heterogeneous entities that need to establish various types of agreements in a standard way. The devised solution integrates blockchain and digital identity technologies in order to exploit the guarantees about the authenticity of the involved entities' identities, coming from authoritative providers (e.g. public), and the trustiness ensured by the decentralized consensus and reliability of blockchain transactions.

Keywords: Service accountability · Blockchain · Digital identity

1 Introduction

In last few years, the number of contracts, transactions and other forms of agreements among entities has grown mainly thanks to the pervasiveness of ICT technologies which eased and speed up the business interactions. However, such growth has not been followed up by suitable technological innovations for that regards important issues like the need for accountability in agreements. Thus, the first problem to tackle is that of handling services where many actors, possibly belonging to independent organizations and different domains, need to base their interactions on "strong" guarantees of reliability and not on mutual trust or on reputation systems.

We, then, aim at defining an innovative platform for handling cooperative processes and services where the assumption of responsibility and the attribution of responsibility concerning activities performed by the involved actors can be clearly and certifiably stated. The platform should assure *trust* and *accountability* to be applied at different steps of service supply, from message exchange to transaction registration, till automatic execution of contract clauses.

Technologies for centralized handling of services are mature and widely employed, conversely open problems arise when the management is distributed or decentralized and there is the need to guarantee reliability and security of services.

J. Mendling and H. Mouratidis (Eds.): CAiSE Forum 2018, LNBIP 317, pp. 16–23, 2018.
https://doi.org/10.1007/978-3-319-92901-9_2

First of all, there is the *consensus* problem. Although exploiting a trusted and certified third-part for certifying identities is reasonable and acceptable by all the involved parts, the details about all the events concerning processes and services handled by the platform cannot be tackled by assuming the presence of a central trusted coordinator which would be one of the involved parts due to the intrinsic nature of decentralization and to need for a strong trust level guaranteed by distributed consensus. Many research efforts have been devoted to this issue and the state-of-the-art decentralized cooperation model is the blockchain.

Blockchain technology was early developed for supporting bitcoin cryptocurrency. Such technology allows the realization of a *distributed ledger* which guarantees a distributed consensus and consists in an asset database shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger [1]. The technology is based on a P2P approach, the community collaborates to obtain an agreed and reliable version of the ledger, where all the transactions are signed by authors and publicly visible, verified and validated. The actors of the transactions are identified by a public key representing their blockchain address, thus, there is no link between transaction actor in the ledger and his real-world identity. One of the main contribution of the proposed platform is the providing of a suitable solution to overcome this limitation.

The second main problem to tackle is the *accountability* in cooperative services. The mechanism of identity/service provider based on the SAML 2 protocol [2] represents a valid solution for handling digital identities through a standard, authoritative, certified, trusted, public entity. Towards this direction, the European Community introduced the *eIDAS* regulation [3] and the member States developed their own identity provider system accordingly (for example the Italian Public System for Digital Identity (SPID) [4]). However, how to embed the accountability in cooperative services in order to state responsibility and to certify activities of involved subjects is still a challenging problem. Solving this issue is a fundamental step for achieving a trustable and accountable infrastructure. Note that since the blockchain can be public readable, this could potentially arise a privacy problem that should be taken suitably into account. The main contribution of the work is, then, the definition of a platform aimed at handling services and processes involving different organizations of different domains that guarantees (*i*) *privacy*, (*ii*) *accountability*, (*iii*) *no third-part trustiness*.

The rest of the paper is organized as follows. Section 2 presents the preliminary notions about blockchain and digital identities technologies. Section 3 illustrates the peculiarities of the considered scenario and the related issues. Section 4 presents the detail about the proposed platform. Finally, Sect. 5 draws the conclusions.

2 Preliminary Notions

Bitcoin [5] is a digital currency in which encryption techniques are used to verify the transfer of funds, between two users, without relying on a central bank.

Transactions are linked each other through a hash of characters in one block, that references a hash in another block. Blocks chained and linked together are saved in a distributed database called blockchain. Changes made in one location get propagated throughout the blockchain ledger for anyone to verify that there is no double spending. The process of verification, Proof of Work (PoW), is carried out by some members of the network called miners using the power of specialized hardware to verify the transactions and to create a new block every 10 min. The miner is compensated in cryptocurrency that can be exchanged for fiat money, products, and services.

The success of Bitcoin encouraged the spawning of a group of alternative currencies, or "altcoins", using the same general approach but with different optimizations and tweaks. A breakthrough was introduced at the beginning of 2015 when Blockchain 2.0 comes in introducing new features, among which the capability to run decentralized applications inside the blockchain. In most cases, protection against the problem of double spending is still ensured by a Proof of Work algorithm. Some projects, instead, introduced a more energy efficient approach called Proof of Stake (PoS). In particular, PoS is a kind of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS based blockchains the creator of the next block is chosen in a deterministic way, and the chance that an account is chosen depends on its wealth, for example the quantity of stake held. The forging of a new block can be rewarded with the creation of new coins or with transaction fees only [6]. Some of the new terminology introduced by the Blockchain 2.0 involves the terms: Smart Contracts or DAPPs (decentralized applications), Smart Property and DAOs (decentralized autonomous organizations). Typically a contract involves two parties, and each party must trust the other party to fulfill its side of the obligation. Smart contracts remove the need for one type of trust between parties because its behaviour is defined and automatically executed by the code. In fact, a smart contract is defined as being autonomous, self-sufficient and decentralized [7]. The general concept of smart property is to control the ownership and the access of an asset by having it registered as a digital asset on the blockchain, identified by an address, the public key, and managed by its private key. Property could be physical assets (home, car, or computer), or intangible assets (reservations, copyrights, etc.). When a DAPP adopts more complicated functionalities such as public governance on the blockchain and mechanisms for financing its operations, like crowdfundings, it turns into a DAO (decentralized autonomous organization) [8,9].

In short, Blockchain 1.0 is limited to currency for digital payment systems, while Blockchain 2.0 is also being used for critical applications like contracts used for market, economic and financial applications. The most successful Blockchain 2.0 project is represented by Ethereum, the, so called, world computer [10].

2.1 Public Digital Identity Provider

The public identity provider mechanism is based on the Security Assertion Markup Language (SAML) protocol [2] which is an open-standard defined by

the OASIS Security Services Technical Committee. The latest version is the 2.0 released in 2005 which allows web-based authentication and authorization implementing the single sign-on (SSO) access control policy.

The main goal of the protocol is exchanging authentication and authorization data between parties.

The SAML protocol introduces three main roles: (*i*) the client (said *principal*) who is the entity whose identity has to be assessed to allow the access to a given resource/service; (*ii*) the *identity provider* (IDP) who is in charge of identifying the client asking for a resource/service, stating that such client is known to the IDP and providing some information (attributes) about the client; (*iii*) the *service provider* (SP) who is the entity in charge of providing a resource/service to a client after a successful authentication phase through a interaction with an IDP who provide client attributes to the SP. Thus, the resource/service access control flow can be summarized as follows:

1. the client requires for a resource/service to the service provider;
2. the service provider requests an IDP for an identity assertion about the requiring client;
3. the service provider makes the access control decision basing on the received assertion.

3 Scenario and Issues

In order to illustrate the advantages of the devised platform and to discuss the adopted solutions, firstly we present peculiarities and issues in the scenarios where the platform could constitute a valid and useful framework.

As previously introduced, the platform is particularly suited when the handled underlying process (for example a business process) involves different entities/companies/organizations that cooperate and want to work together without trusting on each other.

We assume to deal with two main entities: (*i*) one or more companies that cooperate in a common business involving a distributed and heterogeneous process where the accountability of the transactions of a primary importance (e.g. complex supply chains, logistics of hazardous substances); (*ii*) users and supervisors working in the corporates which are equipped with a public digital identity (denoted as *pub-ID* in the following) and a blockchain address (denoted as *bc-ID* in the following). We want to accomplish the following desiderata:

1. having the guaranty that a given transaction T happened from an entity X and an entity Y;
2. having the guaranty about the real-world entities X and Y that have performed T;
3. importantly, the above guarantees should be provided without trusting on any intermediary or third-part authoritative entity.

This corresponds to achieve the following objectives:

Goal 1. *Privacy:* each non-authorized entity should not know any detail about happened transactions.
Goal 2. *Accountability:* each authorized entity should know the real-world entity behind an actor performing a transaction.
Goal 3. *No third-part trustiness:* each entity should not need to trust on a component owned by another entity involved in the business process.

With these goals in mind, the proposed platform exploits the peculiarities of two technologies: *BlockChain* (BC) and *Public Digital Identity Providers*. As for the latter technology the adopted solution exploits the IDP/SP mechanism based on the OASIS SAML standard for exchanging authentication and authorization [2]. The blockchain ensures the trustiness about the effective execution of the transactions stored in the distributed ledger and allows us the accomplishment of goals 1 and 3. The IDP/SP mechanism allows us to obtain the real-world entity behind an account without the need of trusting on authentication mechanisms related to companies. Thus, this allows us to accomplish goal 2.

Since blockchain is like a distributed and shared database and, then, each node in the network can read the contents of the blocks and since a business process may contain sensitive data, the platform should allow to exploits the advantages of blockchains with no harm to the privacy of the data.

The IDP provides some information about the real-world entities associated with the account. However, more specific information are often needed in order to manage the privileges of reading/writing data. This can easily be taken into account thanks to the attribute provider mechanisms which is natively integrated in the IDP/SP mechanisms through the definition of Attribute Providers owned by the companies.

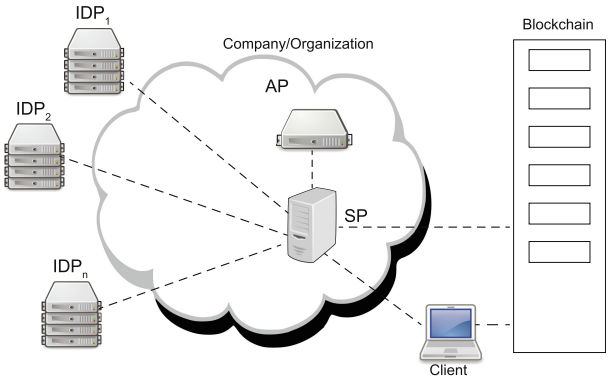

Fig. 1. The proposed architecture

4 Platform

The proposed architecture devoted at accomplishing the goals depicted in the previous section is reported in Fig. 1. The basic processes of the platform are described in details in the following sections. The main actors of the platform are:

- *Public Identity Provider (IDP).* The platform assumes the presence of one or more public IDPs which constitute an *external* authoritative source of information about the digital identity of the entities involved in the business process handled by the platform and, then, are controlled neither by such entities nor by the service provider but are trusted by all.
- *Service Provider (SP).* A relevant role in the platform is played by the service provider which constitutes an *internal* resource and it is in charge of handling business process details and sensitive data about involved entities; thus, it is expected that each company/organization builds its own SP for managing its data and it is not required that a company/organization trusts on the SP of another company/organization.
- *Attribute Provider (AP).* In the platform also one or more attribute providers can be present. Such services provide additional information about the entities accessing the platform through their public digital identity for example concerning roles and privileges with respect to business process data.
- *Blockchain (BC).* One of the fundamental component of the platform is the blockchain 2.0, which is external to the platform, supports smart contracts enactment and execution and implements the distributed ledger.
- *Client.* Each company member involved in the business process represents a client that has to register in the platform through its public digital identity and interacts with the blockchain through its blockchain address.

4.1 User Registration

The first step is to register the company users in the platform. Each company can independently register its members to the platform by defining its own Service Provider. It is required that the SP writes on the blockchain by creating a *smart contract* stating the association between the public digital identity of the member and its BC address. In turn, the member has to invoke this smart contract to confirm such pairing.

Note that it is not required that other companies trust on the SP producing the smart contract, since it can always be checked if the association is true. Indeed, the pairing between pub-ID and bc-ID can be checked by any SP by requiring the user to access the SP through its pub-ID and then to prove it is the owner of the bc-ID by signing a given challenge. The task of *member verification* performed by the service provider will be detailed in Sect. 4.3.

4.2 Smart Contract Handling

This section illustrates the platform core service consisting in exploiting the block-chain to record both business process transactions and the involved actors.

This process is started by the SP that creates a smart contract SC which records the hash of the business process transaction T and the bc-IDs of those actors which are (possibly with different roles) involved in T. To make the transaction effective, each actor has to confirm its participation by invoking an ad-hoc method of SC to confirm his agreement to play the role assigned to him by the SP. This accomplishes the three main goals planned for the platform.

Privacy Issue. Recording the hash of T allows us to ensure the suitable privacy level about the subject of the transaction. Indeed, in this way, the SP which has created the SC owns the transaction data. So, in order for an entity E to know the details of the accomplished transaction, it has to authenticate itself at the SP through its public digital identity and to require the data. The SP can, thus, verify the identity of E and check its privileges w.r.t. T. Optionally, the SP could also record the access request on the blockchain by asking E to invoke a suitable method on an ad-hoc smart contract.

Accountability Issue. From the smart contract SC, the entity E can get the hash of the transaction T and the bc-IDs of the involved actors. The entity E can also get from the blockchain the hash of the pairing about the bc-IDs of these actors and their pub-IDs. The pairing associated with this hash is stored by the SP, which can provide E this information if and only if E has privileges on T.

No Need for Trusted Third-Part Authority Issue. As for this issue, since both the hash of the data of transaction T and the hash of the pairings between bc-IDs and pub-IDs of the involved actors are recorded on the blockchain, each entity E can always check if all the information coming from the SP are valid, without needing of trusting on it. Note that, if E is one of the actors involved in T, E must be able to perform this check before invoking the method on the smart contract associated with T required for confirming T.

4.3 Service Provider Tasks

In this section, we describe the main features that a service provider should offer to be suitably embedded in the platform. We assume that the service provider is registered on one or more public IDPs which handle the public digital identities of the actors involved in the business process that should be managed by the platform. The service provider accomplishes three main tasks: *members registration*, *members verification* and *privileges management*.

Member Registration. The service provider allows a member to register by communicating with the IDPs according to the registration process described in Sect. 4.1. Once getting the bc-ID of the member, the service provider produces a smart contract containing the association between bc-ID and pub-ID which has to be confirmed by the user invoking a suitable method on the smart contract.

Member Verification. Through a service provider, an entity can check the pairing between bc-ID and pub-ID of a member by performing the following step. First, the service provider asks the member to access through its pub-ID on a public

IDP. Second, the service provider asks the member to prove that he is the owner of the bc-ID by requiring him to encode a challenge string (for example a human-readable sentence) with the private key associated with the bc-ID.

Privileges Management. The service provider which owns pairings and transactions can provide the details about them just to entities authorized at knowing such details. This can be accomplished by requiring that (*i*) the entity authenticates itself through its pub-ID on a public IDP and (*ii*) that the privileges of the entity returned by the attribute provider are enough to allow the access.

5 Conclusions

The orchestration of cooperative services is becoming the standard way to implement innovative service provisions and applications emerging in many contexts like e-government and e-procurement. In this scenario, technological solutions have been developed which address typical issues concerning cooperation procedures and data exchange. However, embedding accountability inside distributed and decentralized cooperation models is still a challenging issue. In this work, we devise a suitable approach to guarantee the service accountability which is based on state-of-art solutions regarding digital identity and distributed consensus technologies for building a distributed ledger. In particular, the proposal exploits the notion of smart contracts as supported by blockchain 2.0.

This work has been partially supported by the "IDService" project (CUP B28117000120008) funded by the Ministry of Economic Development under Grant Horizon 2020 - PON I&C 2014-20 and by the project P.O.R. "SPID Advanced Security - SPIDASEC" (CUP J88C17000340006).

References

1. Hancock, M., Vaizey, E.: Distributed ledger technology: beyond block chain. Technical report GS/16/1, UK Government Chief Scientific Adviser (2016)
2. Cantor, S., Kemp, J., Maler, E., Philpott, R.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.02. OASIS Standard Specification (2005)
3. Bender, J.: eIDAS regulation: EID - opportunities and risks (2015)
4. AgID - Agenzia per lItalia Digitale: Spid - regole tecniche (2017)
5. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. White paper (2008)
6. Popov, S.: A probabilistic analysis of the Nxt forging algorithm. Ledger **1**, 69–83 (2016)
7. Tapscott, D., Tapscott, A.: Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio, London (2016)
8. Buterin, V.: Bootstrapping a decentralized autonomous corporation: part I. Bitcoin Mag. (2013)
9. Buterin, V.: DAOs are not scary, part 1 and 2. Bitcoin Mag. (2014)
10. Buterin, V.: A next-generation smart contract and decentralized application platform. White paper (2014)