# On-Chain Global Maintenance Services: Technical, Legal and Managerial Implications*

Alessandro Bellini[5], Antonio Bonifacio[5], Salvatore Esposito De Falco[4], Simone Naldini[5], Francesco Pacileo[3], Diego Pennino[1], Maurizio Pizzonia[1], Domenico Sardanelli[6], Andrea Vitaletti[2], Pietro Vito[4] and Marco Zecchini[2,*]

[1]*Università degli Studi Roma Tre, Dipartimento di Ingegneria, Sezione Informatica e Automazione, Via della Vasca Navale 79, 00146 Rome, Italy;*

[2]*Sapienza Università di Roma, Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Via Ariosto 25, 00185 Rome, Italy;*

[3]*Sapienza Università di Roma, Dipartimento di Diritto ed economia delle attività produttive, Via Del Castro Laurenziano 9, 00161 Rome, Italy;*

[4]*Sapienza Università di Roma, Dipartimento di Management, Via Del Castro Laurenziano 9, 00161 Rome, Italy;*

[5]*Mathema, Via Torcicoda 29, 50142 Florence, Italy;*

[6]*Università degli studi di Macerata, Dipartimento di Scienze della formazione, dei beni culturali e del turismo.*

## Abstract

Facility management deals with all activities that are not core business for a company and are consequently outsourced to specialized companies. Maintenance is a fundamental activity in facility management and it is often handled by *Global Maintenance Services* (GMS) where some maintenance activities are delegated by the company to service providers and are remunerated according to measurable results expressed as Key Performance Indicators. In this context, it would be desirable to have information systems trustable by all involved actors. In this paper, we discuss the design of a blockchain solution capable to support a GMS on-chain. We first introduce the GMS concept and how it is related to the Principal-Agent relationship, then we show a reference architecture to implement GMS on-chain. We discuss a use case and a proof-of-concept of on-chain GMS in a hospital showing how smart contracts and oracles can be used in this context. We finally discuss the main legal and managerial implications of the proposed approach.

## Keywords

Maintanance, Blockchain, Oracle, Smart Contract, Sensors, Legal Implications, Managerial Implications

# 1. Introduction

*Facility Management* (FM) deals with managing the facilities, namely all assets, both tangible and intangible, that support a company's core business making the life of occupants of residential buildings, shops, offices or factories more pleasant and safe. Within FM, a Global Maintenance Service (GMS), is a form of outsourcing contract specifically related to maintenance and based on measurable results. Through a GMS contract, a *client*, or *principal*, entrusts a series of activities aimed at the maintenance of the facilities to a single *primary service provider*, or *agent*, for a well defined period of time. The following elements are relevant to this paper for a GMS contract.

- The contract is based on results. The remuneration is a function of a series of Key Performance Indicators (KPIs) through which it is possible to measure the quality, efficiency and effectiveness of the performed activities.
- There is a working group made up of representatives of the client and the primary service provider, whose function is to ensure the correct start and execution of the project, with particular regard to the implementation of integrated management tools.
- The primary service provider appoints a single manager, with respect to which the client can refer as the sole interlocutor and who has responsibility for the activity of all the personnel involved in the performance of the services covered by the contract. The primary service provider can delegate some activities to *secondary service providers*.

Figure 1 summarizes and clarifies the relations between the parties discussed so far.

Examples of the employment of GMS contract for the maintenance of facilities include the following.

- Lighting. Energy supply and ordinary and extraordinary maintenance of related systems.
- Real estate assets. Their ordinary and extraordinary maintenance, plant maintenance, cleaning and surveillance services.
- Green. Paving, cleaning, cutting of the grass, refurbishment of green areas.
- Heat. Ensure the heating and air conditioning system including the supply of fuel, gas and electricity.

*DLT 2022: 4th Distributed Ledger Technology Workshop, June 20, 2022, Rome, Italy*

[*] This research was partially funded by Sapienza Ateneo Research grant "La disintermediazione della Pubblica Amministrazione: il ruolo della tecnologia blockchain e le sue implicazioni nei processi e nei ruoli della PA". This research was partially founded by Italian Minister of Economic Development (MISE) grant "ReASSET: Piattaforma Maas (Maintanence as a Service) Blockchain-IoT per la gestione operativa in tempo reale degli asset tecnico-impiantistici". This research was partially funded by POR FESR LAZIO 2014 – 2020, call for "Gruppi di ricerca 2020". Det. n. G04052 of Apr. 4th, 2019, under the "LazioChain" project, CUP F85F21001550009 - POR project code A0375E0116.

[*] Corresponding author.

salvatore.espositodefalco@uniroma1.it (S. E. D. Falco); francesco.pacileo@uniroma1.it (F. Pacileo); pennino@ing.uniroma3.it (D. Pennino); pizzonia@ing.uniroma3.it (M. Pizzonia); vitaletti@diag.uniroma1.it (A. Vitaletti); pietro.vito@uniroma1.it (P. Vito); zecchini@diag.uniroma1.it (M. Zecchini)

0000-0001-5339-4531 (D. Pennino); 0000-0001-8758-3437 (M. Pizzonia); 0000-0003-1074-5068 (A. Vitaletti); 0000-0002-2280-9543 (M. Zecchini)

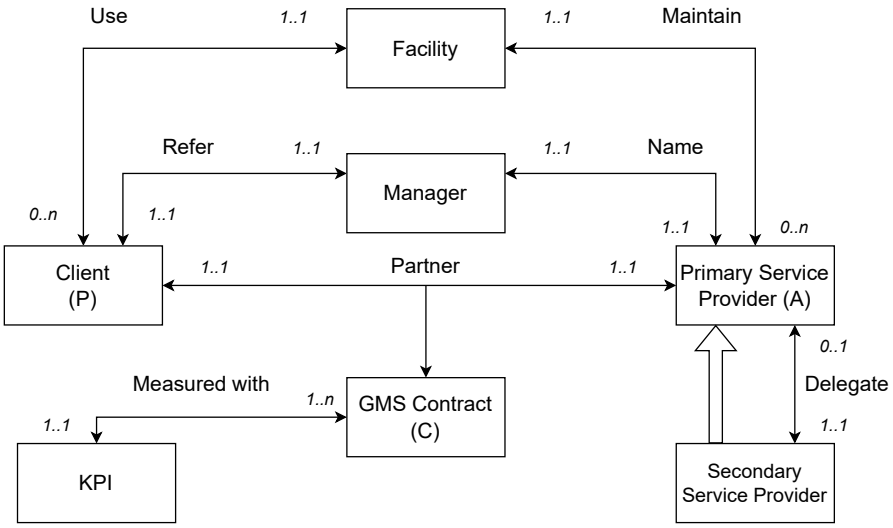


**Figure 1:** Diagram of the relations between parties

GMS can be modelled as a relationship between a Principal (P) and an Agent (A) [4], where the principal appoints the agent to act on its behalf for the maintenance of its facilities. According to the GMS, the relationship is governed by a contract (C) based on results measurable by suitable KPIs.

Usually, the client pays the provider either on the basis of measurements declared by the provider or by performing measurements by themselves. In the first approach, the client must trust the provider. In the second approach, the costs of the client for autonomously performing the measurements might be too high with respect to the benefits of the outsourcing approach.

In this paper, we propose an architecture based on blockchain and IoT technologies to address this problem. We also provide details for a sample use case of this approach encompassing oracles to acquire measurements from IoT devices into the blockchain. Our sample use case is taken from a real tender for heat maintenance related to an Italian hospital. We provide examples of smart contract code to realize that use case.

This paper is structured as follows. In Section 2, we provide background notions about blockchain technologies and how they are able to access off-chain data through oracles. In Section 3, we describe the architecture of a blockchain-based GMS, how it benefits from this technology and we introduce our first proof-of-concept. Section 4 introduces some of the main legal implications of the GSM on-chain focusing on the Italian legal framework, while Section 5 introduces the most relevant managerial implications of our proposed approach. Finally, Section 6 draws the conclusions of the paper and provides some discussion about open problems.

## 2. Blockchain Background

A *blockchain* is a type of *Distributed Ledger Technology* (DLT) [40] where transactions are recorded in an immutable order obtained by means of *cryptographic hash functions* that chain the blocks in which transactions are recorded. Unlike a centralized database, a blockchain is decentralized, namely there is no need for a central authority or intermediary for processing, validating, and/or authenticating transactions[9]. A blockchain is managed by a set of autonomous *nodes* that collectively create a peer-to-peer (p2p) network adhering to a protocol for inter-node communication and validating new blocks. Nodes do not trust each other and malicious nodes are tolerated, within certain limits that depends on the consensus algorithm [19].

Initially, blockchain focused on transactions to exchange cryptocurrencies among blockchain users, as in Bitcoin [30]. For efficiency reasons, transactions are not confirmed one-by-one but aggregated into *blocks* and they are confirmed when a new block is added to the chain. When a new block is proposed by a node of the network, all the other peers verify that it respects the protocol rules, that also depend on the application domain, in a process called *validation*. The *consensus* (for more details, see [45, 46, 19]) is the decentralized process by which the network achieve an agreement on which valid block is eventually stored in the ledger.

In *permissionless* blockchains (e.g. [30, 10]), every user can participate to the consensus, while in *permissioned* one [13], the participation to the consensus is allowed only to specific users known in advance [23]. Furthermore, blockchains can be categorized according to who can access the content of the ledger and make proposals for new transactions. In public *blockchains* , everyone can read the content of the ledger and propose new transactions that, if successfully validated, will be eventually stored in the ledger by the consensus algorithm. On the contrary, in *private* blockchains, users are authenticated and access control allows or denies each user operation as occurs for access control of regular information systems.

While initially blockchain has been primarily conceived to implement cryptocurrency trading, it can now be adopted to realize general-purpose applications through the use of *smart contracts* [47]. They consist of pieces of code that are executed as part of a transaction. In simple terms, in these cases, the blockchain implements a global decentralized virtual machine and smart contracts are the programs running on it.

Smart contracts can process only data that are stored in the blockchain. However, in the GMS use case that we consider in this paper, there is the need of accessing off-chain data. This is possible using an *Oracle* (for more details, see [7]). Oracles are components that allow smart contracts to get inputs from outside the blockchain through regular blockchain transactions. There are several oracle services providing APIs to allow smart contracts to access external data. Examples include Chainlink [1], Provable [3], BandChain [5], and Tellor [2].

## 3. GMS On-Chain

Figure 1 represent a model of a of Global Maintenance Services as a Principal-Agent relationship. In such a relationship, the agent acts on behalf of the principal and should not have a conflict of interest in carrying out its task. An agent may act in its own best interests and in a way that

is contrary to the best interests of the principal, generating the so-called *P/A Problem*. This problem typically arises when P has into enough information to directly ensure that A is always acting in P's best interest.

The transparency, immutability, traceability and algorithmic governance offered by *Blockchain* technologies can contribute to mitigate the P/A Problem [25], reducing (or even eliminating) the asymmetry of information and thus facilitating the creation of a genuine net value.

The employment of the blockchain, allows us to envision new models of governance, where trust between the actors is substituted by A and P relying on the consensus within the P2P blockchain infrastructure, i.e. relying on a community rather than on the trust in individual actors. In this perspective, the natural different interests of P/A, at least economically-wise, as well as the participation of different providers competing in the market, are guarantees to the achievement of a real consensus among the parties, even in less open infrastructure such as the permissioned blockchains.

In particular, the Blockchain can provide:

- algorithmic governance autonomously managed by smart contracts capable to implement decentralized decision-making processes providing the highest guarantee of impartiality to all the involved stakeholders;
- a transparent and immutable bidding process to select the service providers (i.e. Agents);
- a minimization of the information coordination costs on a shared infrastructure, making the organization's data accessible to new customers and suppliers;
- a reduction of verification costs, namely costs involved in verifying the transactions between Principal and Agent.
- a reduction of intermediation costs, i.e. the costs due to the certification activities by a third party, external to the contractors.

### 3.1. Modelling the P/A Relationship On-Chain

The architecture of the on-chain GMS modeled as P/A relationship is represented in Figure 2. Here we assume that both the Principal and the Agent are entities on-chain identified by an address. Note that we currently assume the pseudoanonymity sufficient to carry on the economic transaction behind the GMS contract, however, while this is technically more convenient, we have not yet properly investigated all the complexity of managing identity on-chain [36] in particular when norms, laws, and regulations must be satisfied.

In the following, we will use Solidity code sketches to illustrate the structure and main components of the necessary smart contracts. Smart contracts of the following examples refer to the hospital heating use-case described in Section 3.2. The GMS contract is translated into a smart contract (see Listing 1). The function *payAgent*, at Line 23, performs the payment if the KPI are satisfied. In this case, this occurs when the level of CO emission measured by a sensor is below a given threshold (see line 27). To access the data of the IoT sensors [37], the smart contract interacts with an Oracle [11] as sketched in Listing 2. In this case, we use the Provable Thing Oracle [3], that provides access to off-chain data to a number of Blockchain Technologies, including Ethereum, EOS, R3 Corda and Hyperledger Fabric.

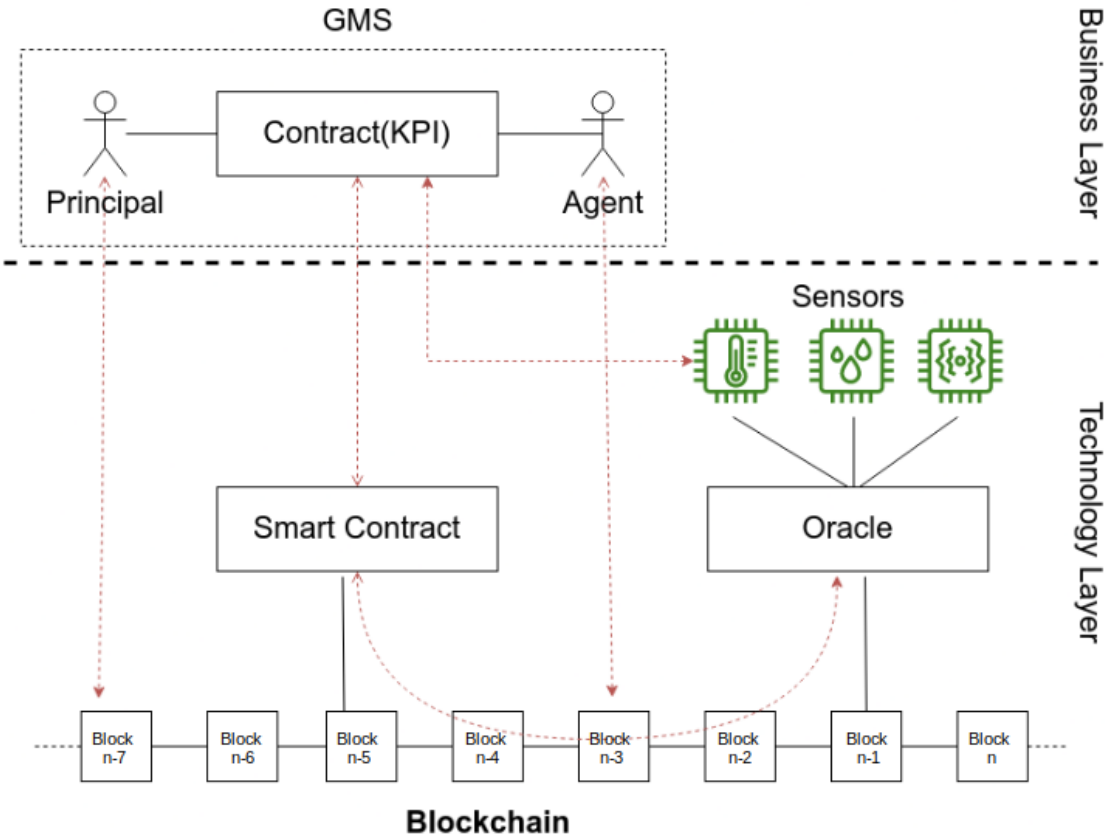


**Figure 2:** At the Business layer, the relationship between the Principal and Agent modeling the GMS, is regulated by a contract based on performance measures defined by suitable KPIs. The Business components are mapped into their technical counterparts in the Technical Layer. Principal and Agents are two entities on the Blockchain. The remuneration of the Agent (i.e. a transaction from the Principal to the Agent) is governed by a Smart Contract according to specific sensors' observations measuring the KPIs. To access sensors' data, the Smart Contract interacts with an Oracle.

In some cases, primary service providers can take advantage of sub furniture provided by secondary service providers. Also in this case, a smart contract can be employed to manage this relationship as a P/A one as shown in Listing 3.

### 3.2. Use-Case: GMS for an Hospital

In this section, we show how the components of Figure 2 can be mapped to a real tender specifications document [34] which defines the modalities through which the Bianchi Melacrino Morelli Hospital in Reggio Calabria, Italy, intends to entrust the ordinary and extraordinary maintenance service of the buildings, the technical plants, and the furniture to a primary service provider for three years.

Art. 6 of [34], details the reference maintenance plan, and provides a number of sheets that list all the maintenance operations that the primary service provider has to perform. For the

sake of simplicity, we simply consider the sheet in Table 1.

| Maintenance guide N. 05 | | |
|---|---|---|
| **Plant or Facility type** | **Operations performed by the maintenance service** | **Cyclicity** |
| **thermomechanical plants** | Combustion control according to Legislative Decree 152/06 | **Annual** |

**Table 1**
Maintenance operations carried by the primary service provider

The sheet mandates that every year, the combustion of thermo-mechanical systems must be checked according to the D.L.gs 152/06 [43] regulation.

**Principal and Agent** The Principal is the hospital company. The Agent is the primary service provider taking care of the maintenance of the hospital facilities as foreseen in the GMS according to the specification provided [34] and possibly taking advantage of secondary service providers.

**Measurable Contract** Articolo 286 of Decreto Legislativo 152/06 [43] defines the threshold values and the measurement modalities to check the emissions. In the following, we summarize the most relevant elements for the considered use case.

- The atmospheric emissions of civil thermal plants with nominal thermal power above the threshold value must comply with the limit values set out in part III of Annex IX to part five of D.Lgs 152/06 (see Table 2).
- The emission values of the plants must be checked at least annually by the person in charge of the operation and maintenance of the plant during normal inspection and maintenance operations. The measured values, with the indication of the relative dates, of the measurement methods used and of the person who carried out the measurement, must be attached to the plant logbook.
- For the purposes of sampling, analysis and assessment of emissions from thermal plants referred to in paragraph 1, the methods provided for in part III of Annex IX (see Table 2) are applied.
- The installer verifies compliance with the emission limit values.

According to the GMS, the smart contract will (a) verify the satisfaction of the requirements for the emissions according to the measured KPIs and the limit defined in [43] and (b) perform the payments to the service providers.

**KPI and sensors** The KPI to measure the satisfaction of the contract terms is clearly defined in Table 2. As an example, if we consider the Total Suspended Particles and a heating system with nominal installed power between 3 and 6 MW, the threshold is 30mg/Nm3.

The measurements of the satisfaction of the KPI are provided by the sensors of Table 2, namely Total Suspended Particles, Total Organic Carbon, Carbon Monoxide, Nitrogen Oxides, Sulfur Oxides. Sensors should sample the environment with accuracy and a sampling period defined by the regulation.

| | Installed Electrical Rated Output (MW) | | | |
|---|---|---|---|---|
| | [1] $> 0, 15\% \leq 3$ | $> 3\% \leq 6$ | $> 6\% \leq 20$ | $> 20$ |
| Total dust | $100 mg/Nm^3$ | $30 mg/Nm^3$ | $30 mg/Nm^3$ | $30 mg/Nm^3$ |
| Total organic carbon (TOC) | n.a. | n.a. | $30 mg/Nm^3$ | $20 mg/Nm^3$ |
| | | | | $10 mg/Nm^3$ |
| Carbon monoxide (CO) | $350 mg/Nm^3$ | $300 mg/Nm^3$ | $250 mg/Nm^3$ | 200 |
| | | | $150 mg/Nm^3$ | $100 mg/Nm^3$ |
| Nitrogen oxides (expressed in $NO_2$) | $500 mg/Nm^3$ | $500 mg/Nm^3$ | $400 mg/Nm^3$ | $400 mg/Nm^3$ |
| | | | $300 mg/Nm^3$ | $200 mg/Nm^3$ |
| Sulphur oxide (expressed in $SO_2$) | $200 mg/Nm^3$ | $200 mg/Nm^3$ | $200 mg/Nm^3$ | $200 mg/Nm^3$ |
| [1] For plants with a rated thermal input equal to or greater than 0.0035 MW and no greater than 0.15 MW, it is applied an emission value for total dust of 200 | | | | |

**Table 2**
An example of requirements and KPIs for a tender. Values shown in this table are taken from the Italian regulation [43] (see text), which applies to the the tender considered in Section 3.2.

**Smart Contract examples.** Listing 1 illustrates how Principal and Agent can manage their collaboration with a smart contract. “PayCOContract" accesses external data through the contract oracle in Listing 2. Finally, “Subcontract" in Listing 3, demonstrates how a primary service provider can delegate a secondary service provider on a blockchain through a specific smart contract.

```
pragma solidity ^0.4.22;
import "./ExampleContract_CO_Oracle.sol";

contract PayCOContract {

   ExampleContract_CO_ORACLE private OracleContract;
   address public P;
   address public A;
   uint public CO_Threshold;
   uint public lastPayment;
   uint public payment;
   uint public INTERVAL = 10;

   constructor (address _OracleContract, address _P, address _A, uint _CO, uint _payment) {
       OracleContract = ExampleContract_CO_ORACLE(_OracleContract);
       P = _P;
       A = _A;
       CO_Threshold = _CO;
       payment = _payment;
       lastPayment = block.number;
   }

   function payAgent() payable {
       require(block.number > lastPayment + INTERVAL);
       require(msg.value == payment);
       require(msg.sender == P);
       if (stringToUint(OracleContract.CO) < CO_Threshold) revert();

        A.transfer(msg.value);
```

```
    }

}
```

Listing 1: A sketch of a smart contract to execute the payment from the Principal to Agent if specific conditions are met. For the sake of brevity “stringToUint" function is omitted but it casts a string into an unsigned integer in Solidity.

```
pragma solidity ^0.4.22;
import "github.com/provable-things/ethereum-api/provableAPI_0.4.25.sol";

contract ExampleContract_CO_ORACLE is usingProvable {

   string public CO;
   event LogConstructorInitiated(string nextStep);
   event LogCOUpdated(string CO);
   event LogNewProvableQuery(string description);

   function ExampleContract() payable {
       LogConstructorInitiated("Constructor was initiated. Call 'updateCO()' to send the
           Provable Query.");
   }

   function __callback(bytes32 myid, string result) {
       if (msg.sender != provable_cbAddress()) revert();
       CO = result;
       LogCOUpdated(result);
   }

   function updateCO() payable {
       if (provable_getPrice("URL") > this.balance) {
           LogNewProvableQuery("Provable query was NOT sent, please add some ETH to cover
               for the query fee");
       } else {
           LogNewProvableQuery("Provable query was sent, standing by for the answer..");
           provable_query("URL", "json(https://api.sensor.it).CO");
       }
   }
}
```

Listing 2: A sketch of a smart contract to get data from a CO sensor by Provable Things Oracles. Provable Things provide oracles for a number of Blockchain Technologies, including Ethereum, EOS, R3 Corda and Hyperledger Fabric

```
pragma solidity ^0.4.22;
import "./PayCOContract.sol";

contract Subcontractor is PayCOContract {
    address public Secondary;
    uint public SecondaryPayment;

    constructor (address _OracleContract, address _P, address _A, uint _CO, uint _payment,
        address _S, uint _secondary_payment) PayCOContract(_OracleContract, _P, _A,_CO,
        _payment) {
```

```
        Secondary = _S;
        SecondaryPayment = _secondary_payment;
    }

    function paySecondary() public {
        require(block.number > lastPayment + INTERVAL);
        require(msg.value == SecondaryPayment);
        require(msg.sender == A);
        if (stringToUint(this.OracleContract.CO) < CO_Threshold) revert();

         Secondary.transfer(msg.value);
    }
}
```

Listing 3: A sketch of a smart contract to execute the payment from the Primary Service (A) to Secondary Service provider if specific conditions are met. Note that, since this is a special case of contract where the agent delegates to another entity the management of some facility, Subcontract inherits the main contract “PayCOContract"

**Proof of Concept** To evaluate the feasibility of the smart contracts involved in the study, we initially considered Solidity (see the previous paragraph) and the Ethereum ecosystem. However, while a permisionless/public blockchain provides the highest guarantees in terms of decentralization and transparency, the industrial sector is still reluctant to the use of these technologies mostly due to a) privacy concerns, b) uncertain development of a legal framework, c) limited scalability and d) relatively high and unpredictable transaction costs (see Sections 4 and 5). For these reasons, we implemented the PoC in Hyperledger Fabric (HF) [8] the open-source blockchain platform that is designed for enterprise use cases. One of the main characteristics of HF is its modular architecture, which allows for flexibility and scalability. It allows for different consensus mechanisms, membership services, and smart contract execution environments to be plugged in as needed. This allows the network to be customized to the specific requirements of each use case. HF supports channels, namely private and confidential networks within the overall blockchain network. This allows for multiple parties to transact on the same network while keeping certain transactions private to specific parties. HF is also designed to support smart contracts, known as Chaincode, written in a variety of programming languages such as Go, JavaScript and Java, making it more accessible for developers with different backgrounds. Overall, HF is a blockchain platform that is specifically tailored for enterprise use cases, with a focus on flexibility, scalability, and security. It is widely adopted by financial services, supply chain management, and healthcare industries among others.

In our use case GMS for an Hospital, private channels have been implemented to allow a private communication between each agent and the principal. This solution allows the agents to have secure communications within the network, without sharing sensitive information with other potential competitors. The proof-of-concept (PoC) implements the smart contracts (Chaincode) to periodically check the conformance of the asset to the KPI according to the measurements of the sensors on the asset. A the time of writing, a real test-bed is not yet available, so the sensors (dust, CO2 presence, etc.) have been simulated. The simulator supports a collection of virtual devices in the network, which issue a measurements at regular intervals. The values

issued are randomly generated in a pre-set range, a range which also includes values considered to be outside the threshold, so as to be able to generate anomalous readings. The presence of possible anomalous readings is used to verify the correct functioning of the implemented smart contracts. The simulated sensors are considered off-chain and are queried by the smart contracts employing Provable oracles [3]. Even if the current status of the implementation can be considered only a PoC it allows us to test all the main functionalities foreseen in our reference use case.

# 4. Legal Implications

A legal framework to regulate the adoption of blockchain technologies (BCTs) and Smart Contracts (SCs) is still under active development and varies significantly depending on the country. For this reason, we limit our discussion on the legal implications of the implementation of an on-chain GSM to the Italian legal framework, considering the European Union Law when possible.

## 4.1. Smart contracts. Legal concerns.

The economic-legal function of the Smart Contracts (SCs) in the proposed model is to ensure the fulfilment of the obligations assumed by the contractual parties, without adopting guarantees (e.g., a demand guarantee) or self-protection regulatory instruments such as the default exception foreseen in the article 1460 of the Italian Civil Code [39], and, as a result, to implement the success of the transactions operating on the blockchain network: these are therefore transaction protocols concerning the execution phase of a contract [28]. Nonetheless, new legal concerns arise, related to automation, immutability, and the use of a computational language. In this regard, there may be difficulties in understanding the text of the SC, even for legal operators, and this justifies the practice of supporting a translation into natural language, also through AI systems. However, in the event of a discrepancy between the computational language and the natural language, the doctrine considers the former to be prevalent, intrinsic to the Code and to the reason for which the SCs are adopted [28, 20]. The computational language is hardly compatible with vague contractual clauses and legal standards: e.g., bitcoin value which becomes excessively burdensome, good faith, correctness, extent of fault, diligence, suitability, and correct execution [39, 28, 20, 27]. Even the European Parliament, in a 2020 Resolution, envisaged difficulties when using SCs in the event of insolvency (and related revocatory actions), of nullity for infringement of the Antitrust Law [35]. Difficulties also arise for terminating or stopping the execution of the contract and for exercising the right of withdrawal [28]. Therefore, problems related to the possible nullity/annullability/termination of contracts. Another problem concerns the law applicable to cross-border transactions. All things considered, compared to the current state of progress of BCT and SC technologies, it is advisable to use in the proposed model the SCs only for standardized and simple agreements or operations, while providing for safeguard clauses or legal standards in the context of an off-chain framework agreement, written in natural language. These SCs should be elaborated as models by competent Universities or Institutions and should have a role to serve and replace mechanical and repetitive human operations [39, 18].

With specific regard to the BCT and the SCs, the Italian D.L. 14 December 2018, no. 135, containing "Urgent provisions on support and simplification for businesses and for the public administration", in Art. 8-ter, added by the conversion law n. 12/2019 and entitled "Technologies based on distributed ledgers and smart contracts", at Paragraph 2, defines the concept of smart contract as "a computer program that operates on technologies based on distributed ledgers and whose execution automatically binds two or more parties on the basis of effects predefined by them". The expression "whose execution automatically binds two or more parties" must be interpreted in a broad and meta-juridical sense, as "automatable" from a technical-engineering point of view [28, 20].

The same paragraph also foresees that "Smart contracts satisfy the requirement of the written form after IT identification of the interested parties, through a process having the requirements set by the Agency for digital Italy (AgID) with guidelines to be adopted within ninety days from the date of entry into force of the law converting this decree". However, to date the AgID has not yet adopted the guidelines and it has not yet identified the required standards, for the purposes of compliance with the electronic IDentification Authentication and Signature (eIDAS) Regulation [12].

As a consequence, someone in doctrine raises doubts on the current legal possibility of using the BCT and the SC in the absence of the documents required by Art. 8-ter [28]. However, such an interpretation would be in contrast with the principle of technological neutrality and the drive towards innovation, promoted by EU Law, given that there would be an unjustified discrimination of the technologies mentioned compared to others not subject to such limitations [20, 38]. Indeed, part of the doctrine considers it reasonable - assuming AgID will issue the guidelines mentioned before and in view of articles 20 and 21 of the (Italian) Digital Administration Code - to consider SCs equivalent of standard contracts [39].

### 4.2. Digital identity.

The GSM requires the identification of the parts, both for the purpose of mapping the responsibilities (accountability) and for verifying the suitable professional skills of the Facility Manager and of the sub-suppliers/contractors. Nowadays, digital identity is usually guaranteed by trusted identity providers such as Facebook (Facebook Connect) and Google (Google Sign-In) that have control of the information associated with users identities. Self-sovereign identity (SSI) [44] is a new approach to digital identity that gives individuals control over the information they use to prove their identity instead of relying on trusted identity providers. In an SSI system, users generate and control unique identifiers called decentralized identifiers (DiD). Most SSI systems are decentralized and the credentials are managed using crypto wallets and verified using public-key cryptography anchored on a distributed ledger [31].

The user is free to accumulate credentials from reliable authorities in DIDs and to produce them as needed (e.g., to prove Italian citizenship, tax code or address or place of residence) providing the guarantee that the person presenting them is precisely the same to whom they refer. This is achieved by means of verifiable credentials (VCs), namely tamper-proof credentials that can be verified cryptographically. The eIDAS Regulation is the main legal reference to govern DIDs.

The European Blockchain Services Infrastructure (EBSI) [15] has developed a generic SSI (i.e.,

ESSIF [14, 17]), which will be integrated and made compatible with the eIDAS Regulation and the GDPR.

However, the current regulatory framework remains uncertain, although an evolution of the legal system in favour of the use of the BCT and the SSI in the eIDAS appears clear and foreseeable [32].

### 4.3. Data protection.

To date, there are no guidelines required by the legislator – at European and national level – that can ensure that blockchain technologies, and public ones in particular, operate in compliance with the GDPR and other data protection regulations.

However, the clear intention of promoting the development and use of these technologies expressed by European, national, and supranational institutions [29, 32], encourages to identify every possible element of compatibility with the GDPR linked to the model being designed.

Some of the most relevant open issues are a) who is the actual data controller for the data processing in a distributed network, b) data minimization in a network conceived to have multiple distributed copies of the same ledger and c) the right to deletion or the right to be forgotten in an immutable ledger, d) the transnational nature of the blockchain. Some of such issues, can be more effectively handled in a private/permissioned blockchain network, where it is easier to reconstruct the group context in which the actors operate and identify the subject or subjects who have a data governance role [41, 16]. However, many consider private/permissioned blockchains simple distributed databases that provide limited advantages with respect to the traditional and dominant Client/Server approach.

Because of the numerous legal concerns above mentioned, the decentralized GSM model to be developed in this research project could operate, at least for a period, in a protected regulatory environment (innovation hubs, sandboxes [33]), in which the operators act together with the supervisory authorities. To date, such environments are not yet envisaged for GSM (sandboxes are usually tailored for fintech, where, moreover, BCT and SCs could be experimented with). Nonetheless, the Italian Ministry for Economic Development (MISE, now Ministry of Enterprises and Made in Italy), in a recent document [29], has expressed its intention to develop use cases and sandboxes in which one could experiment, among others, with projects relating to the use of the BCT for the maintenance of buildings.

## 5. Managerial Implications

The legal aspects discussed in the previous section, and in particular some concerns on privacy, which is needed in many relevant business applications, still limit the adoption of blockchain solutions. However, the implementation of the Global Maintenance Services on-chain, might have breakthrough business implications. The automation and consequent reduction of verification and certification costs makes service providers that rely on this solution more competitive, since their bids are potentially much cheaper than other bidders. This is particularly relevant, given the fact that most public tenders are based on auction mechanisms and that contracting organizations award the most transparent and economically advantageous offer. Even organizations with in-house facility managers might be attracted by the opportunities provided by a

blockchain platform collecting competent and competing contractors. The immutability of the records is a guarantee of the reputation and accountability of such contractors. Internalized facility departments might also use such a platform to outsource specific maintenance services to the most efficient providers. The blockchain architecture can also enhance the procurement process itself [42]. Firstly, it can speed up the publishing of the tenders [22], because it can be used to notify service providers, to send tender request, and to verify the identity of service providers while at the same time ensuring when necessary the confidentiality of tendering information. Buyers can also assess quality of service providers for which FM contracts data is already available within the platform. Enhanced transparency should have also positive upstream effects on filtering high-quality bidders, since only providers who are aware of their own value may confidently bid to acquire a commission. Therefore, the adverse selection problem [26] should be minimized by adopting such a mechanism. In addition, given the ease of the selection process, facility managers may be incentivized to delegate specific jobs to secondary service providers to the extent that subcontracting costs are lower than job-related costs and that certain quality standards are at least met. Increased transparency makes it possible for certificating institutions and peer organizations (i.e., buyers and providers) to prevent collusive practices [6]. Third-part institutions can easily access the record history of tendering transactions and verify their correctness. When more than one service provider is involved, buyers can assess each providers' contribution to overall performance [24]. At the same time, the Agent is protected against the risk of the buyer's not paying the due amount prescribed by the contract. To the extent that all relevant KPIs are encoded as conditions within the smart contracts, payments can be set as automatic upon the achievement of pre-specified threshold values. Finally, reputation-based evaluation systems could be set up, both for buyers and the providers, in order to promote trust and accountability among adopters.

## 6. Conclusions

In this paper, we discuss the design of a blockchain solution capable to support the Global Maintenance Service on-chain, the implementation of the Principal/Agent relationship and how modeling of the GMS on-chain provides several advantages. The transparency of Blockchain can eliminate the asymmetry of information and consequently, it reduces (or even eliminate) the P/A problem and allows a transparent and immutable bidding process for the selection of Agents. The algorithmic governance autonomously managed by smart contracts is capable to implement decentralized decision-making processes providing the highest guarantee of impartiality to all the involved stakeholders and the shared blockchain infrastructure allows us to minimize the information coordination, verification and intermediation costs.

All these arguments encourage us to proceed in this investigation, however, a number of relevant questions still need to be properly handled.

The selection of the most suitable blockchain technology is the first relevant issue. Public/permissionless blockchains provide the highest guarantees but could be difficult to be implemented in an industrial context where some information is necessarily sensitive and private. However, the natural different interests of Principal and Agents, at least economically-wise, as well as the participation of different providers competing in the market, are guarantees to the achievement

of a real consensus among the parties, even in less open infrastructure such as the permissioned blockchains. The employment of the blockchain, allows us to envision new models of governance, where trust to individuals is overcome by consensus from a community. However, it is not yet clear what are the implications in legal terms of this new governance in particular in terms of accountability. More in general, the applicability of the algorithmic governance provided by the blockchain should be better investigated in view of current laws, norms and regulations [21]. In section 4, we discuss some of the main legal implications focusing on the Italian legal framework. From that discussion, and also in view of the discussion of the managerial aspects (see section 5), emerges that a number of relevant issues still need to be effectively addressed to fully support the implementation of our proposed approach, such as the compliance with the GDPR, the adoption of recognised standards and guidelines at least at national level (see the discussion on AgID) and the effective management of sensitive industrial information. All these considerations, suggests that at the date, the most suitable technology to implement GSM on-chain, are private-permissioned technologies. For this reason, we implemented our first proof-of-concept on Hyperledger Fabric. However, the discussion on legal and managerial aspects also clarify that there are significant potential benefits and there is an effort by national and international institutions to better support the adoption of such technologies in their more decentralized fashion (i.e. permisionless/public). This encourages us to continue our exploration on the applicability of these technologies to the Global Maintenance Service.

## References


[1] Blockchain Oracles for Hybrid Smart Contracts | Chainlink. https://chain.link/ [Online; accessed 18. Gen. 2022].

[2] Tellor. https://tellor.io/ [Online; accessed 18. Gen. 2022].

[3] Provable - blockchain oracle service, enabling data-rich smart contracts, 2019. https://provable.xyz [Online; accessed 26. Jan. 2022].

[4] Agency, February 2022. https://www.law.cornell.edu/wex/agency, [Online; accessed 28. Apr. 2022].

[5] Band Protocol - Cross-Chain Data Oracle, 2022. https://bandprotocol.com/bandchain [Online; accessed 26. Jan. 2022].

[6] Temofe Isaac Akaba, Alex Norta, Chibuzor Udokwu, and Dirk Draheim. A framework for the adoption of blockchain-based e-procurement systems in the public sector. In Marié Hattingh, Machdel Matthee, Hanlie Smuts, Ilias Pappas, Yogesh K. Dwivedi, and Matti Mäntymäki, editors, *Responsible Design, Implementation and Use of Information and Communication Technology*, pages 3–14, Cham, 2020. Springer International Publishing.

[7] Hamda Al-Breiki, Muhammad Habib Ur Rehman, Khaled Salah, and Davor Svetinovic. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access*, 8:85675–85685, 2020.

[8] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed

Cocco, and Jason Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA, 2018. Association for Computing Machinery.

[9] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, and Yue Cao. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, 9:61048–61073, 2021.

[10] Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. 2013.

[11] Giulio Caldarelli. Understanding the blockchain oracle problem: A call for action. *Information*, 11(11), 2020.

[12] European Commission. Evaluation study of the regulation no.910/2014 (eidas regulation). Technical report, 2021.

[13] Mohammad Dabbagh, Kim-Kwang Raymond Choo, Amin Beheshti, Mohammad Tahir, and Nader Sohrabi Safa. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Computers Security*, 100:102078, 2021.

[14] European Blockchain Partnership (EBP). Essif - european self sovereign identity framework. https://decentralized-id.com/government/europe/eSSIF/, 2023. Accessed: 08/02/2023.

[15] European Blockchain Partnership (EBP). European blockchain services infrastructure (ebsi). https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home, 2023. Accessed: 08/02/2023.

[16] EPRS. Blockchain and the general data protection regulation. can distributed ledgers be squared with european data protection law? Technical report, 2019.

[17] eSSIF-Lab EU-funded project. European self-sovereign identity framework lab. https://essif-lab.eu/, 2023. Accessed: 08/02/2023.

[18] De Stefano F. Spunti di riflessione sulla decisione robotica negoziale. *Decisione robotica*, page 215 ss., 2019.

[19] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad A. Hoque. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182:103035, 2021.

[20] Rinaldi G. Smart contract: meccanizzazione del contratto nel paradigma della blockchain. *Diritto e intelligenza artificiale*, page 343 ss., 2020.

[21] Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, editors. *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford University Press, Oxford, 2019.

[22] Dilakshan Rajaratnam Hasni Gayathma Gunasekara, Pournima Sridarran. Effective use of blockchain technology for facilities management procurement process. *Journal of Facilities Management*, 20(3):452–468, 2021.

[23] Christine V. Helliar, Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54:102136, 2020.

[24] George John and Lisa K. Scheer. Commentary: Governing technology-enabled omnichannel transactions. *Journal of Marketing*, 85(1):126–130, 2021.

[25] Wulf A Kaal. Blockchain solutions for agency problems in corporate governance. In *Information for Efficient Decision Making: Big Data, Blockchain and Relevance*, pages 313–329. World Scientific, 2021.

[26] Tobias J. Klein, Christian Lambertz, and Konrad O. Stahl. Market transparency, adverse selection, and moral hazard. *Journal of Political Economy*, 124(6):1677–1713, 2016.

[27] De Felice M. Decisione robotica negoziale. nuovi «punti di presa» sul futuro. *Decisione robotica*, page 179 ss., 2019.

[28] Maugeri M. Smart contracts e disciplina dei contratti. Technical report, 2021.

[29] MISE. Proposte per la strategia italiana in materia di tecnologie basate su registri condivisi e blockchain. Technical report, 2020.

[30] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, Dec 2008. Accessed: 2015-07-01.

[31] Razieh Nokhbeh Zaeem, Kai Chih Chang, Teng-Chieh Huang, David Liau, Wenting Song, Aditya Tyagi, Manah Khalil, Michael Lamison, Siddharth Pandey, and K. Suzanne Barber. Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. In *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, WI-IAT '21, page 128–135, New York, NY, USA, 2022. Association for Computing Machinery.

[32] EU Blockchain Observatory and Forum. Blockchain and the digital identity. Technical report, 2019.

[33] Bank of Italy. Regulatory sandbox. https://www.bancaditalia.it/focus/sandbox/index.html?com.dotmarketing.htmlpage.language=1, 2023. Accessed: 08/02/2023.

[34] Azienda ospedaliera Bianchi Malacrino di Reggio Calabria. Servizio di manutenzione degli immobili e degli imianti dell'azienda ospedaliera bianchi malacrino di reggio calabria. https://ospedalerc.it/files/old/CSA_manut_%201_%2014_j.pdf[Online; accessed April 2022].

[35] European Parliament. Digital services act: adapting commercial and civil law rules for commercial entities operating online. Technical report, 2020.

[36] Diego Pennino, Maurizio Pizzonia, Andrea Vitaletti, and Marco Zecchini. Efficient certification of endpoint control on blockchain. *IEEE Access*, 9:133309–133334, 2021.

[37] Diego Pennino, Maurizio Pizzonia, Andrea Vitaletti, and Marco Zecchini. Blockchain as iot economy enabler: A review of architectural aspects. *Journal of Sensor and Actuator Networks*, 11(2), 2022.

[38] Rigazio S. Smart contracts e tecnologie basate su registri distribuiti nella l. 12/2019. *Diritto dell'Informazione e dell'Informatica*, fasc.2:363 ss, 2021.

[39] Cerrato S.A. Appunti su smart contract e diritto dei contratti. *Banca, borsa e tit. cred.*, I:370 ss., 2020.

[40] Ali Sunyaev. *Distributed Ledger Technology*, pages 265–299. Springer International Publishing, Cham, 2020.

[41] Schrepel T. Smart contracts and the digital single market through the lens of a "law + technology" approach. *Research Study commissioned by the European Commission*, 2021.

[42] Algan Tezel, Pedro Febrero, Eleni Papadonikolaki, and Ibrahim Yitmen. Insights into blockchain implementation in construction: Models for supply chain management. *Journal of Management in Engineering - ASCE*, 37(4), July 2021.

[43] Gazzetta Ufficiale. Decreto legislativo 3 aprile 2006, n. 152. "norme in materia ambientale"

pubblicato nella gazzetta ufficiale n. 88 del 14 aprile 2006 - supplemento ordinario n. 96. https://web.camera.it/parlam/leggi/deleghe/06152dl5.htm[Online; accessed April 2022].

[44] Fennie Wang and Primavera De Filippi. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain*, 2, 2020.

[45] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, 7:22328–22370, 2019.

[46] Huanliang Xiong, Muxi Chen, Canghai Wu, Yingding Zhao, and Wenlong Yi. Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms. *Future Internet*, 14(2):47, 2022.

[47] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105:475–491, 2020.