

# “Safe Prescription”: A decentralized blockchain protocol to manage medical prescriptions

Prof. Claudio Cilli<sup>1</sup>, Dr. Eng. Giulio Magnanini<sup>2</sup>, Dr. Marco Silipigni<sup>3</sup> and Dr. Fabrizio Venettoni<sup>4</sup>

<sup>1</sup>Department of Computer Science, La Sapienza - University of Rome

## Abstract

The Blockchain technology, initially intended exclusively for the exchange of digital money, is now widely used in many different business sectors and applications. Today, in particular, one of the most promising fields of application is the certification of facts and information. Blockchain intrinsic characteristics of immutability, non-repudiation, traceability and the leading back to a digital identity, makes the Decentralized Ledger Technology (DLT) a unique and innovative tool in the information registration's field, able to guarantee transparency and protection of data transferred over digital networks. This work describes a system to certificate and digitalize medical prescriptions through the use of the Blockchain technology, namely “Safe prescription”, as well as a prototype of the system itself. The main objectives of the project are fraud prevention and straight-through processing, assuring the necessary confidentiality (e.g. patient's anonymity), integrity (e.g. prescription's immutability) and availability, during the whole life cycle of a medical prescription.

## Keywords

Medical, Prescriptions, Blockchain, Ethereum, Smart Contract, Healthcare, Cybersecurity, DLT, DApp, Medicine, Pharmacy

## 1. Introduction: State of Art

A few years after the birth of Bitcoin, the use of Blockchain technology began to expand compared to the original use of mere electronic money with the rise of the Ethereum platform. The possible DLT fields of application vary from the fashion industry (e.g. “Follow Our Fiber” initiative, in which it is possible to acquire information regarding the origin of the material and its shipment) to the Fintech (e.g. Financial products distribution), up to the world of digital health. In the medical field in particular, among the most promising projects, it is worth mentioning MediLedger: edited by Pfizer, Bayer, IBM, Deloitte, Capgemini and SAP, and many others. These projects focus on the use of the Blockchain to certify the production chain of drugs and specifically their composition, time and place of production and purchase. In the same field, another research has shown various approaches on how to use the Blockchain, such as in Quillhash, an initiative promoted by GBA, Sparkle and Ultratech, which addresses the problem of counterfeiting, abuse and fraud in the field of medical prescriptions.

---

ITASEC'22: Italian Conference on Cybersecurity, June 20-23, 2022, Rome, Italy

✉ cilli@di.uniroma1.it (Prof. C. Cilli); giu.magnanini@gmail.com (Dr. Eng. G. Magnanini); silipignimarco93@gmail.com (Dr. M. Silipigni); fabrizio.venettoni@cdp.it (Dr. F. Venettoni)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

## 2. “Safe prescription”: a new way to manage medical prescriptions

### 2.1. Why “Safe prescription”?

In some countries, like in Italy, the way medical prescriptions are managed by the national health care system (NHS) poses a lot of issues. The following are the main identified limits:

**Anonymity and privacy of patient data:** medical data are managed in cleartext;

**Security of communications:** medical data are sent by email exposing it to phishing, malware or similar attacks;

**Information certification:** there isn't any protocol in place to guarantee certification of the prescription, in terms of authenticity of the content and involvement of actors;

**Availability and resilience of the service:** current platforms are based on centralized applications and databases that are subjected to failures, attacks and routine maintenance unavailability;

**Counterfeiting of the medical prescriptions:** NHS deals with a lot of scams and false prescriptions uses, often facilitated by the weakness of the protocol;

**Paper based processes:** current processes are often cumbersome and not fully digital.

Safe prescription aims to overcome those limits, offering a robust, decentralized, secure and fully digital protocol using the DLT. In particular, it ensures the **privacy of information** through the use of specific cryptographic mechanisms applied on data in transit and at rest on the platform. In Safe prescription the **anonymity** is enforced through the protection of user data of the users at every stage of the prescription life cycle, in compliance with the main reference regulations and GDPR. Thanks to this protocol, all the informations in the system are never sent to users in files or data, but may be only retrieved by the actors through the use of tokens. In our solution the use of a DLT is able to ensure the immutability of the prescriptions managed by the platform, at each stage of their life cycle (**Information certification**). Compliance with the principle of non-repudiation is also guaranteed as well as the certification of any admissible transfer, thus making possible: (i) to trace each step of the prescription among the different actors (e.g. doctor, patient, pharmacist); (ii) to prevent any attempts of improper use (eg not repeatability of a prescription). With “Safe prescription”, in particular, the prescriptions come stored in the DLT nodes; On the other side platform uses applications and decentralized protocols on blockchain, designed to minimize the impact of malfunctions related to the availability of data and services; (**Availability and resilience of the service**). Furthermore, through the introduction of the Blockchain technology, “Safe prescription” guarantees the immutability of the medical prescriptions, addressing the counterfeiting problem.

### 3. The Project: Safe prescription

#### 3.1. Requirements Specification

Safe prescription is a fully blockchain based management system, allowing:

(i) **doctors** to manage their own prescription book in complete autonomy through: generation, filling and transmission of the prescriptions to their own patients;

(ii) **patients** to have prescriptions on their own devices, including smartphones, through a web interface, from the beginning of the lifecycle (the prescriptions are delivered by the doctor), to the end (they decides to send them to the pharmacist in order to get the prescribed medicines);

(iii) **pharmacists** to receive the digital prescriptions directly from their own customer and subsequently to be able to request the reimbursement from the NHS for the relative part the payment exemptions presented by the customer;

(iv) **NHS** to keep track of the status of each prescription, in order to verify their correctness and authenticity as well as to ascertain the claim for reimbursement to the pharmacist for the relevant follow-up, with reasonable certainty, avoiding scams resulting from false claims.

All is drawn in an indelible sequence of event relevant information, within the Ethereum Blockchain.

“Safe prescription” involves the use of a permissioned Blockchain based on an Ethereum Enterprise Alliance architecture.

In particular, medical prescriptions are represented on the platform with special utility tokens, non-fungible type, while the management of their life cycle is done through the use of specific Smart Contracts (NFT), based on the Ethereum standard called ERC-721.

Interaction between users and the platform is coordinated by specific Decentralized Applications (DApp): a separate DApp is associated to each of the categories of actors - Doctor (Doctor), Patient, Pharmacist and NHS - offering an interface to the users and the relevant Smart Contracts registered on the DLT.

Furthermore, NFTs implement the business logic to manage the entire life cycle of the digitized prescriptions, from issue to expiration, ensuring compliance with the process, roles and constraints already in place, in accordance with the principles of Least Privilege and Segregation of Duties.

Finally, the specific DApp allows NHS employees to have full visibility on each stage of the process, for each actor involved and each individual prescription managed, implementing a complete monitor of the system.

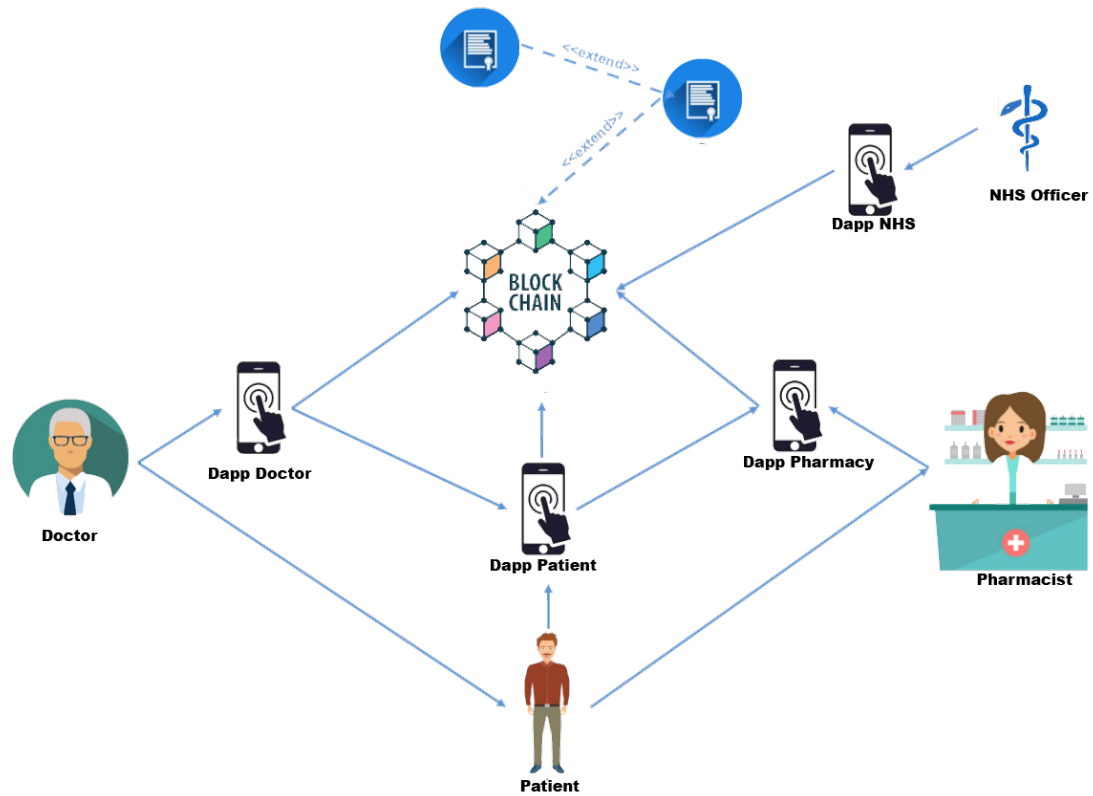


Figure 1: Prescription LifeCycle

#### 4. The protocol

Safe prescription wants to adopt a blockchain-based protocol, for the management of the life cycle of a recipe through the correct level of confidentiality (STP), able to prevent fraud and ensure the correct level of confidentiality (eg. Patient's anonymity) , integrity (e.g. immutability of the prescription) and availability of the system. As described in paragraph 3.1, the whole process can be summarized in the following flow chart:

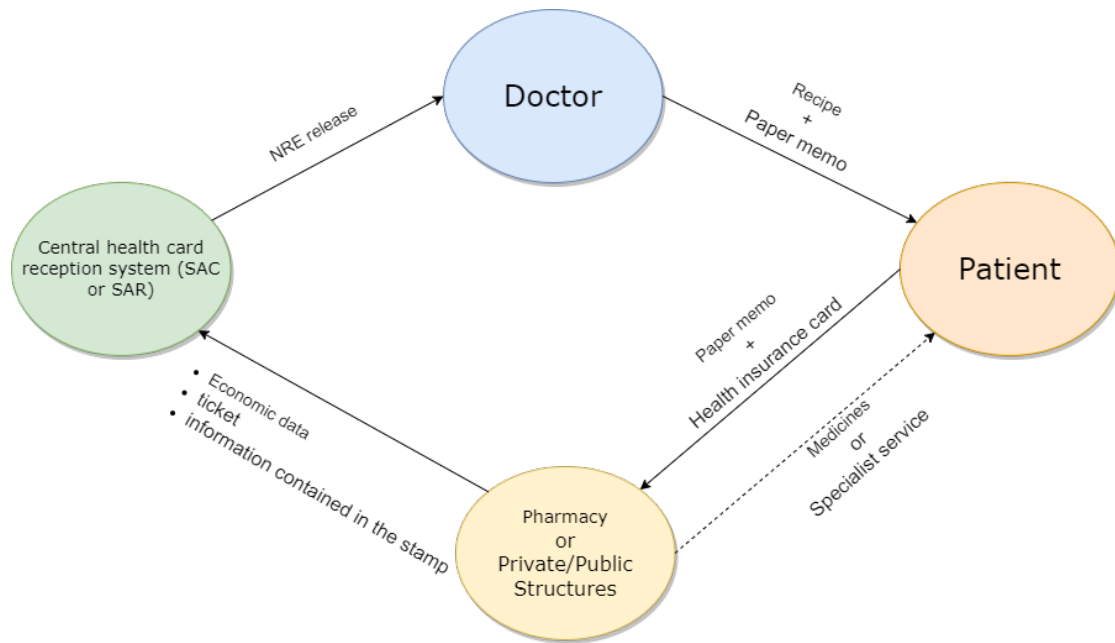


Figure 2: Safe Prescription Architecture

Currently, to make a prescription, the doctor must connect online to the "Central health card reception system" (SAC or SAR if the system is regional) and enter his identification number, patient data, medicine or necessary tests, the diagnostic question (i.e. the health problem that motivates the request for the service), any exemptions (for income or pathology) and the priority code for outpatient specialist services that are carried out for the first time. After having "generated" the dematerialized prescription, which is stored in the system and identified through a unique national code, that is the electronic prescription number (NRE), the doctor delivers a paper memo (also available online where the regional system provides for it), printed on a white sheet in A5 format, which the patient takes to the pharmacy to collect the medicines or to the health facility to perform the examination, or to the CUP (Single Booking Center) to book the visit or diagnostic tests. By connecting to the same system, the pharmacist (or the CUP operator in the case of an assessment) accesses the digital prescription using the electronic prescription number and tax code provided by the patient, finally delivering the drug or booking the service. Like the red recipe, the reminder can be spent only once, within 30 days from the date of issue. After that, the prescription is blocked by the system and the drug or prescription is no longer deliverable.

#### 4.1. Structure and Process diagram

In order to secure and fully digitize the current management process of the life cycle of medical prescriptions, the protocol brings together the main characteristics of the so-called non-fungible tokens [LINK TO APPENDIX] within an Ethereum-based blockchain, to represent medical prescriptions within the system. The protocol is in fact based on the production, exchange and consumption of non-functional tokens (recipes) between the different players involved

(i.e. doctor, patient and pharmacist), each in the exercise of their role within the blockchain (STP) . In particular, it provides for a first phase of accreditation of doctors and pharmacists: the national health service, through its DaPP, enables doctors and pharmacists to use the "Safe Prescription" system through: (i) the delivery to doctors of NRE necessary for the creation of their recipes; (ii) the acknowledgment of the pharmacist at the time of the reimbursement request. Once enabled, the doctor can prescribe a prescription to a patient, by generating an NFT instance containing the characteristic information of the prescription itself (eg list of medicines, diagnostic questions, NRE). These tokens are then transferred to the patient's wallet to then be used in authorized pharmacies, during the purchase of medicines upon presentation of the relative medical prescription. In practice, each pharmacist, who is also registered in the system, can ask the patient to transfer the token relating to the prescription, allowing him to take advantage of the prescription. Once this transfer has taken place, the token is found in the pharmacy wallet to then be transferred in turn to the SSN register and allow you to complete the life cycle of the token and the corresponding recipe.

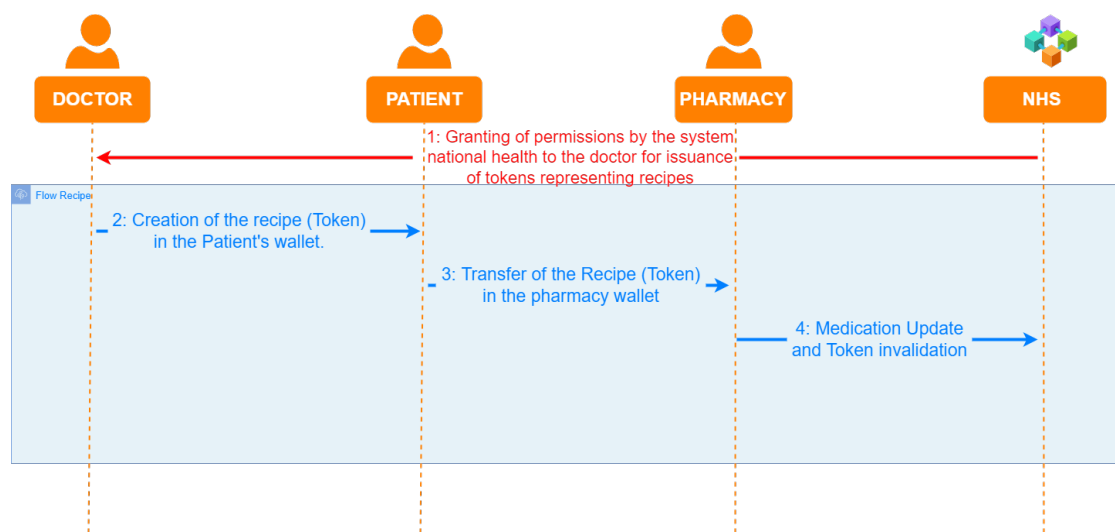


Figure 3: Safe Prescription LifeCycle

As regards the level of authorization to the system, it should be noted that the system provides for an authoritative model based on mutual recognition of users and their role, in order of relevance: the national health system invites doctors to participate in the process through recognition and the delivery of the NREs. Doctors involve their patients in the system by delivering NFT-Recipes to their respective wallets. Finally, once the pharmacists have received the same on their wallets when the patients purchase the medicines, they can present themselves and register the same NFTs at the NHS for any reimbursement, thus completing the life cycle of a medical prescription.

#### 4.2. Security Analysis

This protocol was created with the intention of solving the problems described in paragraph 2.1 without forgetting the IT security aspects, with the aim of preventing fraud and guaranteeing

the correct level of confidentiality, integrity and availability of the system and all information managed internally.

#### **4.2.1. Protocol security overview**

The protocol is based on the use of NFTs within an Ethereum blockchain, an infrastructure capable of ensuring integrity, availability and non-repudiation "by design" at all times. In the proof of work described in this article in particular, a permissioned blockchain was used, to which the various actors have no direct access except through the system's DApps. In this way it is not possible to access transactions external to your account, all this is guaranteed thanks to the management of roles at the contract level. Furthermore, it is worth remembering the following distinctive features of the protocol: (i) only the OWNERS of the tokens [In this case it is necessary to talk about the ownership of smart contracts specifying how they were used in the permissioned blockchain], the OWNER of the system ( NHS) and the prescribing doctor are authorized to read the data within them; (ii) the system segregates responsibilities through the implementation of roles in separate dApps; (iii) the tokenization of the recipes as well as guaranteeing full control of the same by the NHS in every case of their life cycle ensures their limited circulation and prevents their multiple unauthorized presentation / usability (e.g. it is also possible to provide a new parameter associated with the token that specifies the number of submissions or the expiry date of the recipe); (iv) The protocol guarantees the complete auditability of the system by any control bodies or the NHS.

#### **4.2.2. System availability**

The resilience of the system is guaranteed by the trusted operators who provide the permissioned blockchain service, such as the SSN. In this case, the system is able to guarantee the required degree of availability, possibly also 7x24.

#### **4.2.3. Data Integrity**

Also as regards the integrity of the information present in the system (eg medical prescriptions, transactions) it is guaranteed by the intrinsic characteristics of the NFT and DLT.

#### **4.2.4. Data Privacy**

Since these are medical data, current legislation in Europe prohibits their disclosure to other users who are not part of the medical staff (doctors, pharmacists, NHS). Safe Prescription, through the management of the ownership of the individual tokens, guarantees their complete confidentiality. In fact, the recipes can only be consulted by owning the token ownership and therefore having the token inside the wallet. The only ones who can access the reading of the data contained in the tokens at any time are: the doctor who issued it and the NHS (Owner of the whole system). In the proof of work described in this article, the data entered in the NFTs are in clear text but nothing prevents you from encrypting this information in future implementations.

#### 4.2.5. Manage access and privileges

The proposed system is designed to guarantee the principle of least privilege to each of the actors involved in the system. Thanks to the potential expressed by the Solidity programming language, it was possible to guarantee a correct separation of the roles of the actors and management of the assignment of the relative permissions. The identified actors are the following:

ID	ACT-01
Name of the actor	NHS officer (NATIONAL HEALTH SERVICE)
Parent	-
Description	Responsible for the deployment of tokens in the blockchain and therefore he is the only one who can have the vision and control of the whole system at every stage of the recipe life cycle.

Figure 4: NHS

ID	ACT-02
Name of the actor	Doctor
Parent	-
Description	User who interfaces with the Doctor Dapp for the creation of recipes (tokens). It can create recipes and follow their life cycle until they arrive in the national health system.

Figure 5: Doctor



<b>ID</b>	ACT-03
<b>Name of the actor</b>	Patient
<b>Parent</b>	-
<b>Description</b>	User who interfaces with the Patient Dapp for the management of the related recipes. This figure can only perform basic operations, such as receiving a recipe, reading it, transferring it and burning it.

Figure 6: Patient

<b>ID</b>	ACT-04
<b>Name of the actor</b>	Pharmacist
<b>Parent</b>	-
<b>Description</b>	User who interfaces with the Pharmacy Dapp for the management of the related recipes. It is the actor who is at the end of the natural life cycle of a token, it can only read its tokens and deliver them to the national health system.

Figure 7: Pharmacist

Through this identification, a matrix of roles and responsibilities was defined and the minimum possible privileges were assigned to each actor present in the system. A snippet of the matrix is shown in the figure

	Administratori	Create Prescription	Transfer prescription to patient	Transfer prescription to Pharmacist	Transfer prescription to Doctor	Transfer prescription to NHS	Burn Prescription
Doctor		●	●				Always if he has created the prescription
Patient				●	●		Only if the prescription is in his wallet
NHS	●						Always
Pharmacist						●	Only if the prescription is in his wallet

Figure 8: Matrix of roles and responsibilities

## 5. Implementation

### 5.1. Blockchain

In order to implement the decentralized applications, it was first necessary to identify a blockchain network to use for code testing. Using the Main net (main Ethereum network)

was not a reasonable choice, as each transaction needs the payment of a fee, resulting in a significant expense not feasible in the development phase. To overcome this problem, Ethereum developers use the well known test nets, which faithfully simulate the main-net, and don't need any transaction fee. The most used testnets are:

- **Görli:** A proof-of-authority testnet that works across clients.
- **Kovan:** A proof-of-authority testnet for those running OpenEthereum clients.
- **Rinkeby:** A proof-of-authority testnet for those running Geth clients.
- **Ropsten:** A proof-of-work testnet.

These networks did not represent the optimal solution to the problem posed at the beginning of this paragraph since they provide a limited number of miners and therefore make considerable delay in the creation of new blocks and, consequently, in the transaction approvals. Therefore, in order to have a reliable, fast and controllable network to work, we have decided to create a private local testnet. This network guarantees the control of every parameter, it's light and produces a detailed log. To create this network, we adopted the suite named Ganache.

## 5.2. Ganache

For the first phase of testing we decided to use Ganache, a software that allows the creation of a local Blockchain. It was then possible to set up a network with the ideal options for system operation, such the quantity of gasPrice<sup>1</sup>, or the local port on which to run the system as well as the IP address of our machine. An advantage of using Ganache is to have a network that, in case of transactions considered "wrong", produces a detailed status log. This is an advantage that should not be underestimated, as the aforementioned testnets do not allow it. In fact, when an exception is triggered, if this is linked to the code, Ganache identifies the wrong portion and displays the cause that triggers the exception. In addition to the advantages described so far, the implementation of a private network allows to bypass the problem related to the size of the contracts.

Ganache also provides an already pre-configured environment, which means that it already has pre-configured test accounts (by default they are ten) with all details, such as private keys, public keys and seed phrases. It is also possible to set the Ethereum available for each account. In addition to the details of the accounts that interact, it is possible to examine the details of the system, and therefore of all blocks and transactions to obtain information on what is going on in the blockchain. All of this can be achieved with a graphical interface that makes testing faster and easier.

## 5.3. Ropsten

After the alpha phase implemented on a local private network, we decided to move the prototype on the Ropsten network, in which the operation mirrors the Ethereum network (with all its limitations), to verify the actual compliance with the Main-Net.

---

<sup>1</sup>one of the parameters to be set for ensuring the correct execution of the contract. gasPrice shows the the contract processing for a miner

#### **5.4. Medical Prescriptions and Tokens**

In this project, medical prescriptions are represented in the Ethereum Blockchain as tokens of smart contracts. Tokens are issued by a licensed Doctor (who has received minter's permits from the National Health System).

#### **5.5. Medical Prescriptions in the Blockchain**

In order to represent the prescriptions within the blockchain it was necessary to create a struct. Structs are defined and custom types that can group several variables.

```

struct Prescription {
    // Token's id
    uint token;
    // number of electronic medical prescription
    uint nre;
    // Issue date of the prescription
    uint256 release0n;
    // drugs in the prescription
    string farmaci;
    // patient address
    address patient;
    //Doctor address
    address doctor;
    // Pharmacy address
    address pharmacy;
    // date when the recipe was transferred to the NHS
    uint burnedTimestamp;
    /*
     * 0: transferred
     * 1: burned
     * 2: created
    */
    uint16 action;
    /*
     * 0: towards the doctor's wallet
     * 1: towards the patient's wallet
     * 2: towards the pharmacy's wallet
     * 3: towards the NHS's wallet
    */
    uint16 movedTo;
    // timestamp of the last transaction made
    uint transactionTimestamp;
}

```

Figure 9: Struct Model

The struct contains all information necessary to understand the status of a prescription at any stage of its life cycle and the addresses of the actors who interact with it.

## 5.6. Smart Contract

The contracts created for this project have been written in Solidity. They contain the functions that allow to manage and modify the entire life cycle of the prescriptions. Each operation performed is published on the blockchain and everything is recorded on it. Each contract is compiled with Truffle, and is deployed on the Ropsten TestNet.

The other tool used in this part of the project is Metamask, a lightweight client that provides, when installed as a Google Chrome extension, a wallet for managing the ethers of each account and to send transactions to the blockchain.

### 5.6.1. NHS.sol

During the design phase, we used inheritance to manage access to functions or lists, thanks to the different visibility provided by Solidity. In this contract we can find the implementation of the fundamental Struct that represents: the prescription, the modifiers (i.e.: the functions necessary for the validation or verification of particular conditions within the smart-contracts), and the fundamental functions that are made available exclusively to the National Health Service.

### 5.6.2. PrescriptionNFT.sol

In this smart-contract there are the necessary functions for the management of the token by its owner. This means that only the owner of the wallet where the token resides can call these functions. This statement is not entirely correct as there are exceptions: one of these is that the doctor can follow the token life cycle, i.e. the prescription, and perform operations on it, even if the token is not in the doctor's wallet, since the doctor is the actor who issued it.

## 5.7. DApp

As already seen in the previous sections, the system is made up of 4 Dapps, one for each actor involved in the system. We will make an excursus on the main characteristics for the correct functioning of the life cycle of a medical prescription, from issue to its withdrawal by the National Health System.

The system provides additional functionality through each of the platform's DApps. In particular, they allow the actors to read the medical prescriptions held at any time, delete them where necessary and keep their history.

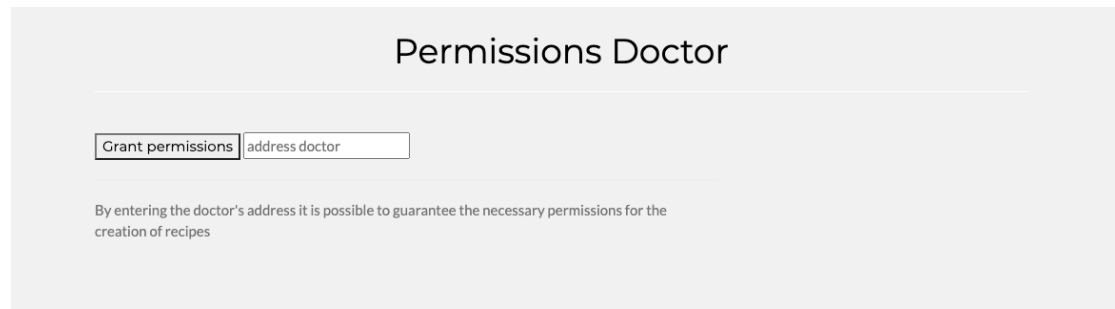
### 5.7.1. DApp NHS

The NHS Dapp represents and manages the most important element in the system, since it is the unique responsible for deploying the contract on the blockchain.

This DApp communicates with all the contracts that make up the system. In this way it has the possibility of having complete visibility of the status of the emissions and on all the changes made.

The functionality that starts the life cycle of a prescription is "the doctor's authorization to issue tokens" and therefore to prescribe medicines and therapies.

It allows the employees of the National Health Service to authorize doctors to create and transfer prescriptions to patients through the system. To do this, at the outset, the public keys of the wallets of the doctors are recorded in the blockchain, by inserting the keys (addresses) into a DApp form, as shown in the figure below.



**Permissions Doctor**

By entering the doctor's address it is possible to guarantee the necessary permissions for the creation of recipes

**Figure 10:** Authorization function of the doctors of the NHS dapp

Through this DApp, an employee of the National Health Service, in addition to authorizing doctors to operate on the platform, can check any time the processing status of each prescription, identify the doctor who created it, the date of creation and when the patient presented it to the pharmacy.

## 5.8. DApp Doctor

This DApp shapes the figure of the doctor and his functions. The doctor is the only actor in the system who can issue tokens and create prescriptions. Another uniqueness of this DApp is to follow the life cycle of the prescriptions it issues, so the Doctor is the only person who, even not being the owner of the contracts, has a view on the tokens issued by him, throughout their life cycle.

In particular, the creation function allows the doctor to make a new prescription and to deliver it to the patient by transferring the corresponding token to the patient's wallet, using a specific function of the NFTs the DApp interacts with.

## Create Prescription

In this section you can create the prescription in the blockchain

Fill out the prescription

NRE:   
Enter the code nre

PRESCRIPTION:

Write the prescription

PATIENT:   
Enter the patient's address

Figure 11: Creation of a new medical prescription

### 5.9. DApp Patient

Once the prescription is in the patient's wallet, they can "spend" it in the pharmacies through the appropriate DApp. The patient's DApp, in fact, allows to transfer a prescription from their wallet to the pharmacist one, specifying in a special form the token representing the chosen medical prescription and the address of the destination pharmacist.

### Transfer prescription to the pharmacy

By entering the address of the pharmacy it is possible to transfer the prescription.

Figure 12: Transfer prescription to the pharmacy

This DApp, in particular, interacts with the NFT Smart Contracts by calling the `safeTransferFrom` function provided by the ERC-721 standard, which implements the logic of the token transfer between two wallets and carries out the necessary checks for the correct execution of the related action checking if the prescription being transferred has expired and, if necessary, sending an alert to both the patient and the pharmacist.

### 5.10. DApp Pharmacy

The Pharmacy Dapp is the last step in the life cycle of a prescription: in fact it is the only actor who communicates with the NHS.

This functionality represents the final phase of the life cycle of a medical prescription and the

corresponding token. Through this DApp, the pharmacist can transfer the prescription he owns from his wallet to that of the National Health Service, specifying the identification of the prescription otherwise no longer usable.

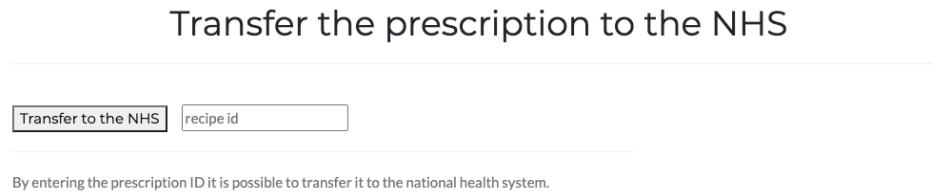


Figure 13: Transfer the medical prescription to the NHS

## 6. Conclusion

Blockchain technology has conquered even those who initially doubted their use in areas of real applications or in public contexts.

This project aims to be a tangible proof of concept, a prototype allowing to manage the entire life cycle of a medical prescription in a fully digital process, with its tokenization on a Blockchain Ethereum, in which all involved parties (doctor, patient, pharmacist and NHS) interact with the DLT and their wallets, through a specific interface.

In conclusion, Safe prescription, as well as a prototype for the realization of a service real with a solid business case, also wants to be an example of what impact could have use of the DLT on the growth of our country in general and on the quality of the National Health Service in particular, through innovation and radical streamlining of current bureaucratic procedures.

## 7. Future developments

### 7.1. KYC and Decentralized Storage

One of the additional feature for future releases could be the implementation of the Know your customer process through the DLT.

Furthermore, the possibility of integrating services that already offer such a functionality among those available on the market could be evaluated (e.g.: UPort).

Another possible feature could be the decentralized management of additional data and documents (so called Decentralized Storage Network).

### 7.2. Enhancement of information assets

With the increasing use of the system, it will be possible to have a large amount of information that could be analyzed - through AI techniques for example - to provide additional value added services, including:

- the definition of predictive models of drug consumption and mapping of related pathologies, supporting the NHS in many ways;



- the production and supply processes optimization of drugs, supporting healthcare industry sector in many ways.

### 7.3. Payments

Security, transparency and non-repudiation remain core features of the Safe Prescription System. These characteristics fit particularly well for any payment scheme implementation. Then, an additional feature could be related to the introduction of its own digital currency payment scheme.

Such an evolution would involve new players, responsible for issuing and managing the electronic money.

### 7.4. Non-digitized patients

During the feasibility analysis it was found that a considerable number of recipes concern people in old age and/or with an objective difficulty in using web and mobile technologies. A first hypothesis being studied is based on the possibility for non-digitized users to delegate one or more people to act in their own name and on their own on the Safe Recipe system, in such a way as to allow authorized subjects to obtain the prescription and collect the drugs. correspondents through the use of the platform. Another solution for the non-digitized patient involves the use of their own health card for the withdrawal of drugs. While NHS, doctor and patient continue to operate through Safe Recipe in the usual way.

## A. Appendices

### A.1. Blockchain

The blockchain or "chain of blocks" is a shared and immutable data structure represented by a chronological sequence of records or "blocks", the integrity of which is ensured by the use of specific cryptographic functions (e.g. Hash functions<sup>2</sup>). In particular, data in a block, once written, cannot be retroactively altered without all the blocks following it being modified. Each block, in fact, contains a digital fingerprint or cryptographic hash of the previous block. In this way, every time a new block is generated, the entire previous chain is made immutable. It's possible to distinguish three types of DLT:

- *Permissionless or Public Blockchain*: they are public blockchains in which the consensus model is decentralized; anyone can access them and contribute to their growth (e.g. Bitcoin, Ethereum). It is worth noting that writing in a public blockchain has a cost, proportional to the remuneration that the participants or miners require for the approval of the transactions; moreover, everything written in the register remains immutable, accessible by anyone and forever.

---

<sup>2</sup>A Hash function is a non-invertible operation (such that it is not possible to trace the origin with which it was generated) that allows you to map a sequence of characters and/or numbers of variable length into a unique string of predefined length. The hash is used, among other things, to uniquely identify each transaction, block and sequence of blocks.

- *Permissioned or Private Blockchain*: they are blockchains with restricted access, managed by a private body, which manages their evolution and controls their access in total autonomy (e.g. Ripple (XRP) and Hyperledger). Since the number of people who can access it is limited, writing to you usually has a lower cost. A private blockchain does not offer any kind of guarantee in terms of immutability, integrity and certification of the data contained therein.
- *Consortium Blockchain*: are particular types of permissioned blockchains where the management is carried out by a consortium of subjects (e.g. Quorum and Corda). The consortium then becomes the guarantor of the blockchain. Also in this case there are not sufficient guarantees in terms of immutability, integrity and certification of the data contained therein.

Our solution is based on the permissioned Blockchain Architecture under the governance of the National Health Services.

## **A.2. Ethereum**

Thanks to its innovative feature of programmable Blockchain, Ethereum introduces a new type of DLT technology, by virtue of which it is possible to create decentralized applications, with a Turing complete<sup>3</sup> computational model, which goes far beyond cryptocurrencies transfers.

With Ethereum, therefore, the concept of Decentralized Database is moving forward to Distributed Computing. Infact it can be considered a computational platform that is remunerated through exchanges of Ether, the internal cryptocurrency.

## **A.3. Smart-Contract**

Smart contracts are portions of code stored on the blockchain and available for execution. In particular, they allow the exchange of money, properties, securities or any other asset, in a transparent way and without any intermediary. As a matter of fact, using Smart contracts it's possible to identify objects (such as cars, paintings, financial securities or medical prescriptions) and the actors involved in the change of state of the objects themselves (e.g. the transfer of ownership of an asset) in full transparency and traceability.

## **A.4. Ether**

Ether plays a dual role within the platform: it represents the internal digital currency and constitutes the reward received by the miners for the approval of the transactions. Participants involved in the Ethereum platform are able to verify and validate usual currency transfer transactions of the circuit (as in the case of Bitcoin) and contribute to the execution of smart contracts through the use of the computational resources of the network, in a dedicated execution environment called Ethereum Virtual Machine (see next paragraph), for which a reward is requested.

---

<sup>3</sup>Properties of computational models that have the same computational power as a universal Turing machine (MTu), as in the case of the main programming languages

## A.5. Ethereum Virtual Machine - EVM

The Ethereum Virtual Machine (EVM)'s physical instantiation can't be described in the same way that one might point to a cloud or an ocean wave, but it does exist as one single entity maintained by thousands of connected computers running an Ethereum client. The Ethereum protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine. It's the environment in which all Ethereum accounts and smart contracts live. At any given block in the chain, Ethereum has one and only one 'canonical' state, and the EVM is what defines the rules for computing a new valid state from block to block.[1]

## A.6. Token

Ethereum tokens are simply digital assets that are being built on top of the Ethereum blockchain. They can be managed programmatically in the Ethereum's existing infrastructure, strengthening the Ethereum ecosystem itself by driving the demand for Ether, needed to power the smart contracts. Ethereum tokens can represent anything from a physical object like gold (Digix) to a native currency used to pay transaction fees (Golem). In the future, tokens may even be used to represent financial instruments like stocks and bonds. The properties and functions of each token are entirely subject to its intended use. Tokens can have a fixed supply, constant inflation rate, or even a supply determined by a sophisticated monetary policy. Tokens can be used for a variety of purposes such as paying to access a network or for decentralized governance over an organization. Tokens are often distributed to public through a crowd sale called Initial Coin Offering (ICO). Tokens creators will issue them in exchange of ether, bitcoin or even other digital currencies. There have been many ICOs recently and in a short time they have completely changed the way projects are funded. There is no requirement that tokens must be well distributed, although if you are building a decentralized application ideally you want the tokens to be owned by as many people as possible. Similar to bitcoin and ether, Ethereum tokens are also tracked on the blockchain which is the public ledger of all transactions that have occurred. This is because Ethereum tokens are just a specific type of smart contract that live on the Ethereum blockchain.[2]

### A.6.1. NFT vs. FT

When we talk about not-fungible token (NFT) we are talking about unique objects, which can neither be divided nor exchanged with other similar ones. Instead, when we talk about Fungible Token, like Ether or any ERC20 tokens (see below), we are talking about objects that can be exchanged or divided. To better understand the concept, it is possible to refer for example to the 100€<sup>4</sup> banknote: it can be exchanged for two 50 € banknotes or five 20 € banknotes. On the contrary, if we take a car, it cannot be exchanged with others or with their parts (i.e. motor, wheels, etc.). For example, if tokens are used for payments, this must necessarily be of the fungible type. On the other side, if a token represents a unique object, such as an asset to be collected, then it must necessarily be of type "not fungible".

---

<sup>4</sup>Currencies gain more value from their fungibility. The more a specific currency is considered and accepted, the more people will use it and consequently, ceteris paribus, the greater is its perceived value.

## A.7. ERC Standard - Ethereum Request for Comment

To create highly scalable and interoperable ecosystems, it has been necessary to create specific standards that classify and categorize the various types of Smart contracts and tokens. These standards are called "ERC", Ethereum Request for Comment, with a unique number associated with them. The most mentioned standards are the ERC20, standard for fungible tokens and the ERC721 standard for non-fungible tokens.

Safe Prescriptions is implemented on Enterprise Ethereum Alliance Architecture and uses ERC-Based Smart Contracts open standard.

## References

- [1] A. Beregszaszi, Ethereum virtual machine (evm), 2021. URL: <https://ethereum.org/en/developers/docs/evm/>.
- [2] L.Xie, A beginner's guide to ethereum tokens, 2017. URL: <https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b>.
- [3] investopedia.com, Fungibility, ????. URL: <https://www.investopedia.com/terms/f/fungibility.asp>.
- [4] trufflesuite.com, Smart contracts made sweeter, ????. URL: <https://www.trufflesuite.com/>.
- [5] djangoproject.com, Django, ????. URL: <https://www.djangoproject.com/>.
- [6] trufflesuite.com, Ganache overview, ????. URL: <https://www.trufflesuite.com/docs/ganache/overview>.
- [7] ethereum.org, Ethereum testnet, ????. URL: <https://ethereum.org/en/developers/docs/networks/>.
- [8] V. Buterin, Contract code size limit, ????. URL: <https://github.com/ethereum/EIPs/issues/170>.
- [9] N. S., Bitcoin: A peer-to-peer electronic cash system; 2008, Available from: <https://bitcoin.org/bitcoin.pdf> (Accessed July 3, 2019).
- [10] K. T-T, K. H-E, O.-M. L., Blockchain distributed ledger technologies for biomedical and health care applications, *Journal of the American Medical Informatics Association*. 2017;24(6):1211–20. Epub September 8 (2017).
- [11] D. Ichikawa, M. Kashiyama, n. T. Ueno: "Tamper-resistant Mobile Health Using Blockchain Technology", gov, 2017.
- [12] H. Yu, H. Sun, D. Wu, T.-T. Kuo, "Comparison of Smart Contract Blockchains for Healthcare Applications", *AMIA Annu Symp Proc*, 2019.
- [13] Y. X, W. H, J. D, L. M, J. W., Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, *Journal of medical systems*, 2016.
- [14] W. Dai, b-money, <http://www.weidai.com/bmoney.txt>, 1998. URL: <http://www.weidai.com/bmoney.txt>.
- [15] H. Massias, X. S. Avila, J. J., Quisquater,, ????
- [16] K. T-T, H. C-N, O.-M. L., *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States: 2016. ModelChain: Decentralized

Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks, 2016.

- [17] S. Haber, W. S. Stornetta, How to time-stamp a digital document, in: *Journal of Cryptology*, vol 3, no 2, 1991, pp. 99–111.
- [18] D. Bayer, S. Haber, W. S. Stornetta, Improving the efficiency and reliability of digital time-stamping, in: *Sequences II: Methods in Communication, Security and Computer Science*, 1993, pp. 329–334.
- [19] S. Haber, W. S. Stornetta, Secure names for bit-strings, in: *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 1997, pp. 28–35.
- [20] X. Q, S. EB, A. KO, G. J, D. X, G. M., MeDShare: Trust-less medical data sharing among cloud service providers via blockchain, *IEEE Access*, 2017.
- [21] A. Back, Hashcash - a denial of service counter-measure, <http://www.hashcash.org/papers/hashcash.pdf>, 2002. URL: <http://www.hashcash.org/papers/hashcash.pdf>.
- [22] R. C. Merkle, Protocols for public key cryptosystems, in: *Proc*, 1980, pp. 122–133.
- [23] C. B, K. B, M. E, P. E, T. A., *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States: 2016. *Blockchain: Securing a New Health Interoperability Experience*, 2016.
- [24] K. T-T, Z. R. H, O.-M. L., Comparison of blockchain platforms: a systematic review and healthcare examples, *Journal of the American Medical Informatics Association*. 2019;26(5):462–78. Epub March 25 (2019).
- [25] W. Feller, *An introduction to probability theory and its applications*, 1957.
- [26] T. S. C.-O. P. Language, Available from: <https://github.com/ethereum/solidity>, (Accessed July 3, 2019).
- [27] Z. P, W. J, S. DC, L. G, R. ST., Fhircain: applying blockchain to securely and scalably share clinical data, *Computational and structural biotechnology journal*, 2018.
- [28] D. A, X. Z, R. S, S. M, W. F, editors, *AMIA Annual Symposium Proceedings*, 2017.
- [29] H. Zhao, Y. Zhang, Y. Peng, R. X. (Eds.), *Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys*, Institute of Electrical and Electronics Engineers Inc, 2017.
- [30] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T., Hayajneh: "health-care blockchain system using smart contracts for secure automated remote patient monitoring", *Syst*. 42 (2018).
- [31] J. Dias, L. Reis, . H. Ferreira, Martins: "Blockchain for Access Control in e-Health Scenarios", arXiv preprint arXiv:180512267, 2018.
- [32] F. Angeletti, I. Chatzigiannakis, A., Vitaletti: "privacy preserving data management in recruiting participants for digital clinical trials", *Proceedings of the First International Workshop on Human-Centered Sensing, Networking, and Systems*; Delft, Netherlands, ACM (2017) (????) 3144733.
- [33] T. Nugent, D. Upton, M., Cimpoesu: "Improving data transparency in clinical trials using blockchain smart contracts", *F1000 Res*, 2016.
- [34] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S., Liu: "blockchain-based data preservation system for medical data", *Syst*. 42 (2018).
- [35] M. A. Uddin, A. Stranieri, I. Gondal, V., Balasubramanian: "Continuous patient monitoring with a patient centric agent: a block architecture", *IEEE Access*, 6 (2018), ????
- [36] M. Raikwar, D. Gligoroski, K., Kralevska: "SoK of used cryptography in blockchain", *IEEE*

Access, 7 (2019), ????

- [37] S. J, R. L, W. S, Yao X: "A blockchain-based framework for electronic medical records sharing with fine-grained access control, " PLoS ONE (????).
- [38] Y. Y, M. M., Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-encryption Function for E-health Clouds[J], IEEE Transactions on Information Forensics and Security; 2016, 2016.
- [39] K. H, S. H, L. S., A simple approach to share users' own healthcare data with a mobile phone, Eighth International Conference on Ubiquitous and Future Networks (ICUFN), 2016.
- [40] N. D. C, P. P. N, D. M, S. A., Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems, IEEE Access, 2019.
- [41] J. T. S, Fast probabilistic algorithms for verification of polynomial identities in Journal of the ACM (JACM), 1980.