POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Executive Summary of the Thesis

Application of the Blockchain to Supply Chain Traceability Systems

Laurea Magistrale in Computer Science and Engineering - Ingegneria Informatica

Author: Alessandro Sommaruga

Advisor: Prof. Francesco Bruschi

Co-advisor: Prof. Vincenzo Rana

Academic year: 2020-2021

1. Introduction

The faster and faster technology development makes the standard methods adopted in the supply chain management inadequate for the growing requirements of the increasingly globalised context.
In addition, the large number of actors involved in a supply chain network leads to a lack of transparency and accountability. Consumers are becoming more ecological and environment-aware when shopping or selecting services, and paper-based certificates on products packaging are no longer enough to prove their quality and provenance.
These phenomena do not affect one single supply chain sector, but are rather widespread. A possible solution is to exploit the emerging technology of the blockchain. As recent research highlights [1], blockchain-based services have a huge potential to improve supply chains. The advantages of this approach are several. For example, the presence of a shared ledger, publicly available in almost no time, greatly reduces the downtime, thus enabling a faster and more cost-efficient delivery of products.
Within this context, the aim of this work is to design and develop a blockchain-based platform to manage supply chain traceability. A model is proposed, meant to be flexible and applicable to multiple sectors. A main requirement to be met is to provide a user-friendly tool to be integrated within the existing systems, that can also be used by non-experts in blockchain. The realisation of such a system poses a large number of challenges, addressed in this document.
In order to prove this requirement, a real-world project implementing the model is introduced, whose realisation includes different phases, like the design and development of a blockchain infrastructure, involving the author's contribution. Specifically, the development of some smart contracts is provided on the Ethereum ecosystem.
The solution brings many benefits to the supply chain, the main one being increased efficiency. The innovative aspects include full traceability along the chain, versatility to different use cases, and blockchain scalability, achieved through a particular solution to concisely store data. All those properties are supported by a carefully studied usability.

1.1. Outline

This section gives an outline of the current document, in order to make the argumentation clearer. First, blockchain technology and its link

to the supply chain are introduced. An overview of the state of the art in this context is provided. Second, a theoretical model to solve the problem is presented, including the ideas and the blockchain solutions. Third, a use case is provided, which implements the model in reality. The author's contribution is explained in this part. After that, a section is devoted to some considerations about the system: a comparison between the proposed model and its realisation, as well as a completeness analysis for the code implemented. Finally, a section is devoted to the conclusions.

2. Blockchain and the Supply Chain

This section describes the blockchain technology from a theoretical point of view, in order to provide the tools to fully understand the contents of this work. The relation between such a technology and the supply chain is explored, giving an overview of the state of the art in this context.

2.1. Blockchain

The blockchain (literally *chain of blocks*) takes advantage of the characteristics of a computer network of nodes and allows users to manage and update, unambiguously and safely, a ledger containing data (in the form of *transactions*) in an open, shared and distributed manner, without the supervision of a centralised authority. Such a mechanism provides great benefits in terms of decentralisation, transparency, traceability, and immutability. It finds application in many contexts, where the most popular is certainly the Bitcoin cryptocurrency on the finance domain. The contents reported in this section are due to the mysterious creator of Bitcoin, Satoshi Nakamoto, which stated them, back in 2008, in his white paper [2].
The blockchain belongs to the broader class of Distributed Ledger Technologies (DLT), which give read and write access to a ledger shared among a network nodes. In the absence of a central entity, nodes must reach *consensus* in order to validate the changes to be made to the ledger. The ways in which consensus is reached and the structure of the register are some of the features that characterise the different blockchains, and DLTs in general.
Based on the network type a distinction is made between:

- *permissioned* - networks in which, in order to access, a user must be registered, identified and then authorised by some admins or the network itself;
- *permissionless* - networks where anyone can access without permission.

The consensus mechanism on a permissioned network is simpler, since it is somehow a controlled environment: for example, it could be based on a majority vote.
Regarding permissionless platforms, the most widespread mechanism for reaching consensus is the Proof-of-Work (PoW) algorithm, that serves at making effective the transactions on the blockchain, by verifying and organising them in *blocks*. A set of validator nodes, called *miners*, compete with each others to create (i.e., mine) the next block. Each block can be mined through computers with high computing power, which work to solve mathematical problems, involving finding a specific hash for the block, which can be thought as the block fingerprint. The miner who exhibits the solution as a proof of its work is rewarded with new cryptocurrency tokens. This mechanism stimulates the creation of non-counterfeit blocks, thus securing the network.

2.2. Blockchain for the supply chain

The present solutions in the supply chain domain are not adequate. As specified by Gaur and Gaiha [1], the problem is that the standard methods for supply chain management do not keep up with the fast development of technologies and increase in the requirements.
Among the blockchain applications, an emerging one that suits our case is that on the supply chain. Blockchain technology, thanks to its properties, allows to fix data in an immutable way on a distributed ledger. The advantages of this approach include enabling faster and more cost-efficient delivery of products, enhancing product traceability, avoiding product counterfeiting, improving interoperability and coordination between all supply chain members.
An example of a solution based on blockchain is IBM Food Trust. Such project, by IBM in collaboration with Walmart, employs the blockchain for tracing different food products. In case of a damaged product, the blockchain en-

ables the company to trace the product, identify all suppliers involved with it, and efficiently recover it. The blockchain can also be used to help identify counterfeit goods, because these kinds of products would lack a verification history on the blockchain.
Other solutions exist, acting in different sectors of the supply chains and accomplishing different tasks. However, they all have some common limitations, as also specified by Jabbar et al. [3]. There is no general framework that encompasses different sectors and could constitute a standard, but there are only specific ones (e.g., the IBM solution is only for food chains).
The usability of the blockchain is still a great obstacle for non-experts in the industry; indeed, several solutions realised lie on permissioned platforms, which can be better controlled, and do not fulfil the blockchain decentralisation.
The information stored on-chain is only about specific aspects and products: there is not a platform that is transversal to the supply chain and allows to completely trace raw materials, processes, products and how the first two contribute to the realization of the last.
The next section proposes a model that solves some of the above-mentioned limitations, involving innovative solutions.

3. Model

The current section contains the description of a model, based on the blockchain, able to improve efficiency and traceability in the supply chain context.
After the analysis of the state of the art, it is clear that a unifying standard solution does not exist in this field. However, it is possible to exploit the benefits of the blockchain technology to implement a platform that could handle different supply chains. One the one hand, the use of blockchain brings improvements (e.g., the tracking process becomes more efficient), but on the other hand it poses a large number of challenges (e.g., how an ordinary person, inexperienced in the sector, can interact with the blockchain).
The main idea of the thesis is to employ the blockchain into different supply chain domains to implement a modular traceability service, that is also user-friendly.
The solution should be integrated into supply chain systems, also from different sectors, and improve their efficiency. In particular, it should be possible to write to the blockchain data about processes occurring in the supply chain and products handled. Afterwards, it should be straightforward to read such data with the guarantee that there was no change.

3.1. Blockchain role

The role of the blockchain in the model is large. First, blockchain allows to improve the speed of tracking process and decrease its costs, by making the data immediately available to the actors, thus decreasing the downtime.
Second, this technology enforces transparency and security. The data stored on-chain are immutable and their correctness can be verified by anyone. In particular, this is achieved by means of notarization. Notarizing a document to the blockchain means to store the hash of such document to the blockchain instead of the full document. A hash is a cryptographic function that, given an input, associates it with a string identifying it like a fingerprint. The notarization guarantees that the document is immutable from the date and time at which is made on. Only uploading the hash and not the full document allows to save costly storing space and to keep the good properties of the blockchain.
Finally, notarizing on the blockchain is also a way to overcome the heterogeneity of the old supply chains. Since they are based on several customised solutions, incompatible with each others, their integration requires an expensive burden, avoided with notarization.

3.2. Blockchain architecture

The architecture of the model has a blockchain part and a non-blockchain-related part. This section presents the former, represented in Figure 1 below.
Three main aspects emerge from this scheme: the presence of two blockchain platforms (a mainchain and a sidechain), some smart contracts (SC) and a relayer.
Concerning the two blockchains, the *mainchain* is a public permissionless blockchain; the *sidechain* is not restricted to a specific type. This specific model requires the sidechain to be public and permissionless as well and works as following. The data are not directly stored on the mainchain, but on the sidechain, which is

anchored to the former. The *anchoring* consists of certifying entire sequences of sidechain blocks on the mainchain on a regular basis, significantly reducing time and costs, without renouncing the transparency and legal validity of the permissionless mainchain. This allows to solve the scalability issues, affecting several existing blockchains.

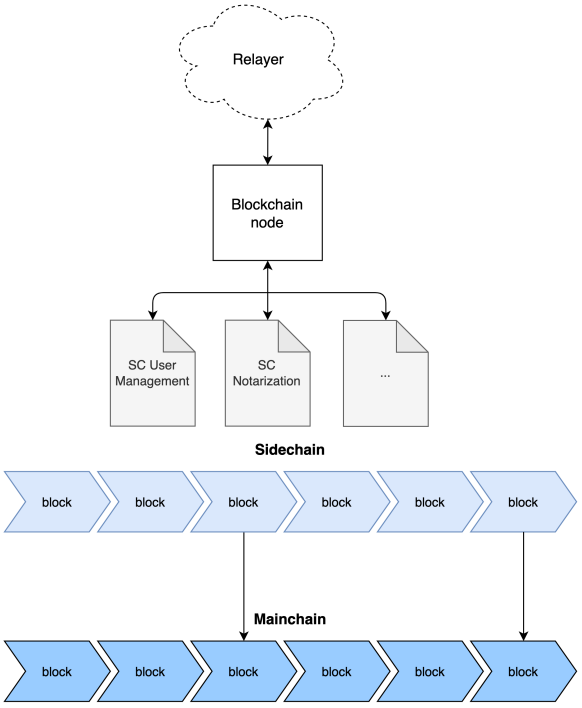

Figure 1: Blockchain architecture of the system.

Smart contracts (SC) consist of executable code snippets of contractual terms, lying on the blockchain. They operate as autonomous actors: the execution of the code is automatically and independently activated when the contractual terms are satisfied. Their behaviour is predictable, verifiable, and deterministic. For the purposes of this application, at least two smart contracts are required: one for the management of the users and one for the notarization, which relies on the first to check for users' authorisation. Other possible smart contracts are omitted due to space constraints.

The third notable component is the *relayer*, that solves another important problem affecting blockchain-based systems: the transaction fees. Indeed, notarizing has a cost in terms of cryptocurrency tokens, but the model is meant to be used by common people, non-expert of blockchain. For this reason, besides an intuitive user interface and facilitated use of the blockchain wallet, the issue of paying for transaction fees must be addressed. The solution proposed is to rely on an external service, called relayer, able to pay for executing the transactions sent by the users. This works by encapsulating the actual transaction into a so-called *meta-transaction*, executed by the relayer. The whole mechanism is transparent to the end users, perfectly fitting to the required user-friendliness.

4. Use Case

Given the proposed model, a real-world use case including its implementation is introduced. Such project, called Deply, was carried out into a company and involved the contribution of the author during different phases, like the design of the system architecture, the design and development of the blockchain part, the user interface implementation and the testing. The realisation of the blockchain part involved the development of some smart contracts on the Ethereum ecosystem.

4.1. Technologies adopted

This section describes the technological choices taken for Deply, shown in Figure 2. The system includes an application (web and mobile), made up of a front-end and a back-end.

For the front-end, Deply exploits Next.js, a React framework provided by Vercel, to develop fast and responsive web applications. Vercel hosting service is used, on which the application bundle is loaded, autonomously published and distributed to the clients.

On the other side, there is not a real back-end, rather a cloud, *backend-as-a-service* solution, provided by Google's Firebase ecosystem. The latter is a serverless infrastructure, managing the functionalities of authentication, Cloud Firestore database and Cloud Functions, i.e., functions triggered by events fired.

Besides Firestore, another database is included: IPFS. It is worth to remark the differences between the two. Firestore is the application real-time database, allowing authenticated users to access in a really fast way data about users, subscriptions to Deply, supply products and processes. IPFS, instead, is a distributed file system, employed for storing larger files. Specifically, through the hash of a specific blockchain

transaction containing supply chain data, it is possible to retrieve the associated images and documents. IPFS being distributed provides scalability and immutability, while data encryption enables confidentiality.

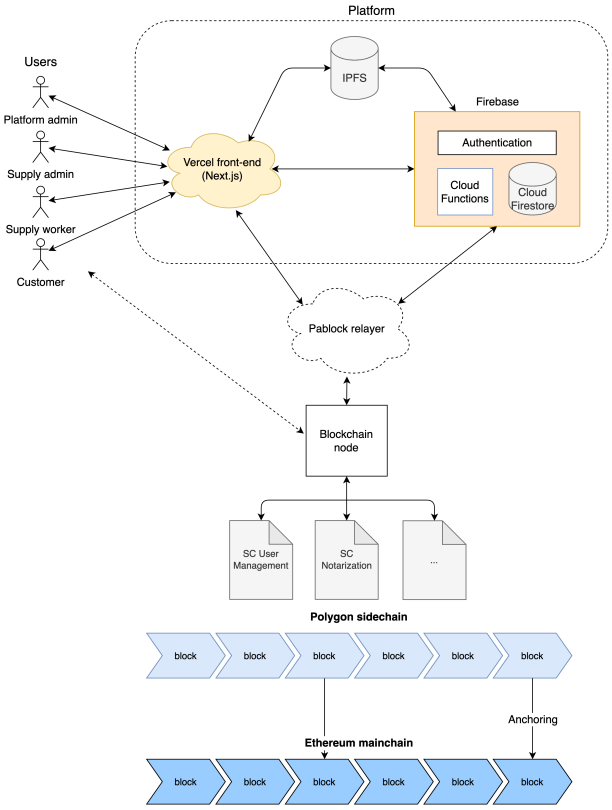

Figure 2: Deply architecture with technologies.

The link to the blockchain is realised through Pablock relayer, which is the only way to notarize on blockchain from the application.
Deply mainchain and sidechain are respectively Ethereum and Polygon. The reason for this choice is that the former is the most used platform for developing smart contracts, the latter is an efficient sidechain, with low transaction fees and an extremely high transaction rate.
Finally, users are distinguished in four roles: the customers, the supply chain insiders including admins and workers, and the platform admin.

4.2. Smart contracts

As shown above, two smart contracts have been implemented: user management and notarization. They are described in detail in the thesis document, here only an overview is given. They are written in Solidity, a language compatible with the Ethereum ecosystem, by using the Truffle framework. Pablock smart contracts interact with them in order to execute the meta-transactions. They are both deployed by the platform admin, the only one who could make certain operations.
The user management contract manages the supply admin registration and subscription to Deply, as well as the addition of workers from the supply admins. The notarization contract allows to notarize supply chain data. To do that, Pablock meta-transactions are exploited, after checking for authorisation by calling the user management contract. Also, to make it possible to notarize directly to the blockchain without the relayer, an alternative method is provided as a fallback.

4.3. Contribution

The author's contribution includes the system and blockchain architecture design, the implementation and testing of the smart contracts, the development of the application user interface (UI).
First, the author contributed to the architectural and blockchain design of the system, focusing on the smart contracts, under the supervision of a blockchain engineer. The implementation and testing of the smart contracts was then undertaken by the author. Regarding the front-end, the author collaborated to the development of the backoffice UI, corresponding to the views for Deply admins. This part included static views and dynamic parts, as the queries to Firestore and the calls to smart contracts. At the end, the author contributed to the system integration and testing.

5. Discussion

This section presents some considerations about the proposed system and use case.
Deply implementation is slightly different from the proposed model. The latter contained further smart contracts, such as some for the integration of IoT devices, not present in the first version of the project, but planned for upcoming developments. Moreover, the theoretical model did not specify the back-end nature and did not involve a second database.
About the smart contracts, a completeness analysis has been done, through testing. The tests have been written in JavaScript, through the

Truffle suite. They include positive and negative tests, respectively verifying the proper working and failure of methods. First, user management contract has been tested, then notarization, whose testing exploited the correctness of the first contract tests. The testing included a phase on a local network and one on a testnet, dedicated to development purposes.
Multiple aspects concerning usability are relevant: here we report two of them. First, the cryptographic keys are handled in a non-custodial way: users' private key is locally stored on their browser, a seed phrase is available for recovering the wallet. Second, the presence of a centralised application is a limitation for blockchain benefits. For example, if the platform or the relayer go offline, it is impossible to notarize through Pablock. This could be bypassed by directly executing the transactions on the smart contracts, but requires to have blockchain knowledge, funds to pay the fees and to manually upload related documents to IPFS.

6. Conclusions

In conclusion, the innovative aspects of this work are threefold: firstly, a great *flexibility* of application to different sectors, providing traceability to all the supply processing phases; secondly, blockchain *scalability*, obtained by means of a sidechain and anchoring techniques; thirdly, the use of a relayer to handle transaction costs.
Future works about Deply might be in the direction of IoT devices integration, through some smart contracts, but they can also concern overcoming the centralisation problem. A possible way to avoid the centralised access to the blockchain is to establish fixed entry rules for the system, and rely on a DAO (Decentralised Autonomous Organisation) for its management.

References

[1] Vishal Gaur and Abhinav Gaiha. Building a transparent supply chain blockchain can enhance trust, efficiency, and speed. *Harvard Business Review*, 98(3):94–103, 2020.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, Dec 2008.

[3] Sohail Jabbar, Huw Lloyd, Mohammad Hammoudeh, Bamidele Adebisi, and Umar Raza. Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Systems*, 27(4):787–806, 2021.