A Secure Blockchain-Based Architecture for the COVID-19 Data Network

Darine Al-Mohtar*, Amani Ramzi Daou†, Nour El Madhoun ‡§, Rachad Maallawi
*Lebanese University, Faculty of Technology, Department Communications and Computer Networks Engineering, Beirut, Lebanon
†Lebanese University, Faculty of Technology, Department Business Computer, Beirut, Lebanon
‡ Security and System Laboratory, EPITA, 14-16 Rue Voltaire 94270 Le Kremlin-Bicêtre, France
§Sorbonne Université, CNRS, LIP6, 4 place Jussieu 75005 Paris, France
Email: darinemohtar@gmail.com; amani.daou2@gmail.com; nour.el-madhoun@{epita.fr, lip6.fr}; rachad.maallawi@gmail.com

2021 5th Cyber Security in Networking Conference (CSNet) | 978-1-6654-0722-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSNET52717.2021.9614272

***Abstract*—The COVID-19 pandemic has impacted the world economy and mainly all activities where social distancing cannot be respected. In order to control this pandemic, screening tests such as PCR have become essential. For example, in the case of a trip, the traveler must carry out a PCR test within 72 hours before his departure and if he is not a carrier of the COVID-19, he can therefore travel by presenting, during check-in and boarding, the negative result sheet to the agent. The latter will then verify the presented sheet by trusting: (a) the medical biology laboratory, (b) the credibility of the traveler for not having changed the PCR result from "positive to negative". Therefore, this confidence and this verification are made without being based on any mechanism of security and integrity, despite the great importance of the PCR test results to control the COVID-19 pandemic. Consequently, we propose in this paper a blockchain-based decentralized trust architecture that aims to guarantee the integrity, immutability and traceability of COVID-19 test results. Our proposal also aims to ensure the interconnection between several organizations (airports, medical laboratories, cinemas, etc.) in order to access COVID-19 test results in a secure and decentralized manner.**

***Index Terms*—Blockchain, COVID-19, PCR, Security, Smart-contracts, Ethereum, Traceability.**

I. Introduction

The COVID-19 pandemic is a health crisis caused by an emerging infectious disease. It has impacted the world economy, mainly all activities where social distancing cannot be respected, for example in airports, concerts, theaters, and so on. Rapid and precise screening tests such as "PCR (Polymerase Chain Reaction)" and "Immunochromatography" are essential for an effective response to this pandemic because they help to identify infections and then to mitigate them. Indeed, the results of these tests have become very important, for example in the case of a trip: the traveler needs to perform a PCR test within 72 hours before his departure to detect whether he is a carrier or not of the COVID-19. If the result is negative, the person can therefore travel by presenting the negative result sheet to the agent, during check-in and boarding, to ensure that he does not have the COVID-19. The agent will then check the result sheet presented by the traveler by trusting: (a) a centralized system "the medical biology laboratory" which provided the result of the PCR test to the traveler, and (b) the credibility of the traveler for not having changed the PCR test result from "positive to negative" [1] [2].

In fact, the trust and verification procedure performed by the agent is not based on any security and integrity mechanism, despite the great importance of securing PCR test results to combat the COVID-19 pandemic. The biggest issue in this context is that laboratories send the results through mails to the people who have been tested. These people then print their results to present them later to organizations (airport, station, etc.) and this process presents both following vulnerabilities:

- *Vulnerability (1):* failure to ensure the integrity of PCR test results [3]:
  - For example, in the case of a trip (airplane or train), the agent cannot guarantee the integrity of the PCR test results, given by travelers, because he does not have access to internal laboratory data. However, if the agent "really" wants to confirm the integrity of a PCR test result, he then needs to call the laboratory but this is not really possible when traveling.
  - In the case of a positive result of a PCR test, a malicious traveler can modify the result of his test from "positive to negative" easily and without any control: "this is because the result is presented in a simple PDF file". The agent cannot subsequently detect these changes except in the case where he calls the laboratory to confirm the result.
  - A malicious traveler can also create his own document of the PCR test result with the name of a known laboratory in his country and a forged signature. The agent also cannot detect these changes except if he calls the laboratory to confirm the result.
  - Indeed, there is an absolute risk that people who are in the same airport (or in the same train station) and in the same airplane (or the same train) will be contaminated if a malicious traveler changes the result of his PCR test from "positive to negative" or creates his own PCR test result document.
  - The first fraud attempts based on false negative PCR results have already appeared in [4]. Therefore, the integrity of PCR test results is essential.
- *Vulnerability (2):* impossibility of finding the history of all PCR tests carried out by a person and therefore there

978-1-6654-0722-9/21/$31.00 ©2021 IEEE

is a lack of traceability: in the case of a trip (airplane or train), when the traveler arrives in the country of destination, he once again needs to show the agent in that country the PCR test result carried out in the country of departure, and do another PCR test within the next 72 hours. So there is no absolute traceability to know the history of all PCR tests previously performed by a person. These tests were carried out in different countries and in completely independent laboratories [5].

Indeed, these vulnerabilities are also present in the case of another type of COVID-19 test such as Immunochromatography test (see section II-A2). For vaccination, *Vulnerability (1)* is also strongly present in the case of verification if the person is vaccinated or not. Accordingly, our goal in this paper is to design a blockchain based decentralized trust architecture that aims to: (a) guarantee the integrity and immutability of the COVID-19 test results while sharing them in a decentralized and secure way between laboratories and other organizations, (b) ensure the traceability of all the results of COVID-19 tests carried out by people in national and international laboratories. We note that in this paper we will not address the case of vaccination because even though its verification procedure may be the same as the verification procedure of the COVID-19 test results, we however have not studied this context in this paper. In addition, vaccination is not mandatory today but is strongly recommended, and if there are currently some countries that open their borders without restriction to vaccinated people, there are other destinations that also require presenting a negative result of a PCR test [6].

This paper is organized as follows. In section II, we introduce an overview of COVID-19 tests and blockchain technology. In section III, we describe our proposed blockchain-based architecture. The last section concludes the paper.

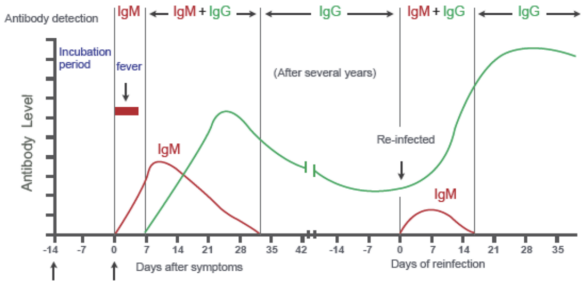

Fig. 1. IgM and IgG after Infection [7]

II. Generalities

A. COVID-19 Tests

1) PCR (Polymerase Chain Reaction): it allows to detect if a person is a carrier or not of the COVID-19, with a response: "negative search" or "positive search". For a trip for example, it must be undergone 72 hours before departure (it is only valid for 72 hours) [8].

2) Immunochromatography: it is the COVID-19 Serology test. It is used for the qualitative detection of Immunoglobulin G (IgG) and Immunoglobulin M (IgM) at the same time. IgG is a type of antibody representing about 75% of serum antibodies in humans [9]. IgM is a class of antibody representing about 10% of the immunoglobulins in an immunoserum [10]. As shown in Fig. 1, the level of IgM antibodies begins to increase approximately one week after the initial infection, while IgG antibodies appear later than IgM (generally within 14 days of infection) and can last 6 months or even several years. This means that IgG is used as an indicator of a previous infection. Patients who are infected with SARS-CoV-2 can be quickly identified by simultaneous monitoring of IgM and IgG [7].

B. State of the Art

The choice of a centralized solution was generally applied for the storage and management of health data such as in [11] [12] [13] and [14]. Indeed, with the urgency of the COVID-19 health crisis and the lack of skills on the market, the application of decentralized solutions, such as blockchain technology, was not considered, although they respond to several security aspects [15] and also to the decentralization of our health system: ARS (Agence Régionale de Santé), hospitals, laboratory, and so on [16].

1) Blockchain Technology: it is one of the solutions that seems quite apt to decentralize digitized medical networks in a reliable, secure and robust manner. In fact, it is proposed today as a new technical infrastructure to decentralize IT applications [17] [18]. The Bitcoin was the first implementation of the blockchain technology to exchange, in a decentralized manner, cryptocurrencies. The customers appreciated the Bitcoin application because of its absolute security that is guaranteed thanks to the blockchain technology [15] [19]. So, this security comes firstly from the intrinsic main property of blockchain that allows two nodes to execute transactions together without going through a Trusted Third Party (TTP), and secondly from the fact that the history of all these transactions is stored in a distributed and an immutable data ledger among blockchain nodes (it is impossible to modify the underlying records in the blockchain ledger) [16].

There are several types of blockchains and there is a dichotomy between them [20] [21]. For a permissionless public blockchain (Bitcoin, Ethereum, etc.), anyone, without revealing his true identity, can be part of such a network and ensure that peer-to-peer transactions are secure and consistent, while remaining private and available only on network nodes that support blockchain. Decentralization is strong but the lack of control of network participants can lead to a risk on the infrastructure [16] [22]. For a permissioned private blockchain (Hyperledger Fabric, Hyperledger Besu, etc.), each participant who joins the network, to contribute to the infrastructure, must first register his identity and the identity of the resources that contribute to the entire network. This is necessary so that a malicious entity, such as a hidden node, can be detected. Due to this registration process, there is also a need for an efficient node identity management mechanism in addition to the immutable blockchain ledger keeping. In this case, the decentralization of the network is weaker but thwarted by the trust placed in the participants [16].

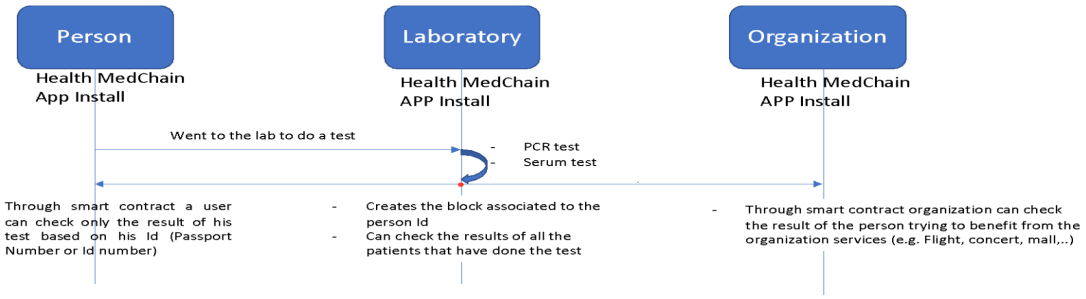

Fig. 2. Exchange Flow

2) Ethereum & Smart-Contracts: Ethereum is a distributed, an open source and a public blockchain. Ethereum's cryptocurrency is called "Ether (ETH)". In fact, since the introduction of blockchain technology and the Bitcoin system, one of the most remarkable innovations has been the introduction of the "smart-contracts" on the Ethereum blockchain. A smart-contract is written in Solidity "a Scripting Language specially designed for Ethereum". It allows developers to model, secure and exchange whatever they can mathematically represent thanks to turing-completeness. It allows two anonymous parties to do business or execute a service with each other without the need for an intermediary. The instructions of a smart-contract work exactly as they were programmed, without any possibility of immobilisation, censorship, fraud or interference of a third party [23] [24].

III. Proposed Architecture

In this paper, we propose an innovative blockchain-based architecture that will help prevent, fight and control the spread of the COVID-19 pandemic as follows :

- It allows laboratories to store, communicate and share their PCR test results in fully decentralized trust with organizations (airports, trains, etc.), requiring negative results of PCR tests, while ensuring a very high level of security, immutability and integrity of all PCR test results.
- It guarantees, for each patient, the chronological traceability of his results of the PCR tests carried out previously, while ensuring secure access control. Therefore, it allows a very reliable management of the PCR test result documents.
- It is also implemented to process the results of another type of COVID-19 test such as the Immunochromatography test (see section II-A2).

A. Architecture Prototype

We have developed a prototype of our architecture based on the use of the Ethereum public blockchain and smart-contracts (see section II-B2). Our prototype needs a graphical and user-friendly interface to allow data manipulation. This interface must communicate with the core of the blockchain that allows the creation of the blocks and their diffusion (see section III-B). In our prototype, we identify three actors (see Fig. 2):

- The user (person/patient): who wishes to benefit from a service requiring the presentation of a negative COVID-19 test result.
- The laboratory: that performs the COVID-19 tests and guarantees their validity.
- The organization: it is the entity (airport, cinema, shopping center, etc.) that aims to ensure that all participants are not infected with COVID-19.

In our proposed prototype, we consider two main use cases "PCR Tests" and "Immunochromatography Tests":

- **Use Case 1 "PCR Tests"**: it aims to add and/or read information related to the PCR test results of a person. The included data are: *Date of the test, Expiration date (by default 72 hours), Result of the test (Negative or Positive), Name of the laboratory, Country of the laboratory, Address of the laboratory, Identifier of the person (passport number, security social number, etc.).*
- **Use Case 2 "Immunochromatography Tests":** it aims to add and/or read information related to the immunity system of a person. The included data are: *Date of the test, Name of the laboratory, Country of the laboratory, Address of the laboratory, Identifier of the person, IgM (Negative or Positive), IgG (Negative or Positive).*

After performing a PCR test or an Immunochromatography test, the laboratory and from the graphical interface creates a block containing all the data specific to the test, where only the eligible organization and the user that can obtain the data encapsulated in this block. The eligible organization that wishes to access the data must establish a smart-contract with the laboratory. The primary key of this smart-contract is the person's identifier communicated by the person himself. Fig. 2 shows the flow of exchanges between the three actors.

B. Prototype Software Components

Several software components need to be integrated together in order to provide an end to end prototype. Our prototype is divided into 3 main components (see Fig. 3): off-chain component, on-chain component and integration component. We describe these components as follows:

- Off-Chain Component (Graphical Interface): it is developed through HTML and CSS languages. Three main pages are ensured via this interface:

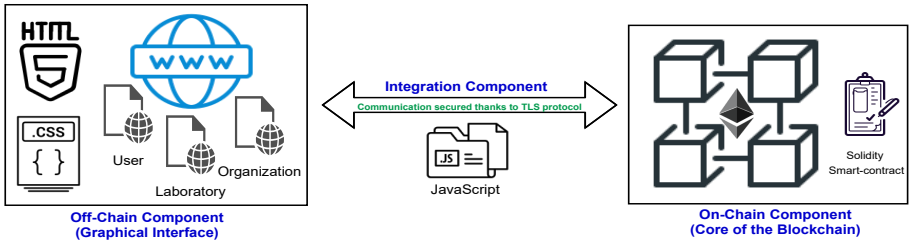

Fig. 3. Prototype Software Components

– User (person/patient): it allows the user to read only the data corresponding to his specific COVID-19 test.
– Laboratory: it allows the laboratory to add the results of COVID-19 tests by creating a new block in the blockchain. It also allows the laboratory to read the data corresponding to a specific test.
– Organization: it allows the organization to read the result of a COVID-19 test for a user after authenticating him thanks to his identifier.

The connection to each page is secured with a login and password, so only eligible parties can access these pages.

- On-Chain Component (Core of the Blockchain): it allows to create blocks in the case of adding the results of COVID-19 tests and also to communicate them between the parties involved (user, laboratory and organization). It is implemented via smart-contracts "solidity language on the Ethereum blockchain [25]" (see section II-B2) . It is the main skeleton of our prototype.
- Integration Component: this component ensures a secure connection, thanks to TLS protocol, between the core of the blockchain and the graphical interface. It is developed through JavaScript language and allows to communicate the values entered on the graphical interface with the core of the blockchain. Two main functions can be performed: get to read and set to write.

C. On-Chain Component (Core of the Blockchain)

we have used multiple smart-contracts in our application for more clarity of the code, organization and classification of the required data. We have also used inheritance to combine our Patient, Labs and Organizations contracts into one main contract, whose basic functionality is to set, edit and get the test results for each patient.

As illustrated in Fig-4, we defined for the Patient contract a structure that contains the username and a Boolean value to indicate whether this patient's id exists or not. We also defined two mappings: "Patients" that maps the hashed id to the user's information and "patientByAddr" that maps the user's address (device's public key) to the hashed id, and an array "patientsList" that contains the hashed ids of all the patients registered on this Blockchain. The function "setPatient" is called upon signing up to set the information of the patient.

As illustrated in Fig-5, the Lab contract contains a structure with all the details of a lab. It also has three mappings: "isLab" to indicate whether an address corresponds to a lab or not, "labInfo" that maps the lab's id to its details, and "labByAddr" to map the different addresses of a lab to its id. The function "setLab" sets the information of a lab when first signing up. "getLabId" returns the id of this lab if it is registered on the device calling the function (returns 0 otherwise). This is used upon logging in such that if the id returned is 0, then "setLabId " is called to set the id to the currently used device's address.

```
pragma solidity ^0.5.0;

contract Patient
{

struct PatientInfo
{
string username;
bool exist;
}

mapping(uint256=> PatientInfo) public Patients;
mapping(address=>uint256) public patientByAddr;
uint256[] patientsList;


function setPatient(string memory _patientid, string memory _username) public
{
uint256 id = uint256(keccak256(abi.encodePacked(_patientid)));
patientsList.push(id);
Patients[id].exist = true;
Patients[id].username = _username;
patientByAddr[tx.origin] = id;
}
}
```

Fig. 4. Patient Smart-Contract

```
pragma solidity ^0.5.0;

contract Lab
{
struct labDetails
{
string email;
string name;
string country;
string location;
}

mapping(address=>bool) public isLab;
mapping(uint=>labDetails) public labInfo;
mapping(address=>uint) public labByAddr;

function setLab(string memory _email, string memory _name, string memory
_country, string memory _location, uint _labId) public
{
labInfo[_labId].email=_email;
labInfo[_labId].name=_name;
labInfo[_labId].country=_country;
labInfo[_labId].location=_location;
}

function setLabId(uint _labId) public
{
isLab[tx.origin] = true;
labByAddr[tx.origin] = _labId;
}

function getLabId() view external returns(uint id)
{
id = labByAddr[tx.origin];
}
}
```

Fig. 5. Lab Smart-Contract

As illustrated in Fig-6, Organization contract is used to register a certain organization on our network. It has only one mapping from address to the organization's info, and a function to set its info upon signing up. No other functions or mappings are required since organizations have no special access; they can only get the patient's test results.

Our Main contract inherits all three contracts. We developed two functions: "setPCRresults" and "setSerum" to set the results' details, and can only be accessed by labs and only if the patient is registered on the network. We developed also two functions "getAllPCR" and "getAllSerum" that allow labs

to return a list of ids for patients that have been tested in the lab calling each function. Then the front-end code can take this array and call the "getPCRresult" and "getSerumResult" in a loop, which in turn returns all results for tests done in this lab. That being said, the getters of the results take into consideration the sender of the function, and set the id of the patient accordingly: in case the patient is calling, the id is automatically set to this patient's id depending on the address; in case the lab is calling, the id is set to the _patientId given as an argument, but converted to integer type (the argument is the patient's hashed id given as string); otherwise (in case of an organization), searching for a patient's id hashes the given value and uses it as id of the test results to be returned.

```
pragma solidity ^0.5.0;

contract Organization
{
struct OrganizationDetails
{
string name;
string country;
string location;
}

mapping(address=>OrganizationDetails) organizationInfo;


function setOrganization(string memory _name,string memory _country,string memory
_location) public
{
organizationInfo[msg.sender].name=_name;
organizationInfo[msg.sender].country=_country;
organizationInfo[msg.sender].location=_location;

}
}
```

Fig. 6. Organisation Smart-Contract

IV. Conclusion and Future Work

In this paper, we proposed a blockchain-based decentralized trust architecture that aims to guarantee the integrity, immutability and traceability of COVID-19 test results. Our proposal also aims to ensure the interconnection between several organizations (airports, medical laboratories, cinemas, etc.) in order to access COVID-19 test results in a secure and decentralized manner. For future work, we aim to extend this paper by improving our smart-contracts and our prototype. In addition, we aim to study and develop a solution for the third case study which is "The vaccination".

References

[1] M. V. Kiang, E. T. Chin, B. Q. Huynh, L. A. Chapman, I. Rodríguez-Barraquer, B. Greenhouse, G. W. Rutherford, K. Bibbins-Domingo, D. Havlir, S. Basu *et al.*, "Routine asymptomatic testing strategies for airline travel during the covid-19 pandemic: a simulation study," *The Lancet Infectious Diseases*, 2021.

[2] P. Munoz, B. Vincent, C. Domergue, V. Gissinger, S. Guillot, Y. Halbwachs, and V. Janillon, "Lockdown during covid-19 pandemic: Impact on road traffic noise and on the perception of sound environment in france," *Noise Mapping*, vol. 7, no. 1, pp. 287–302, 2020.

[3] C. Long, H. Xu, Q. Shen, X. Zhang, B. Fan, C. Wang, B. Zeng, Z. Li, X. Li, and H. Li, "Diagnosis of the coronavirus disease (covid-19): rrt-pcr or ct?" *European journal of radiology*, vol. 126, p. 108961, 2020.

[4] "Covid-19. un trafic de faux certificats de tests négatifs démantelé à l'aéroport de roissy," *https://www.ouest-france.fr/sante/virus/coronavirus/covid-19-un-trafic-de-faux-certificats-de-tests-negatifs-demantele-a-l-aeroport-de-roissy-7041748*, last connection (19/06/2021).

[5] G. A. Salg, M. K. Ganten, M. Baumhauer, C. P. Heussel, and J. Kleesiek, "A globally available covid-19-template for clinical imaging studies," *medRxiv*, 2020.

[6] C. Moreau, "Faut-il faire un test pcr même si l'on est vacciné contre le covid pour voyager ?" *https://www.geo.fr/voyage/vacances-en-europe-faut-il-faire-un-test-pcr-meme-si-lon-est-vaccine-contre-le-covid-19-204934*, last connection (19/06/2021).

[7] "Sars-cov-2 (covid-19) : Test rapide igg/igm pour le diagnostic," *https://www.clinisciences.com/lire/newsletter-26/sars-cov-2-covid-19-test-rapide-2264.html*, last connection (19/06/2021).

[8] L. Lan, D. Xu, G. Ye, C. Xia, S. Wang, Y. Li, and H. Xu, "Positive rt-pcr test results in patients recovered from covid-19," *Jama*, vol. 323, no. 15, pp. 1502–1503, 2020.

[9] Q.-X. Long, B.-Z. Liu, H.-J. Deng, G.-C. Wu, K. Deng, Y.-K. Chen, P. Liao, J.-F. Qiu, Y. Lin, X.-F. Cai *et al.*, "Antibody responses to sars-cov-2 in patients with covid-19," *Nature medicine*, vol. 26, no. 6, pp. 845–848, 2020.

[10] I. Cassaniti, F. Novazzi, F. Giardina, F. Salinaro, M. Sachs, S. Perlini, R. Bruno, F. Mojoli, F. Baldanti *et al.*, "Performance of vivadiag covid-19 igm/igg rapid test is inadequate for diagnosis of covid-19 in acute patients referring to emergency room department," *Journal of medical virology*, 2020.

[11] M. Koutli, N. Theologou, A. Tryferidis, D. Tzovaras, A. Kagkini, D. Zandes, K. Karkaletsis, K. Kaggelides, J. A. Miralles, V. Oravec *et al.*, "Secure iot e-health applications using vicinity framework and gdpr guidelines," *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 263–270, 2019.

[12] S. Sengupta and S. S. Bhunia, "Secure data management in cloudlet assisted iot enabled e-health framework in smart city," *IEEE Sensors Journal*, vol. 20, no. 16, pp. 9581–9588, 2020.

[13] M. F. Ayub, K. Mahmood, S. Kumari, A. K. Sangaiah *et al.*, "Lightweight authentication protocol for e-health clouds in iot based applications through 5g technology," *Digital Communications and Networks*, 2020.

[14] D. Georgiou and C. Lambrinoudakis, "Cloud computing framework for e-health security requirements and security policy rules case study: A european cloud-based health system," *International Conference on Trust and Privacy in Digital Business*, pp. 17–31, 2020.

[15] N. El Madhoun, J. Hatin, and E. Bertin, "A decision tree for building it applications," *Annals of Telecommunications*, vol. 76, no. 3, pp. 131–144, 2021.

[16] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," *2018 27th international conference on computer communication and networks (ICCCN)*, pp. 1–11, 2018.

[17] D. Maldonado-Ruiz, J. Torres, N. El Madhoun, and M. Badra, "An innovative and decentralized identity framework based on blockchain technology," *11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–8, 2021.

[18] N. El Madhoun, J. Hatin, and E. Bertin, "Going beyond the blockchain hype: In which cases are blockchains useful for it applications?" *2019 3rd Cyber Security in Networking Conference (CSNet)*, pp. 21–27, 2019.

[19] D. Maldonado-Ruiz, J. Torres, and N. El Madhoun, "3bi-ecc: a decentralized identity framework based on blockchain technology and elliptic curve cryptography," *2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 45–46, 2020.

[20] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

[21] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe, and S. Chen, "Public and private blockchain in construction business process and information integration," *Automation in Construction*, vol. 118, p. 103276, 2020.

[22] J. Hatin, E. Bertin, B. Hemery, and N. El Madhoun, "Welcome to the jungle: A reference model for blockchain, dlt and smart-contracts," *Tokenomics 2020 on Blockchain Economics, Security & Protocols (2nd International Conference)*, 2020.

[23] E. Hildenbrandt, M. Saxena, X. Zhu, N. Rodrigues, P. Daian, D. Guth, and G. Rosu, "Kevm: A complete semantics of the ethereum virtual machine," 2017.

[24] J. Pons, "La mise en œuvre de la blockchain et des smart contracts par les industries culturelles," *Annales des mines-réalités industrielles*, no. 3, pp. 81–90, 2017.

[25] R. Modi, "Solidity programming essentials: A beginner's guide to build smart contracts for ethereum and blockchain," *Packt Publishing Ltd*, 2018.