Digital Forensics and Privacy-By-Design: Example in a Blockchain-Based Dynamic Navigation System

David Billard[1] and Baptiste Bartolomei[2]

[1] Geneva School of Business Administration, HES-SO, Geneva, Switzerland
david.billard@hesge.ch
[2] Geneva School of Business Administration, HES-SO, Geneva, Switzerland
baptiste.bartolomei@hesge.ch

Abstract. This research presents an experimental model and prototype to exploit digital evidence in Internet of Things (IoT). The novelty of this research is to consider new data privacy mechanisms that should be implemented in IoT, in compliance with the GDPR regulation, and their impact on digital forensic processes. The testbed is an innovative project for car navigation [1] [2], GDPR compatible, which offers users the possibility to submit their GPS position into a blockchain for obtaining road traffic information and alternative paths. The vehicles are communicating among themselves through IoTs and circumvent the use of third-party services. We propose a solution for forensic investigations of such a service by building a solid case thanks to the non-repudiable, immutable, identifiable as current and authentic properties of data logged into the blockchain. This solution applies to criminal and insurance cases, where law enforcement and individuals need to prove their claims.

Keywords: Forensics, IoT, Blockchain, Privacy, Insurance, Hyperledger Fabric, proximity storage.

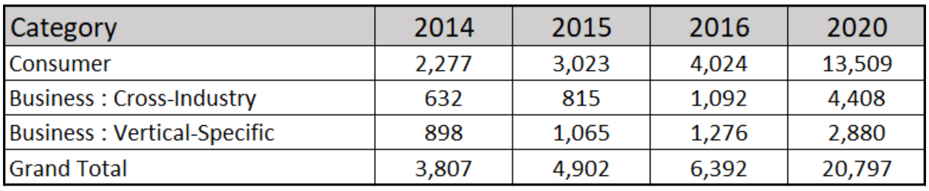
1 Introduction

Internet of Things (IoT) is an ongoing technological revolution, which enables small devices to act as intelligent objects thanks to their sensors and tends to make life easier and more dynamic [3]. The model behind IoT is often a sensor (or set of sensors) submitting data to a service provider which turns data into meaningful information, transmitted to the user's phone or dedicated device. IoT may also be active and can act on its environment.

While some service providers tend to use the data of their clients to produce augmented services by using AI technology or simple algorithms, we witness a contradictory use of data. On the one hand, personal data might be used unfairly by some companies and exposed in the process. On the other hand, data that can be useful in forensic cases remain out of reach to investigators (law enforcement) or users (for their own defense).

If we take a broader picture, nowadays IoT is composed of millions of machines and objects such as smart cars, smart watches, smart cameras, smart refrigerators or smart coffee makers. IoT is used in fields as different as e-health, smart cities, home automation, social fields and the quantified-self which generate huge amounts of data. This number increases steadily and in 2020, more than 20 billion devices will be connected to the Internet [3]. Table I shows the number of IoT devices from 2014 to 2020, classified by category [4]. This development will bring a certain comfort in our daily life but will also create privacy problems.

Table 1. Number of IoT by category (by million)



Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business : Cross-Industry	632	815	1,092	4,408
Business : Vertical-Specific	898	1,065	1,276	2,880
Grand Total	3,807	4,902	6,392	20,797

Unfortunately, privacy problems often lead to security problem: every technology is exposed to cybercriminality because some of this technology (IoT) is not designed with privacy in mind. And it is also true the other way around: security flaws jeopardize privacy and even safety.

According to MELANI’s semi-annual report concerning IoT [5], different malwares may take over control of IoT’s vulnerable devices by creating armies of zombies launching attacks to paralyze Internet service providers like Dyn in 2016 [6].

Last year, the US Food and Drug Administration (FDA) issued a warning concerning series of pacemakers (a device that sends electrical impulses to the heart in order to regulate its rates) which are vulnerable to hackers. That means in fact that users of the system may be exposed to suffering or death if the system becomes the target of a hacker who may be able to control the pacemaker [7]. This risk was unacceptable, so the FDA called back 464,000 pacemakers.

These examples demonstrate why IoT must solve three categories of problems: security, confidentiality and trust.

The project presented in this paper focuses on confidentiality and trust: the solution does not compromise data privacy by avoiding the use of third-party services but in the same time allows for a voluntarily and spontaneous release of data for forensic purposes. In addition, the data collected by our smart car’s solution offers the possibility to better understand the environment of a crime scene.

Whereas security is a much active research field for IoT, confidentiality and trust are quite absent from contemporary researches in IoT model. By using local, or proximity, storage and processing, we overcome the need of data being collected by IoT providers. These providers deal with the privacy of users for personal, commercial or other purposes [8] even though the new General Data Protection Regulation (GDPR), which became effective March 2018, reinforces the protection of the user’s data [9].

As a matter of fact, data collected by IoT providers are used by providers for conducting their own business and are seldom readily available for law enforcement forensic purposes. By offering a proximity storage and processing, users have a better hold on their own data.

We propose such a privacy-protecting solution in the framework of an innovative navigation project, which offers users the possibility to submit their GPS position for obtaining road traffic information and alternative paths, using a blockchain technology solution.

The blockchain is an information storage and transmission technology, transparent, secure, and functioning without a central control organ [10]. The blockchain provides the *non-repudiable*, *immutable*, *identifiable as current* and *authentic* properties of data logged. In addition, the blockchain helps in resolving the issues associated with the interchange of information inside the network.

The HACIT project [1] [2] therefore proposes to rely on a distributed system of IoT to supply a higher-level service to the final user. Instead of feeding a central system with data collected at the IoT level, an IoT is able to collect partial knowledge from other IoTs in the vicinity and provides the best possible service to the user. The HACIT project also evokes a solution for gathering forensic policies that may reveal useful for the police authorities, or the user himself.

This forensic solution is the subject of this paper which is organized as follows: in section 2 we present related work on blockchain and forensics. Then the forensic capabilities are detailed in section 3. Section 4 concludes this work and opens venues for future works.

2 Related and previous work

This paper proposes a better understanding of the forensic capabilities at work in the Hardened and Collaborative Internet of Things project (HaCIT). It proposes a GPS navigation application using the blockchain technology, which allows users to use the navigation service without compromising privacy. An overview of the project can be found in [1] [2].

This innovative project uses IBM blockchain framework [11] on top of Hyperledger Fabric developed by Linux Foundation [12], which offers an extensive framework for blockchain technology implementation. Hyperledger Fabric (HF) proposes a framework for developing permissioned blockchain technology. Contrary to Bitcoin, access to the blockchain is controlled by an entity called the Membership Service Provider (MSP) [13], which guarantees access for its users and the peers with the help of cryptographic material (certificate and keys) delivered by a certificate authority (CA).

The blockchain includes a ledger of transactions but also a representation of the global state through a key-value database. Access, queries, modifications and Smart Contracts are deemed to use the blockchain rule called Chaincode [14]. This allows efficient querying and modification of the dataset without having to analyze the entire chain of data transactions. In order to set up the project, we used an external device such as Raspberry Pi to delegate the computing and the storage of the peer clients' data. Furthermore, we added the OpenStreetMap files [15], the GraphHopper Java library [16] as well as OSMAnd Android library [17] which are used respectively for the map file, the graph handler and the dynamic navigation UI on Android.

Finally, this innovating approach offers forensic capabilities for our application. Indeed, data is stored at multiple places in proximity of the IoT. Therefore, any legal officer may have access to a navigation path in the immutable ledger without violating user anonymity. The aim of this work is to extend the comprehension of our model and to explore its forensic capabilities [11].

The problem of navigation in Vehicular Ad-Hoc Network (VANET) using only local information has been well studied in recent years. For example, [18] proposes a dynamic routing application and [19] offers a suboptimal offline rerouting solution while addressing the communication problems that might arise in VANET. In addition, [20] provides an anonymous and secure navigation system in VANET.

Although these works satisfy most requirements for security and privacy, they still need to rely on third parties in order to remove the anonymity of vehicle ID. However, all the aforementioned papers use direct communication between vehicles (via Wi-Fi or radio) in a dynamic ad-hoc network. As a result, only partial and local traffic information is shared between moving nodes, as opposed to a system centralizing all traffic information such as Google Map.

To the best of our knowledge, although the security in VANET is a well-researched field [21], no paper takes care of the privacy and forensic capabilities. Indeed, no publication offers a system which allows dynamic rerouting and forensics for the mobile devices using a fully implemented blockchain technology. For instance, the Sharma [22] and Leiding [23] projects use the blockchain technology in VANET. However, they use it for monetary applications such as an automatic smart contract for insurance or tolling and uses Ethereum to host smart contracts.

3 Forensic capabilities

The judiciary inquiries have undergone many changes since the beginning of the 1900s. In fact, traces of fingerprints started being used at this period. The investigators had to adapt to the new traces to make proper use of them. As of 1985, the first use of DNA in the Pitchfork case in the United Kingdom [24] allowed to exclude a suspect.

Following the year 2000, data on mobile phones created a shock in the forensic field, with many new data attached to a user now available for investigations. As a consequence, the judiciary inquiries had to change their methods and processes.

In 2007, the smartphone revolution changed the society and with this change, new data had to be explored again. As a matter of fact, smartphones reveal more on one individual's life than the home computer.

Today, multimedia, artificial intelligent and IoT have brought totally new data to be explored by the investigators. We speak today of Big Data and the three V (Volume, Variety and Velocity) and new dimensions appear like Value and Validity [20].

It is a challenge and a necessity for forensics to manage the volume of these new traces. Everything change quite rapidly and the exponential changes have a strong influence on the functioning of inquiries that are based on new types of data. We are talking about a new magnitude in scale [25].

Furthermore, most data are not always available to law enforcement, due to different country laws, inadequate regulations or absence of treaties.

In this paper, we mainly focus on data present in IoT, and more specifically in our project, which is exploitable in a forensic field as digital evidence.

3.1 HACIT project

The architecture of the proposed application allows every user to have access to the history of transactions and thus enables forensics inquiries.

Each user holds a *UserId* and each transaction of the user is logged into the system through its *UserId*. He is the only one to know his *UserId* and can thus recover the history of his transactions.

Hyperledger Fabric stores a database system (asset, e.g. *RoadAsset*) and a transaction blockchain. Both are permissioned, so anyone with rights has access to these two entities, atomic and immutable. Therefore, anyone with rights may have access to the submitted transaction list. For the time being, our application registers only transactions when there is a traffic jam since the application is initially a dynamic navigation application before being a forensic tool. However, we can easily force the user to regularly submit his speed and therefore reveal his position via the *RoadId*.

3.2 Hurdles on the way

In this section, we present the several barriers that can be considered as impediments to our proposed solution. We show that some solutions exist to overcome most of the difficulties.

Security

First, the evidence collected by IoT devices could be modified or removed due to lack of security, which could make the evidence invalid in court. That is why our solution is based on blockchain technology. It provides confidence since its data is immutable and authenticated. Therefore, the evidence cannot be tampered with.

However, our solution supposes that calculated information is accurate with can be proved wrong is the user has submitted faked information before the incident. The way this is actually achieved is not investigated in this paper.

Authenticity and veracity

Since the data is immutable and authenticated, it is necessary to question the authenticity and veracity of the data stored in the blockchain. Indeed, a corrupt system could submit false transactions. The solution to this problem would be to have the transactions validated by other peers and encourage the users not to cheat. For instance, data can be used for the user's defense in case of a road accident. Of course, it will be always possible for a user to submit false information, so this must be costly for the user and the benefit of submitting correct information should always be much higher than submitting faked ones. In addition, some safe guards must be implemented in the system in the future in order to detect abnormal behavior.

In addition, our blockchain can achieve consensus without computationally expensive proof-of-work, for instance with a Practical Byzantine Fault Tolerance (PBFT) algorithm [26].

Privacy

The last problem is the question about data protection since data are not anonymous but pseudonymous. Anonymous data do not allow to find the identity of the person while the pseudonymous data can potentially allow it. In fact, thanks to patterns, it is possible to find the user's identity. Suppose we know the itinerary of a user; we could check the transactions and find his UserId and discover all the transactions he made.

However, the risk is low since we are using a permissioned blockchain, and users must have permission to read and write in the blockchain. A public blockchain allows everyone to view the transactions, whereas in a permissioned blockchain, a specific permission must be given [27]. Therefore, the number of people with access to the ledger is less than in a public blockchain. Although the risk is lower, the problem remains the same.

From the point of view of Swiss law, it is necessary to protect the data which is pseudonymized which makes it potentially possible to retrieve the personal data of the user [28]. These data are sensitive if they provide information about religious opinions or activities, health, privacy, intimate sphere, race, social assistance, criminal or administrative prosecutions or sanctions. We must therefore pay attention to this information.

The data collected by our system do not directly affect a priori the categories listed above. However, they can be attached to it. Take for instance a person who goes every Sunday morning with his car to a worship center to practice his religion. Thus, the personal data of this user may become sensitive and therefore need a different treatment.

At this stage of the project, we yet don't have total anonymity but only a strong pseudonymity. It is planned to use temporal *UserId*, which means the *UserId* is randomly changed after a predefined period of time. Only the user keeps track of its succession of *UserId* (and the timestamp when it changed).

3.3 Forensic investigation

Each IoT device provides important information that could assist in the investigation process.

Our system brings brand-new digital traces that can be used in the judicial field. The data, which can be given to the investigators, are those that have been sent to the blockchain in transactions like speed of the car, road, traffic jams, etc…

These data may help investigators to understand and reconstitute road accidents. Furthermore, this information may also be used for prevention purposes, since the investigators can recognize the problems of the road and can set up different processes to mitigate the risk of accident.

Investigations concerning car accidents are very complicated and often differ from one canton to the other in Switzerland. Indeed, each police has its own specialist team and its own investigative habits [30]. Our system could help the investigation service in standardizing its procedures by having access to the data stored on the blockchain and using the same method of analysis.

Moreover, real-world application is problematic for the judiciary examiner, especially with respect to the location of data and the heterogeneous nature of IoT devices such as differences in operating and communication systems. Our project provides solutions to these problems but does not solve all of them effectively.

In our case, the data may be used in forensic investigation because it may be connected via a UserId directly to the user.

However, a problem remains: the fact that the data collected is associated to a device and not directly to a user may be problematic to investigators. This can lead to several problems such as the veracity of these data. Indeed, the system can validate that the device (Raspberry Pi) was well on this road (RoadId), at a precise hour (Timestamp) and at a certain speed (Speed), but it cannot validate that the user providing the data to the administration was the user driving the vehicle.

Even with blockchain technology which offers transparency of transactions or with a private key system that could validate the identity of the user, nothing prevents this user from sharing his private key or devices (Raspberry Pi) with another person.

A validation should be added to prove that the person was driving the vehicle. For instance, the identification to the Android application with fingerprints. Of course, other ways to validate the user can be installed. There are therefore several means of proof that can be put in place and prove the identity of the user.

However, this is a common problem in forensic science: the attribution of fact to an individual. Unfortunately, no universal solution exists, in digital forensics or other related disciplines.

3.4 Forensic insurance

Concerning insurance companies, data protection is also to be taken into account. Swiss insurance companies may ask their customer for agreement to implement a system which will harvest personal data on the activities of their customer [31]. The law on data protection in Switzerland [28] and more generally the GDPR in Europe [9] puts a point of honor on the protection of individuals. This is why such follow-ups are only possible with the customer's consent. However, the purpose of collecting and processing these data must be clearly defined and not be used for other purposes than those originally defined in the contract. Insurance companies may therefore use this system.

In a centralized system, insurance companies have access to all the information collected from the user: journeys, speed limits (respected or not), ignored stop signs, addresses, etc. This is a massive intrusion on individual privacy and collected data can serve to other purposes than to verify the validity of insurance claims.

If the centralized system is also owned by the same actor than the medical centralized system storing the health information of the individual, the possibility to use both data is tempting. This case is not entirely fictional, since it is now known that Google has been "*accused of breaking promises to patients, after the company announced it would be moving a healthcarefocused subsidiary, DeepMind Health, into the main arm of the organisation*." [32].

With our decentralized system, data stay within the car IoT, and the other car IoTs that shared traffic information. The data will not be available to the insurance companies until a situation arises and a case is opened. These data are then used by the insurance companies to process the case.

The data that could be used by insurance companies are the same than in the legal field but their use will have a different purpose. This system will benefit insurance companies as much as their customers. In fact, insurance companies will have more information on the cause of an accident and will be able to fight fraud more effectively. For instance, between 2014 and 2016, more than 24 million Swiss Francs of insurance fraud were discovered in Switzerland [33]. Conversely, customers could take advantage by paying lower premiums.

Our system allows insurance companies to have a follow-up of their clients like travel, speed, distance, etc... This follow-up may provide useful data, which will help to understand how users behave just prior to an accident. Indeed, the insurance must protect the victims and predict the risks involved. These risks may be more or less predictable depending on the data collected. Our system collects many data that allow insurance companies to anticipate risks and avoid them as much as possible.

Insurance companies are already in the field of IoT. As an example, the life insurance giant John Hancock asked customers to wear an electronic bracelet for being able to follow their activity. In that manner, John Hancock will have information on their global health and will modulate premiums accordingly [34]. This insurance may also favor sporting activities such as running that allows its customer to take advantage of lower premiums. Of course, the user should be free to accept or decline the use of such devices.

Finally, our system may profit to the customer. On many occasions, it is very difficult for an individual to prove his good faith, that he was not at fault or did not violate the law, for example by speeding.

4 Conclusion and future works

In this paper, we have presented the digital forensic capabilities of an experimental project by exploiting digital evidence in Internet of Things (IoT). The novelty of this research is to consider new data privacy mechanisms that should be implemented in IoT, following the GDPR regulation, and their impact on digital forensic processes.

The testbed is an innovative project for car navigation where vehicles are communicating among themselves through IoTs in order to determine the best route. The project circumvents the use of third-party services by relying only on inter-vehicle exchanges and submission of GPS position into a proximity blockchain for obtaining road traffic information and alternative paths.

Data privacy is well respected in this model, which is GDPR compatible, but poses new challenges for digital forensics. This paper presents the difficulties of conducting a forensic investigation and the solutions implemented in the model. The explored forensic scenarii are traffic police and insurance.

Our solution provides forensic investigations with a solid case thanks to the *non-repudiable*, *immutable*, *identifiable as current* and *authentic* properties of data logged into the blockchain. These data can be used indiscriminately by law enforcement agencies, insurance companies and individuals who need to prove their claims. The solution respects the privacy of the user's data since law enforcement agencies and insurance companies have access to the basic set of data needed to process a case, but not the whole life of the user.

Future works on health care data privacy are currently envisioned. The purpose of these works is to allow health care while restricting access to health data for non-medical bodies.

References

1. K. Decoster and D. Billard, Eds., “HACIT: a privacy preserving and low cost solution for dynamic navigation and Forensics in VANET,” Proc. 4th Int. Conf. Veh. Technol. Intell. Transp. Syst. VEHITS 2018, 2018.
2. D. Billard and K. Decoster, “HACIT2: a privacy preserving, region based and blockchain application for dynamic navigation and Forensics in VANET,” presented at the 10th EAI International Conference on Ad Hoc Networks, Cairns, Australia, 2018.
3. Gartner, “Leading the IoT e-Book.” Available: https://www.gartner.com/en/publications/iot-business. [Accessed: 31-Oct-2018].
4. J. Rioche, “L'enjeu de la sécurité des objets connectés,” I2D – Inf. Données Doc., vol. me 54, no. 3, pp. 64–65, Oct. 2017.

5. R. and A. C. for I. A. MELANI, “Data leaks, crimeware and attacks on industrial control systems – topics in the MELANI semi-annual report.” Available: https://www.melani.admin.ch/. [Accessed: 31-Oct-2018].
6. “The DDoS Attack Against Dyn One Year Later.” [Online]. Available: https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attackagainst-dyn-one-year-later/#44f2b8311ae9. [Accessed: 31-Oct-2018].
7. C. for D. and R. Health, “Safety Communications - Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott’s (formerly St. Jude Medical’s) Implantable Cardiac Pacemakers: FDA Safety Communication.”.
8. A. R. Beresford and F. Stajano, “Mix zones: user privacy in locationaware services,” in IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second, 2004, pp. 127–131.
9. P. O. of the E. Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance),” 27-Apr-2016.
10. D. Guegan, “The Digital World: II – Alternatives to the Bitcoin Blockchain?,” Jun. 2018.
11. IBM, “IBM Blockchain Platform.,” 2017. [Online]. Available: https://ibm-blockchain.github.io/develop/. [Accessed: 04-Oct-2018].
12. Linux Foundation, “HyperLedger Fabric docs,” 2016. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release/. [Accessed: 26-Sep-2018].
13. hyperledger-fabric, “Membership Service Providers (MSP) — hyperledger-fabricdocs master documentation,” 2018. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.3/msp.html. [Accessed: 31-Oct-2018].
14. hyperledger-fabric, “Chaincode Tutorials - hyperledger-fabricdocs master documentation,” 2018. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.3/chaincode.html. [Accessed: 31-Oct-2018].
15. OpenStreetMap, “OpenStreetMap,” OpenStreetMap, 2018. [Online]. Available: https://www.openstreetmap.org/. [Accessed: 31-Oct-2018].
16. GraphHopper, “GraphHopper Directions API with Route Optimization,” GraphHopper Directions API, 2018. [Online]. Available: https://www.graphhopper.com/. [Accessed: 31-Oct-2018].
17. OsmAnd, “OsmAnd - Offline Mobile Maps and Navigation,” 2018. [Online]. Available: https://osmand.net/. [Accessed: 31-Oct-2018].
18. “On the Effectiveness of an Opportunistic Traffic Management System for Vehicular Networks - IEEE Journals & Magazine.” https://ieeexplore.ieee.org/document/5970119. [Accessed: 15-Nov-2018].
19. M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, “Scalable reactive vehicle-to-vehicle congestion avoidance mechanism,” in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 2015, pp. 943–948.
20. L. Wang, G. Liu, and L. Sun, “A Secure and Privacy-Preserving Navigation Scheme Using Spatial Crowdsourcing in Fog Based VANETs,” Sensors, vol. 17, no. 4, Mar. 2017.
21. M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J Comput Secur, vol. 15, no. 1, pp. 39–68, Jan. 2007.
22. “Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City,” J. Inf. Process. Syst., 2017.
23. B. Leiding, P. Memarmoshrefi, and D. Hogrefe, “Self-managed and Blockchain-based Vehicular Ad-hoc Networks,” in Proceedings of the 2016 ACM International Joint Conference

on Pervasive and Ubiquitous Computing: Adjunct, New York, NY, USA, 2016, pp. 137–140.

24. J. D. Aronson, “DNA fingerprinting on trial: the dramatic early history of a new forensic technique,” Endeavour, vol. 29, no. 3, pp. 126–131, Sep. 2005.
25. D. A. Stoney and P. L. Stoney, “Critical review of forensic trace evidence analysis and the need for a new approach,” Forensic Sci. Int., vol. 251, pp. 159–170, Jun. 2015.
26. J. Bahsoun, R. Guerraoui, and A. Shoker, “Making BFT Protocols Really Adaptive,” in 2015 IEEE International Parallel and Distributed Processing Symposium, 2015, pp. 904–913.
27. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018.
28. “CC 235.1 Federal Act of 19 June 1992 on Data Protection (FADP),” 19-Jun-1992. Available: https://www.admin.ch/opc/en/classifiedcompilation/19920153/index.html. [Accessed: 31-Oct-2018].
29. hyperledger-fabric, “MSP Implementation with Identity Mixer — hyperledger-fabricdocs master documentation,” 2018. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html.
30. S. Hafsi, “L’exploitation des traces dans les accidents de la circulation,” University of Lausanne, Lausanne.
31. “RS 221.229.1 Loi fédérale du 2 avril 1908 sur le contrat d’assurance (Loi sur le contrat d’assurance, LCA),” 02-Apr-1908. Available: https://www.admin.ch/opc/fr/classifiedcompilation/19080008/index.html. [Accessed: 31-Oct-2018].
32. A. Hern, “Google ‘betrays patient trust’ with DeepMind Health move,” The Guardian, 14-Nov-2018.
33. ASA, “Versements évités de 24 millions de francs d’indemnités injustifiés,” ASA, 2018. Available: https://www.svv.ch/fr/newsroom/versements-evites-de-24-millions-de-francs-dindemnites-injustifies.[Accessed: 31-Oct-2018].
34. D. Gershgorn, “A life insurance giant is asking customers to wear health trackers,” Quartz. [Online]. Available: https://qz.com/1396035/lifeinsurance-giant-john-hancock-is-asking-customers-to-wear-healthtrackers/. [Accessed: 31-Oct-2018].