Blockchain as a privacy enabler: an odometer fraud prevention system

Blockchain as a Privacy Enabler: An Odometer Fraud Prevention System

Mathieu Chanson
ETH Zurich
8092 Zurich, Switzerland
mchanson@ethz.ch

Elgar Fleisch
ETH Zurich
8092 Zurich, Switzerland
University of St. Gallen
9000 St. Gallen, Switzerland
efleisch@ethz.ch

Andreas Bogner
ETH Zurich
8092 Zurich, Switzerland
abogner@ethz.ch

Felix Wortmann
University of St. Gallen
9000 St. Gallen, Switzerland
felix.wortmann@unisg.ch

UbiComp/ISWC '17, Adjunct, September 11–15, 2017, Maui, HI, USA
ACM 978-1-4503-5190-4/17/09.
https://doi.org/10.1145/3123024.3123078

Abstract
Giving people ownership of the data they produce becomes more and more important in times of ever-growing capabilities to collect and analyze data of individuals. In light of this challenge, we show how blockchain technology can enable privacy by presenting an odometer fraud prevention system. It records mileage and GPS data of cars and secures that on the blockchain, which strongly hinders odometer fraud. Our users own and control their data while at the same time data integrity is ensured. This facilitates the certification of that data. We discuss the advantages of this approach compared to current systems and also highlight limitations of our architecture and the use of blockchain technology.

Author Keywords
Blockchain; Ethereum; Privacy; Data Ownership

ACM Classification Keywords
K.4.1 [Public Policy Issues]: Privacy

Introduction
With ever-rising amounts of data being gathered on persons and increasing capability to analyze this mass of information it becomes more and more important to give people ownership of their data [2]. We chose the virulent problem of odometer fraud as a showcase of how blockchain technology can be used to achieve this.

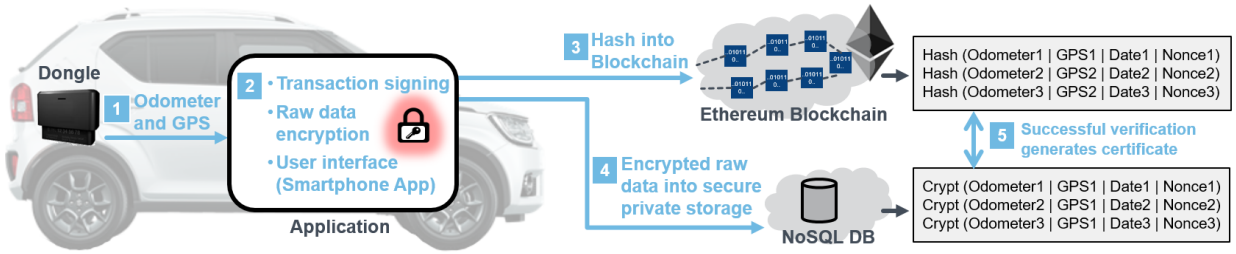

Figure 1: Architecture of the prototype presented

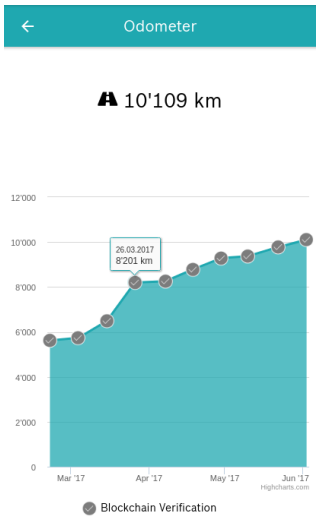

Figure 2: A screenshot of the smartphone app: Three months of the odometer history of a car is shown. All the blockchain entries are indicated by a circle with a tick.

Odometer fraud is a huge problem in many countries, for example Germany where around a third of resold cars are affected, leading to an annual damage of almost 6 billion euros [3]. Typically, the true car mileage is reduced in order to increase the car value on resale. The procedure is extremely simple and can be performed within minutes.

Current systems to fight odometer fraud, like AutoCheck, Carfax or CarJam, have several serious issues, including severe privacy problems. They all publish sensitive data in central databases accessible to the public. With CarFax, for example, knowing merely the Vehicle Identification Number (VIN), often visible on a car's windscreen, one can see at what date a car was brought to which garage, the type of work executed and the mileage at that time. Privacy problems like those prohibit todays systems to be implemented in countries with strict privacy laws, like Germany, as it is not possible to comply with the regulation. Another issue of current systems is the low frequency of data records. New records are only written occasionally, usually if a repair is performed at a garage. The timespan between two records can range from a few months to several years. Especially for new cars the registration frequency is very low, however in that case odometer fraud is most prevalent and lucrative and therefore a detailed monitoring necessary. Furthermore, only one type of odometer fraud can be detected by these systems: The case of mileage reduction in hindsight. However, if a hardware manipulation device is applied which continuously records only a partial amount of the driven distance, these systems fail.

All the problems mentioned before are addressed with our system. The data gathered is only accessible to the user, the registration frequency is high and continuous odometer fraud can be detected. Clearly, there are also limitations of the solution proposed, considering attack vectors on the architecture and regarding the use of blockchain technology. This will be outlined in detail in the discussion.

System Overview

An overview of the prototype architecture is shown in Figure 1. Odometer values are retrieved from the car using a dongle (1) which also records GPS values. This data is sent to the core application (2) running in the car on a laptop. There, a timestamp and a random nonce are added to the dataset. The nonce prohibits the identification of the raw data in the public blockchain by hash guessing. The application hashes the dataset and (3) writes it to the public

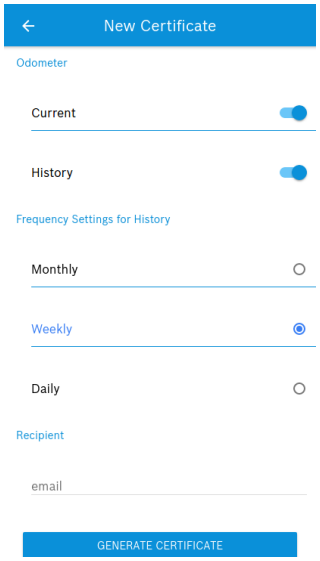

Figure 3: A screenshot of the smartphone app: At the time of the sale of a car the certification process is started. The user can decide on the amount of data to be shared for the creation of the certificate for a potential buyer. Till then no private data of the user has been available to any third party. The certificate can be hosted online and sent via a link to the potential buyer.

Ethereum blockchain [1]. Note that the transaction is signed locally with the private key of the user and only then sent to an Ethereum client in the cloud. The full raw dataset is encrypted locally and then saved in a cloud database (4). Only the holder of the car to which this data belongs can access it, ensuring his privacy the whole time. A smartphone app serves as the user interface and receives data from the core application (2). The certification process (5) is started if a car holder wants to prove his odometer history. The raw data is transmitted to the requesting party which can verify the match of the hashes of the transmitted data with those from the blockchain. This certification process is integrated in our app. This key feature allows the user to gather data privately and share selected parts of it at a later time when he has a direct interest to do so.

Prototype Implementation

Our dongle retrieves the odometer values and the VIN of the car via the on-board diagnostics II (OBD-II) interface, a standardized interface for all cars in the European Union. The dongle also measures the GPS position and sends all the data via bluetooth to the laptop in the car (1). On the laptop a Node.js application is running (2). It uses the Web3 JavaScript Dapp API to sign the SHA256 hashes of the raw data into Ethereum transactions locally and send them via RPC calls to an Ethereum full node in the cloud, which broadcasts the transaction to the Ethereum network (3). The raw data is encrypted in the application using AES and saved in the Amazon dynamoDB which is a NoSQL database (4). The smartphone app communicates with the Node.js application using a REST API. The certificate creation process (5) is integrated in the Node.js application, where the raw data is decrypted and the comparison of the hashes takes place. Once the verification is finished, the certificate is created and can be sent via email to a third party or be published on a web page online.

Discussion

We presented a system that puts users in charge of the data they produce, namely mileage and GPS information, while at the same time enabling them to share it at a later stage with guaranteed data integrity. This implements the idea that people should own their own data, a central pillar of the new deal on data [2]. It also makes our system comply with strict data protection law, for example German data regulation. Furthermore, it enables users to participate in the monetization of their data: In the case of odometer fraud it is expected that a guaranteed odometer history will significantly increase the resale price of a car and a user therefore monetizes the publishing of personal data for an odometer certificate.

In addition to general data privacy issues our system also addresses problems specific to the case of odometer fraud. A crucial improvement comparing to current systems is the increase of the registration frequency. It is on a trip level, instead of months to years, which is especially important for new cars. Another key feature is the cross validation with GPS data. As we see a shift from one-time odometer fraud towards a continuous tampering, it is indispensable to check the plausibility of the recorded mileage readings. Our system achieves that by cross validating the mileage with the GPS values from a peripheral device, the dongle.

The Ethereum blockchain is a cornerstone of our architecture [1], enabling the verification of data integrity without relying on any third party. The immutability of the blockchain guarantees that the hashes remain unchanged and the verification will succeed if the original data has not been modified. The distributed nature assures its service continuity. But the use of blockchain bears also drawbacks. Transaction costs are volatile and difficult to predict in the long term. In the last six months only they have risen from 0.5¢ to 10¢

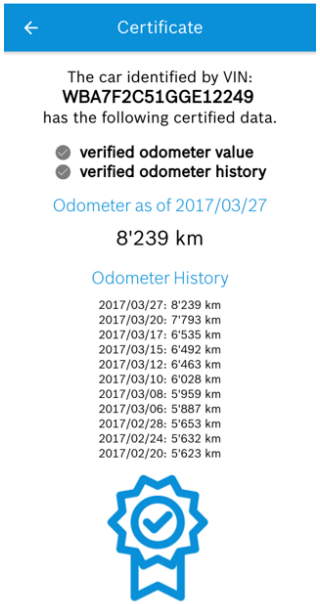

Figure 4: A screenshot of the smartphone app: The issued certificate is shown on the screen as a double check for the user before the certificate link is sent to the requesting party by email.

for a standard transaction. Moreover, enabling the scalability of Ethereum and other blockchains remains an open issue, leaving doubts regarding their suitability for large scale systems. Additionally, being in its infancy, it is uncertain if this technology will persist more reliably than, for example, a government controlled database. These issues could be resolved by replacing the blockchain with a conventional database. However, that would require the users to trust the third party operating the database that the hashes are stored safely and access to them is always guaranteed and this under reasonable conditions.

Besides blockchain related issues several challenges remain. First of all the presented system still features a number of attack vectors. All the data that leaves our application is encrypted or hashed in a signed Ethereum transaction and thus secured. But until the data arrives in our application, it could still be manipulated. The readings from the OBD-II could be tampered using common mileage filtering methods. This is counteracted through cross validation with GPS data. However, adversaries could interfere with the connection of the dongle and the app and introduce tampered data there. An additional challenge is to replace the laptop in the car with a smaller device or let a big part of the app run in the cloud without decreasing the security. This might be achieved by putting the cryptographic part of the app in the dongle itself: Thereby data leaving the dongle could not be tampered anymore and the usability of the system would increase dramatically.

We plan to test our system in the field. The focus is the user interaction with the system, if trust is increased by the use of blockchain technology and if users are sharing more data compared to legacy architectures. Additionally technical questions are of concern, for example if edge cases, like the transport of cars on trains, are detected reliably.

Conclusion

In a world where many parties obtain ever-increasing capabilities to collect and analyze personal data, users should own and control the data they produced. Our system proves with a specific showcase how blockchain technology can enable more privacy and data ownership for end users. Odometer values are stored securely and made verifiable in retrospect by comparison with the blockchain. This enables the holder of a car to prove the accuracy of data in hindsight, without the need of sharing them with anyone continuously nor putting any trust in a third party. Comparing to current fraud detection systems our prototype excels in privacy consciousness, data collection frequency and the ability to detect different types of odometer fraud, as explained in the discussion. The use of blockchain offers many advantages, however a lot of uncertainty remains regarding the future development of the technology. A further improvement of the system could be to move the cryptographic part from the application to the dongle itself.

REFERENCES

1. Vitalik Buterin. 2014. A Next-Generation Smart Contract and Decentralized Application Platform. (2014). `https://github.com/ethereum/wiki/wiki/White-Paper/wiki` (Accessed 11-April-2017).
2. Alex Pentland. 2009. Reality mining of mobile communications: Toward a new deal on data. *The Global Information Technology Report 2008–2009* (2009), 1981.
3. TÜV Rheinland. 2015. Das Problem Tachomanipulation. (2015). `https://www.arvato.com/content/dam/arvato/documents/financial-solutions/PK_Tachomanipulation_T%C3%9CV_Rheinland.pdf` (Accessed 22-May-2017).