CarBlock

A GLOBAL TRANSPORTATION DATA PROTOCOL WITH DECENTRALIZED APPLICATIONS

WHITEPAPER

Version 4.0
Last Update: August 13 2018

Table of Content

Summary

CarBlock is a decentralized blockchain platform and ecosystem that serves the entire automotive and transportation industry. While the internet has enabled the flow of information, Carblock will do the same for data and assets. This increased access to data will enable businesses to make better decisions and stimulate a more efficient operation for them on CarBlock, while also attract individuals, teams, universities and research institutions to join the ecosystem and eventually change the entire automotive and transportation industry.

CarBlock's ecosystem is built based on extensive research and investigation. Based on that information, we work off of the following fundamental principles:

- The ownership and interest of all data should belong to the data provider, in most circumstances, the car owner. First, this is where the regulations are headed (especially in most Western countries), and second, car owners are the foundation of CarBlock's ecosystem and serve as the link between business and data. Our expectation is that Blockchain and its decentralized nature will provide the perfect solution for these scenarios.

- CarBlock will not profit as the middleman in the data marketplace. On the contrary, CarBlock will ensure the free circulation of data and decrease the friction during this process. The purpose of transaction consumption is to merely cover the cost of the system. CarBlock will even subsidize individuals, teams, universities and research institutions with creative capacity if the organization perceives the potential of those offerings to better the ecosystem.

- Data circulation will create a mutually beneficial situation for all participants within CarBlock's ecosystem.

As veterans in the connected car industry, we believe that applications and services built on car data will present a massive, disruptive force in the industry. However to date, the development hasn't reached its full potential yet. The reason why is due to the lack of consensus among data owners, collectors, and demanders, leaving interests that are impossible to share equitably. In the past, data owners couldn't trust the entity to protect their privacy and have no incentives to share it with them, this is the main reason that no one has built this technology. These are the reasons we've created CarBlock to solve data circulation problems in the automotive industry through blockchain technology.

The Disruptive Power of Connected Cars and Connected Car Data

For the purpose of this white paper, we herein define a connected car as a car that is equipped with internet access or outfitted with smart hardware that taps into the internet or wireless LAN and provides benefits to the driver.

The vast majority of auto industry experts concur that connected cars and connected car data will be a disruptive force in the auto industry and its peripheral industries. This chapter highlights the auto industry's major changes and future trends.

How Smart Devices and the Mobile Internet Are Changing the Automotive Industry

Smart devices and the mobile internet have had a major impact on the century-old automotive industry. Not only have they made the collection and analysis of vehicle driving data possible, they have also dramatically changed people's driving behavior with the introduction of various intelligent electronic systems and driving assistance systems.

Accurate Data Modelling To Replace Traditional Data Analysis

"Connectivity will have a more dramatic effect on cars than any other automotive technology in the last century. That's because the car is a great 'data centre' with the potential to collect and share information from a huge range of sources. It will know where you shop, work, when you drive and even what you do on your weekends off. Cars will therefore become much smarter and understand you and respond to you in a way that in the past was considered science fiction."

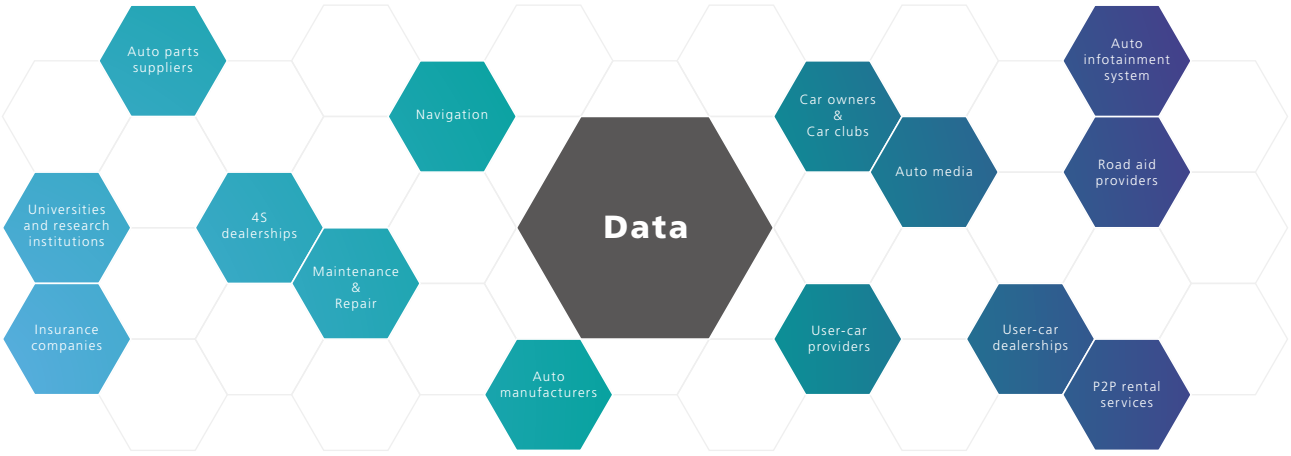
- Tom Rivers, vice president connected car marketing, automotive connectivity specialist Harman

When it comes to vehicle data, traditional data analysis no longer appears adequate. We're currently seeing emerging trends in which connected car data modelling can more accurately represent a vehicle's real profile and therefore serve as a more reliable source of information for making decisions about insurance quotes, vehicle maintenance, and used car transactions.

While the old way of doing business is still very much alive, a company with data modelling capabilities can have a huge competitive advantage over others and thus potentially redefine the automotive landscape. For instance, an insurance company with vehicle driving data could offer a more tailored and competitive package to their customers while maintaining a higher profit margin compared to their competitors. We are seeing early signs of this in North America from a startup called Metromile[2] that is able to offer competitive insurance quotes by allowing its customers to purchase insurance based on their driving mileage. With the continued advancement and adoption of connected car technology, data will undoubtedly become a driving force for the entire transportation industry.

Understanding the Connected Car Ecosystem and Its Potential

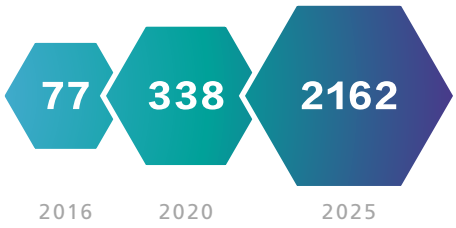
The connected car system is essentially an ecosystem in which each party interacts and collaborates through data. The auto industry is already a mature industry with different parties contributing and consuming data. Data enables the different parties in the ecosystem to form synergies, achieve progress, and make transportation safer and more convenient.



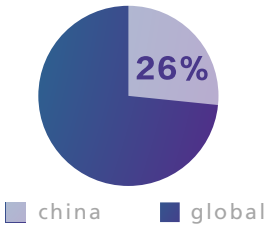
Connected Car Ecosystem

The connected car market holds immense potential. According to Accenture's report[3], the global connected car market will reach $840 billion in 2025 (excluding car manufacturers) with China estimated to take up 26%[4] of that market.

China connected car market size
(unit:billion dollars)

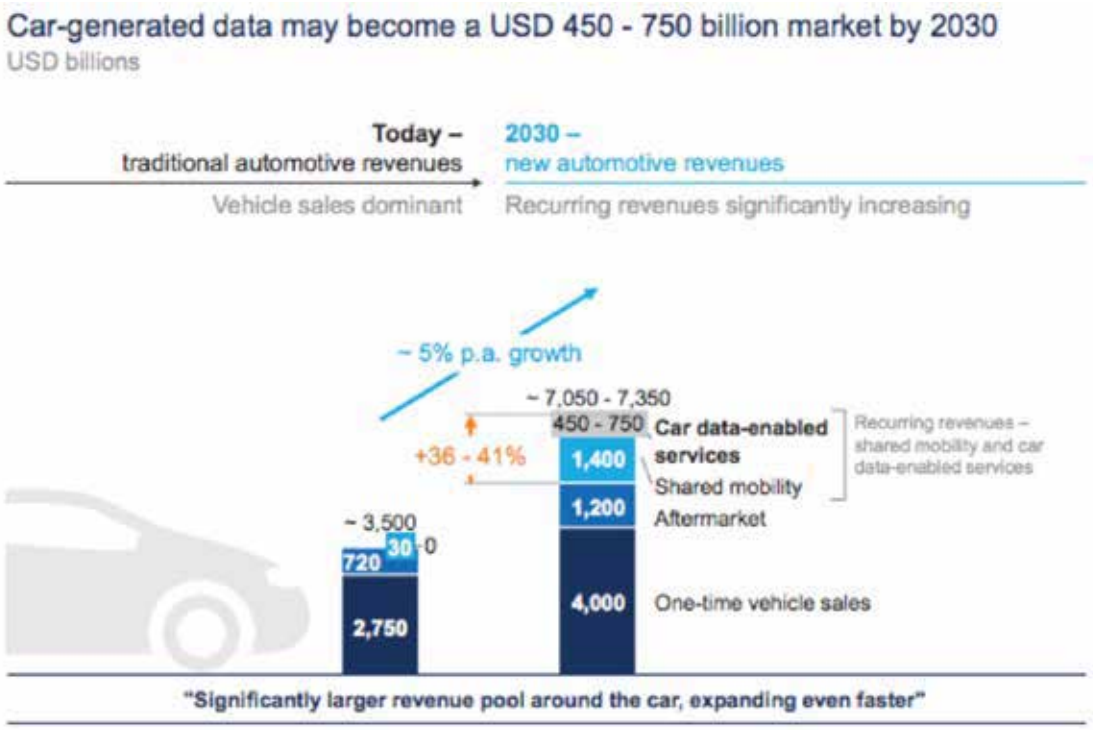


2025 Global connected
car market size



Accenture's report on the connected car market

Another report from Mckinsey shows the car data market will reach to $750 Billion in year 2030.



The 4 Core Data Problems in the Connected Car Ecosystem

While the connected car market is poised for growth, the market is currently fragmented and hindered by the following problems which CarBlock aims to solve with a blockchain solution.

Data Ownership - The Conflict Between Corporate Interest and Data Privacy

Vehicles have enabled people to be more mobile and more free than ever before, so inevitably driving has become a core part of people's daily lives. North Americans are estimated to spend over 20% of their lives in the car. Vehicle and driving data can be used to derive insights about people's lifestyle and preferences and is therefore invaluable. Without advanced data encryption and strict authorization, there is a huge potential threat to people's personal privacy and safety.

Being that the automotive industry is a highly market-driven industry, it's not surprising to hear that companies are facing increasing pressures from consumers to protect their privacy and data. So how can companies protect their users' privacy and regulate data access? This is a key problem that the connected car industry has been trying to solve but with minimal progress, leaving big question marks around the best ways to handle connected car data collection and storage.

The topic of car data ownership has always been very controversial. Almost all car manufacturers have begun to pre-install Telematics Box (T-Box) into vehicles to collect data. Yet, car owners believe that vehicle data is rightfully theirs and is a matter of personal privacy. Consumers are reluctant to trust privacy commitments from car manufacturers and other commercial companies. As a result, there is a clear consumer need for a solution that ensures that the vehicle data belongs to the car owner.

Data Incentives - Data Contributors Receive Zero Benefit

Unquestionably, the rights to use and distribute data should belong to the person who contributes the data. Yet, when we drive, the data we generate often does not belong to us. For instance, the navigation software knows where we are going and pushes relevant ads. Advertisers, in turn, give money to the navigation company. We, as data contributors, do not receive anything in return. This is precisely why the

connected car industry has made little progress; users are not motivated to provide relevant data without proper incentives.

While manufacturers and companies have tried to keep things quiet for fear of losing revenue streams, consumers are becoming increasingly aware of the privacy invasion and are now demanding rights to their personal data.

- In the North America, debates over whether it's right for companies to profit from personal data are all over the media[5].
  https://www.dailynews.com/2017/09/12/equifax-profits-by-selling-your-personal-data/

- In China, people were livid about Alipay's privacy invasion of their annual spending data[6].
  http://tech.sina.com.cn/i/2018-01-11/doc-ifyqnick7174902.shtml

We believe that companies' ability to profit freely from user data will dramatically change in next two to three years and CarBlock will help to significantly speed up that process.

Data Value - Desensitised data Vs User-specific data

Although car data possesses huge value, yet due to privacy regulation, companies can only use desensitised data for application development. Since desensitised data can only be used to form some generalized conclusion, but not reflect drivers' behavior, it's very hard to truly promote industry progress based on it.

On the other side, with desensitised data only counts about 2.5% of all data collected, the other 97.5% of the data, which is a way more valuable set of user-specific data, hasn't been properly used and just kept idle, there's no way for the industry to truly take off from a data-driven perspective.

Data Allocation - Data for the Creation of Transportation Applications Is Nonexistent

When Waymo (formerly Google's autonomous vehicle project) expanded its fleet to 100 vehicles in December 2016, it reported collecting 3 million miles of data[7] in May 2017. Now, the company collects data from hundreds of vehicles each day. Managing

such a large fleet with road tests in real conditions requires significant investment, which makes getting valuable data a game only giant companies can afford to play. While there is vehicle data available to small companies, the data is extremely scattered and insufficient in scale to provide any significant value for building transportation applications.

In fact, the lack of access to vehicle data has prevented individuals, teams, universities, and research institutes with innovative ideas from making headway into building useful future transportation applications.

The current boon in the mobile internet ecosystem exemplifies what can be achieved when a community of individual developers and startups have the resources they need to develop applications for users around the world. The same thing can happen with the connected car industry when an open platform such as CarBlock is created to enable simple, cost-effective, and safe circulation of real-world transportation data. By doing so, people in the ecosystem can develop their ideas and foster breakthroughs in the connected car industry.

The viability of connected car applications ultimately relies on an infrastructure that can support the safe and automated circulation of massive amounts of vehicle data.

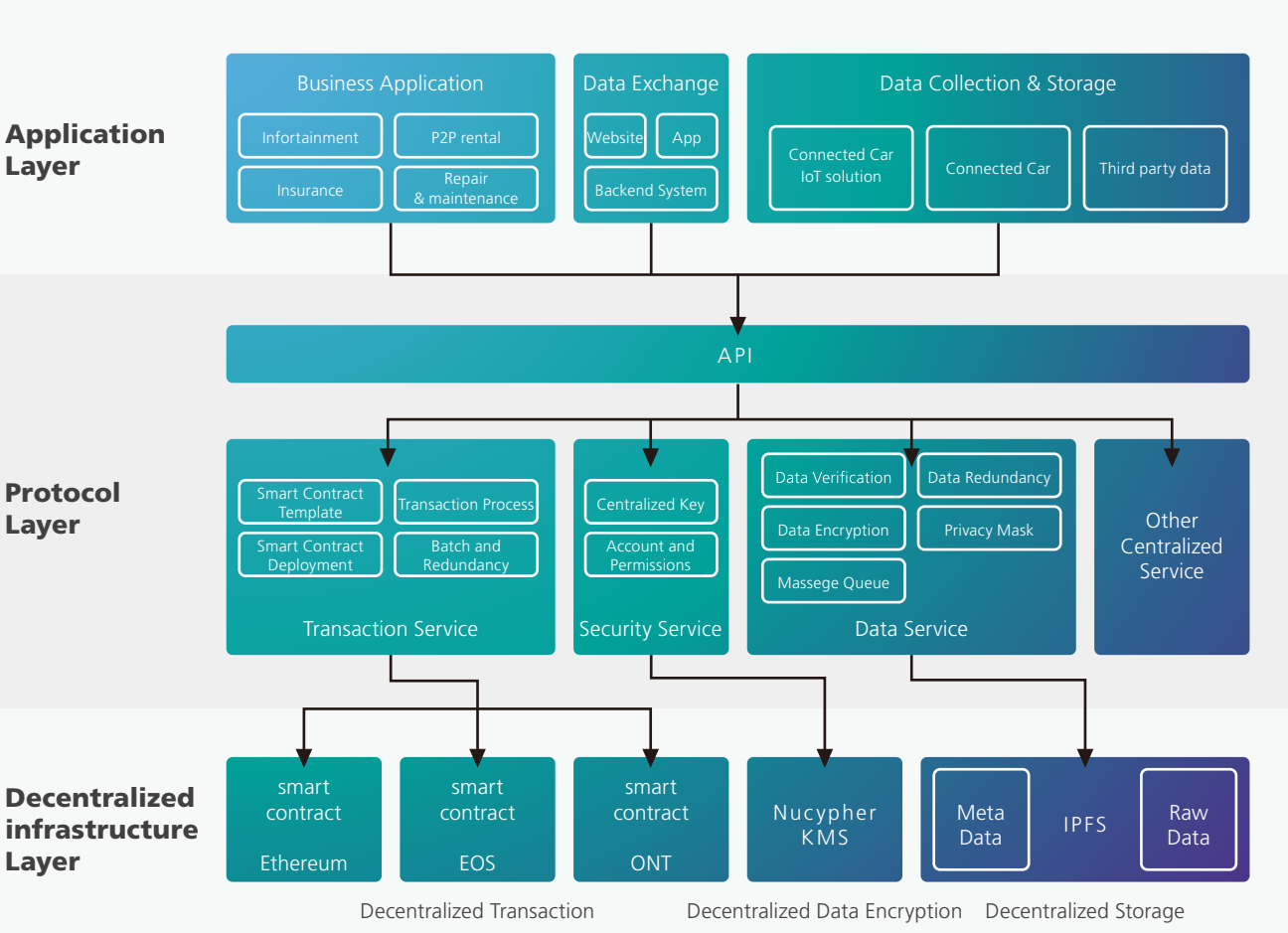
Core System Design

CarBlock Architecture

CarBlock will build a decentralized transportation data ecosystem through

1. Set transportation data protocol
2. Roll out transportation data market
3. Realize easy data access and seamless integration for centralized transportation data application

The core architecture would be a 3-layer structure as shown below:



The CarBlock Architecture

- **Decentralized infrastrcuture layer:** Different public chains have provided different decentrazlied infrastructures, like Ethereum's decentralized transacation, Nucypher's decentralized encryption and IPFS's decentralized storage. The problem of that is the bottom layer and its API are relatively primitive with different limitation (concurrent performance for example), it sets a very high threshold for end users (businesses and car owners) to use and integrate all of them.

- **Protocol layer:** The most important part of CarBlock platform is to build a unified standard above all public chains specifically for transportation industry. On the one hand, CarBlock will encapsul the original interface and integrate all different functions, set the data protocol and provide open API for everyone to use. On the other hand, because the current blockchain technology is not mature, the requirements are not necessarily met in terms of performance and availability. At this stage we are complemented by partially centralized technologies such as batching of operations, redundancy of data, and caching. The entire protocol layer is built by the current stateless microservice architecture of the Internet industry, with high availability, scalability, and concurrency.

- **Application layer:** Data is the cornerstone of the entire system, so the core application is the collection, storage and transaction of data. Application developers do not need to interact directly with the infrastructure layer with all different public chains, they could greatly lower the threshold of application development and simplify the whole process by using CarBlock's program-friendly and unified interface through the protocol layer. At the same time, when the entire CarBlock ecosystem acquire large-scale transportation data, various decentralized business applications can be built on it such as P2P car sharing, insurance, maintenance and so on.

Our philosophy is to use a centralized protocol layer to better serve a decentralized traffic data business, even with the current public chain technology limitation:

1. Essentially all data will eventually be implemented in the decentralized public chain facility, and can be accessed without going through the CarBlock protocol layer, such as querying transactions through the blockchain browser and viewing data through IPFS client. Public chain is still authoritative regarding the data and transactions, and the CarBlock protocol layer is only used for caching and redundancy.

2. The key work of the CarBlock protocol layer is to formulate transportation data protocol and interface standards, and implement interfaces based on the current public chain technology. These standards and specifications won't change greatly from the evolution of the underlying technology, so that the upper layer applications will not need to iterate too much because of this.
3. In the future, when various decentralization technologies mature, the CarBlock protocol layer may exist in various forms, such as a lightweight library, and it can be more convenient for applications to utilize the public chain.
4. The CarBlock protocol layer code will be open source, ensuring complete transparency of the technology implementation, and also bringing together the community to improve the entire system.

In order for easy understanding, we can summarize transportation data-driven business into two scenarios: data collection & storage and data transaction. We will discuss CarBlock's core modules in detail based on these two scenarios and demonstrate how CarBlock can ensure data safety along the whole process.

Data Collection and Storage

Data collection and storage is the cornerstone application of the CarBlock system. By collecting various usage data of vehicle terminals, it is transferred to the IPFS through the CarBlock platform. Business applications in the CarBlock ecosystem will be based on these data.

Data Collection Method and Dimension

CarBlock will first support compatible hardware for data collection which serves as the bottom IoT and sensor layer.

The raw signal collected by the
sensor is encrypted by the hardware and becomes the original data. The encrypted data is transmitted via Bluetooth to the smartphone, or directly through the networking module on the device. The protocol layer's data validator will verify the authenticity of the data from the hardware communication. The data is stored in two parts:

- **Metadata** which only contains all of the dimension information used for the query, as well as an index to their corresponding raw data, such as a hash on IPFS (Merkel Hash) [8]. Metadata will also contain some validation data. For example, data stored based on IPFS will use the same “copy proof” technology as Filecoin [9-10] to implement the original data storage and verification (storage availability) of the car data.

- **Raw Data** Verified, encrypted, and compressed raw data is stored on IPFS similar to the integration of compatible hardware and CarBlock, CarBlock will launch a hardware certification service in the later stage. As long as the certified hardware conforming to CarBlock's data standard, the car network data can be stored through the CarBlock platform interface. Further, CarBlock is also working with the car manufacturer to allow easy implementation for new car to be deployed on CarBlock.

The original signal collected by the sensor will be encrypted by the hardware and become the encrypted raw data, which is then transmitted via Bluetooth to a smartphone or directly from the networked module on the device. Different kinds of data are important for different business scenarios.

The Data Node's core function is to store the connected car data in the CarBlock architecture. The bottommost Validator first verifies the authenticity of the data that's coming from the hardware. Then, the data will be stored in two parts:

The first part is the Metadata, which contains only the information used for the query and indexes to the corresponding raw data, such as Merkel Hash on IPFS. Metadata will also include validation data such as data stored on IPFS using the same "copy proof" technology as Filecoin for on-premise raw data storage and validation (storage availability).

Data Storage and Optimization

Considering that the performance and availability of the IPFS public network may not meet the production standards at current stage, the CarBlock team has made the following optimizations:

- As long as the data provider is willing to share some of the profit from data transaction, they can use a storage service node provided by a third party. In the early days, the CarBlock Foundation could exist as a third-party storage provider, providing high-quality storage service nodes in IPFS networks.

- The CarBlock platform uses the persistent message queue such as Kafka to balance the IPFS workload and improve the performance and throughput.

- The CarBlock platform will build IPFS private network for read-only data redundancy to improve data query performance and availability

- Since IPFS is only for original file storage, and the transportation data has time-series and multi-dimensional features, the CarBlock team is working on

extensions over IPFS to support better storage and access of transportation data.

The Importance of Valid Data

Transportation data is of immense value for the building of applications. To protect the CarBlock community against such fraud, CarBlock has designed two types of data validation.

- Valid Data Collection

  CarBlock requires the data provider to assume two roles - that of the data collector and storage provider. The data provider is a node in the IPFS network and is responsible for storing data. This typically consumes one to three times as much storage as his/her collected data (extra storage space will be used to backup other miners in the community data). This design helps prevent data collectors from forging fake data in large quantities to avoid wasting large amounts of storage resources. For the miners who want to generate huge amounts of fake data for community rewards, they will have to pay significant costs for the storage themselves while their data may still be ultimately rejected and therefore worthless.

  In addition, used car trading is an important use case for CarBlock. Fake driving data increases the apparent usage of the vehicle, which reduces the vehicle's valuation. As a result, miners are unlikely to want to cheat.

  In the data collection phase, CarBlock has a data validator to ensure that the data is collected by the real IoT sensor. In the data trading phase, the data purchaser also has the right to request a sample from the smart contract as a reference for the validation test. If any fake data is found, it will terminate the execution of the contract, and the fake data miner will not obtain any reward via the smart contract.

  CarBlock also performs KYC verification for miners and the corresponding vehicle identification (VIN). Any miner who falsifies the sensor data will be punished by the foundation and permanently expelled from the trading market.

- Valid Data Storage

  CarBlock deploys decentralized data storage verification nodes to perform routine storage verification tasks. The verification node can verify the integrity of the data stored in a way that is more efficient than downloading all the data. Proof of storage is generated as a response protocol to the verification node by sampling a small block of random data blocks and submitting a small amount of data. It is the same as FileCoin, which is also based on IPFS.

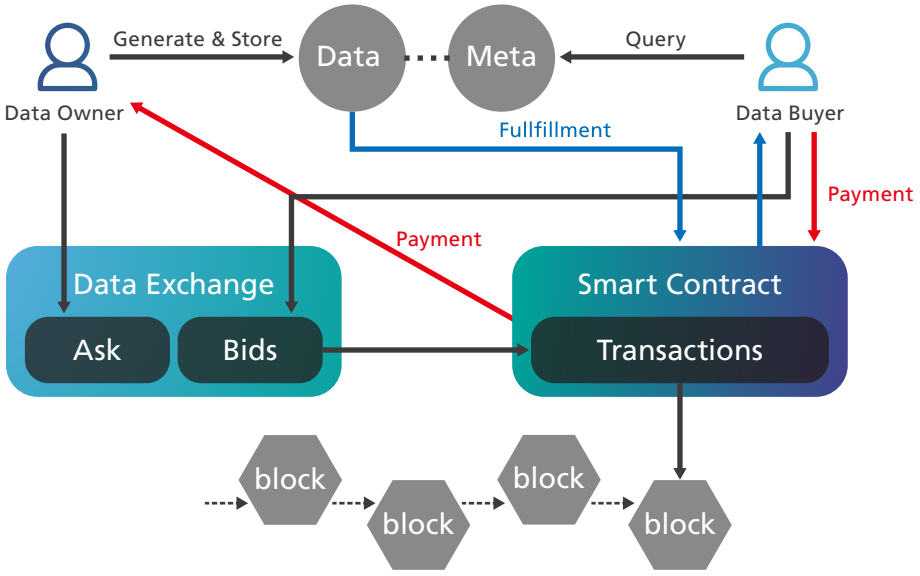
Data Exchange

Similar to data collection and storage, data transaction is a cornerstone application for CarBlock. Only when data can be freely circulated and utilized, the whole CarBlock ecosystem can grow properly.

Data transaction flow

Data transaction in the data marketplace will be deployed through smart contract, the process will be as follows:

1. Select an appropriate configuration template.
2. Set the parameter of data purchase. Eg. Sensor, Scope, Amount, Price, Start/End data of contract, data receiving gateway, etc.
3. A pre-examination will be deployed after the request has been sent to eliminate improper transaction request. (Eg. request that against local regulation)
4. Automatically generate smart contract and deploy.
5. Smart contract will search for data that fits the dimension and scope.
   A. If the data owner has chosen opt-in as the default authorization rule, then the transaction will be automatically matched and conducted.
   B. Otherwise, data owner will receive a request and proceed with a Request & Approval method.
6. Smart Contract will obtain the data through a filter, send the data to the designated receiving gateway and transfer payment to the data owner's wallet.



Example of Date Exchange Process

Smart Contract Template and Audit

The smart contract configuration template is at the heart of the Data Exchange, and the system will be developed and maintained by the CarBlock team and ecosystem partners. Since the owner's privacy is to be protected, the owner's personal information (name, contact details, etc.) will not be sent to the data user, so any transactions between the data owner and the business must occur on CarBlock. There will be more complicated usage scenarios that requires various follow-up steps such as “quote” and “digital contract”. For example, if an insurance company wants to provide an accurate auto insurance offer for a California car owner, after sending the data to the receiving gateway, the smart contract will wait and get an accurate offer from the insurance company and send it to the car owner. If the owner agrees, some kind of incentives will be automatically transferred to the insurance company to pay for the insurance and both parties will complete the digital contract.

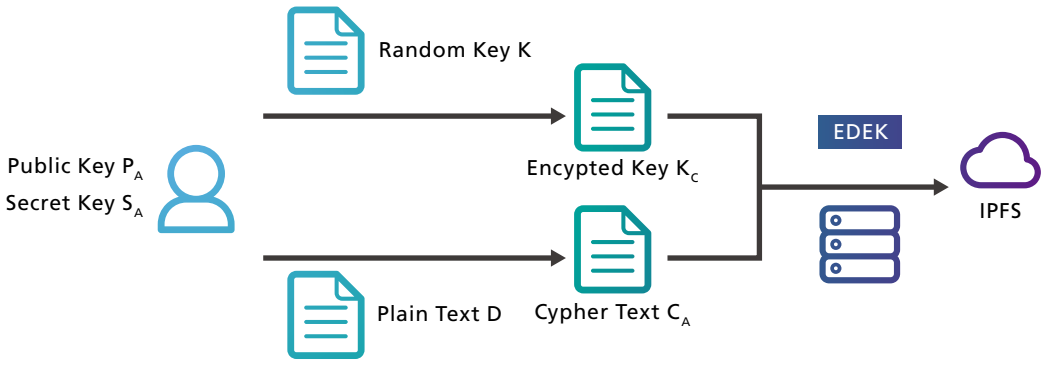
Since smart contracts are open source code running on the CarBlock platform, it is possible to ensure security though lots of means (such as "code review", etc.), and it will not pose any risks to the privacy or confidentiality of both parties. Therefore, we believe that the future is inevitable that this platform will become more and more trusted by the public, extending from data services to subsequent business services, and with the addition of more ecological partners, to have a more diverse and booming usage scenarios.

Data Security

We can not stress enough the important of data security. So we have taken thorough consideration in every aspect of the data flow.

Data Storage security

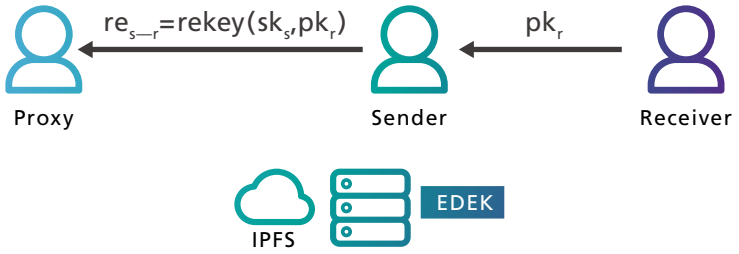
On the IPFS layer, CarBock will use Proxy Re-encryption[13] to implement data encryption and access control. When the raw data is stored into IPFS, it will be further divided into two parts: the encrypted string for the random key K (EDEK) and the data le encrypted with key K, as shown in the following gure:



Encrypt data & save to IPFS

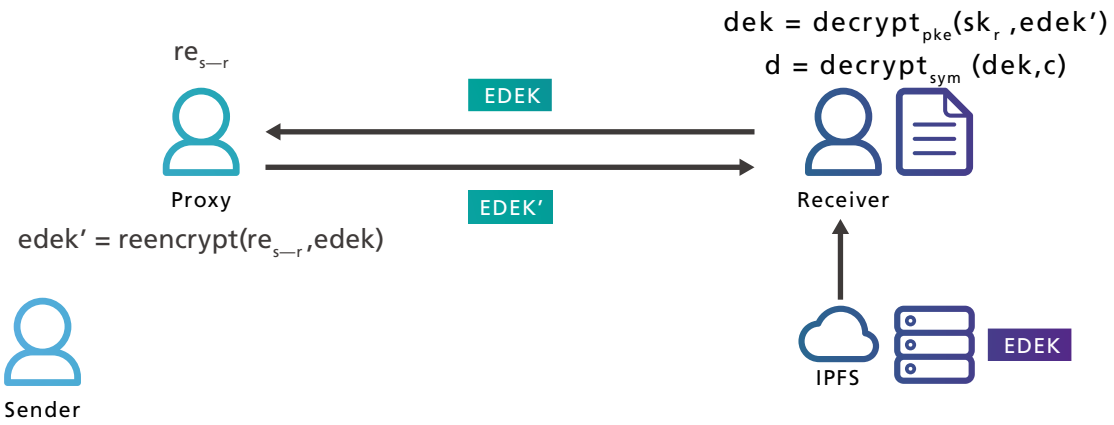
Data Transaction Security

When data demander wants to access and decrypt the data, it needs to initiate a request to the data provider. If the data provider agrees, it will send a rekey to the Proxy. In this scenario, there can also be some third-party services, such as verifying the identity of requester, providing access log service, and so on, which will not be further discussed here.



Data user requests to access & decrypt data

Next, the data demander will initiate a request to Proxy, and get a rekey-ed EDEK copy. Together with the private key, the data demander can now decrypt and access the raw data.



Data user decrypts data by working with Proxy

With Proxy Re-encryption, we can achieve one-time data encryption + multiple-times authorizations, and ensure that:

- Only the authorized party can use its own key to decrypt and access the original data;

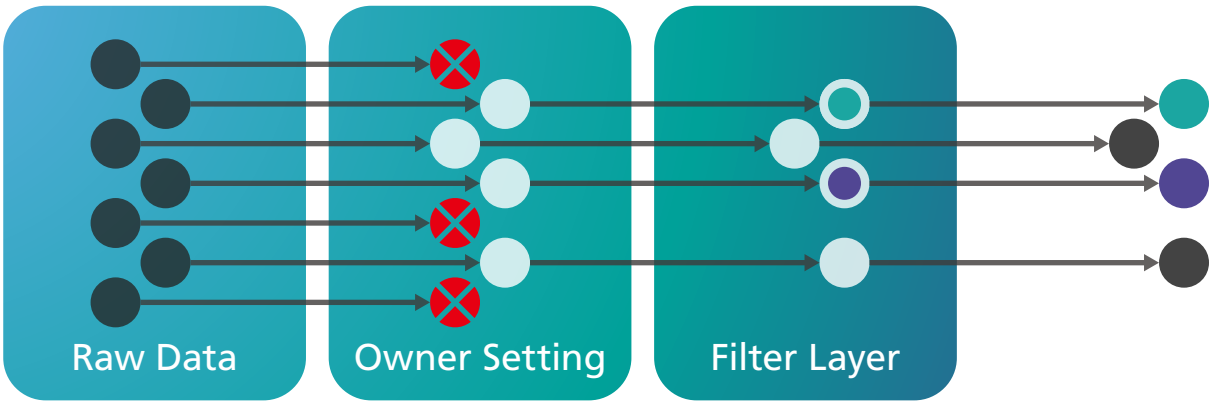
- The authorized party can only access the specified data from data provider, but not all data; And fortunately, there is already an implementation of Proxy Re-encryption in the decentralized world - Nucypher KMS[14]. The CarBlock team can thus use the existing services and further ease the whole development process.

Privacy Protection Module

The Privacy Mask, as part of CarBlock's privacy protection module, is designed to manage the sharing of connected car data. It provides data encryption and protection of users' private data. We believe that the data belongs to the data provider (car owner) and that access to this data must be authorized by the provider. This authorization process can be found in the Request & Approval Model and the Authorization Rules Model.

There are 3 kinds of strategy to the filter layer (we may develop more in the future):

- Confusing strategy: connect a different stage of the trip with a different order.
- Blur strategy: within the range of position accuracy, do the offset processing for the geographical position and blur the exact position.
- Random strategy: within the scope of time accuracy, randomize the order of the logs.



Privacy Mask

The various user settings and filters ensure maximum protection of users' privacy, while also allowing users to disclose more data at will to help further future transportation applications.

Copyright protection based on data watermarking technology

Data leakage or unlawful data resale may occur after the data transaction is completed.We use data watermarking technology to embed some identification information directly into the data, which has no impact on the use value of the data,

and is not easy to be detected or modified, but can be identified by the producer. Through these hidden information, the purpose of anti-counterfeiting and copyright protection is realized.

At present, the most common watermarking algorithms for relational databases or big data are:

- Using the error tolerance of numerical data, randomly select unimportant locations in numerical data, embedding a small amount of watermark information
- Based on the statistical characteristics of the data set, we will sort out different data set to construct a subset, and use the continuous sequence data as the basic unit of the embedded watermark.

Our watermarking algorithms will be based on these common algorithms and make our own optimizations:

- We will implement various algorithms according to the distinct characteristics of the transportation data. For instance, the watermark information generation and embedding methods will be different for location-based driving track data and sensor-based engine data to better conceal the watermark information.
- Add watermark information to multiple dimensions to improve the robustness of the watermark (make it difficult to remove or difficult to remove completely).
- Part of the watermark data itself is encrypted and confused, ensuring the security of the watermark information itself.

At present, there are various methods of removing and destroying watermarks emerge in the market. The attacker and the watermark algorithm designer are also constantly competing with each other. The CarBlock security team will continue to develop a higher quality watermark algorithm to ensure data security.

Disclaimer

This document is only for conveying information and does not constitute an opinion on the transaction of project shares or securities. Any proposal or request for offer to such effect will be made under credible terms in accordance with the permission of applicable security laws and other related laws. The above information or analysis does not constitute any investment decision or concrete advice.

This document does not constitute any investment proposal, investment intent or investment solicitation on securities. This document does not constitute and shall not be construed as a transaction offer or an invitation to transact any form of securities, neither is it a contract or promise in any form.

All the examples of returns and profits in this document are for demonstration purpose only or represent the industrial average, and do not constitute a guarantee for the result of user's participation.

CarBlock clearly states that users with relevant intent shall have clear knowledge of risks on the CarBlock platform. By making an investment, investors confirm their knowledge and acceptance of the project risks, and are willing to personally take responsibility for all corresponding results or consequences.

CarBlock clearly states that it will not take responsibility for any direct or indirect losses arising from the participation in the CarBlock project, including: (i) reliability of all information provided in this document; (ii) any resulting mistake, negligence, or information inaccuracy; (iii) or any subsequent behavior.

Reference

[1] “Top 6 Digital Transformation Trends In The Automotive Industry”, Daniel Newman
https://www.forbes.com/sites/danielnewman/2017/07/25/top-6-digital-transformation-trends-in-automotive/#2fffb3e54e1e

[2] “Metromile”, Wiki
https://en.wikipedia.org/wiki/Metromile

[3] “Connected vehicle Succeeding with a disruptive technology”, Andreas Gissler
https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_21/Accenture-digital-Connected-Vehicle.pdf

[4] “国信证券行业研究报告”, 国信证券
http://pg.jrj.com.cn/acc/Res/CN_RES/INDUS/2016/12/16/ed422d0b-176c-4c65-8cc8-2864fbb81d70.pdf

[5] “Equifax profits by selling your personal data”, THE EDITORIAL BOARD
https://www.dailynews.com/2017/09/12/equifax-profits-by-selling-your-personal-data/

[6] “还有多少App在窥视个人隐私 支付宝年度账单事件背后”, 新浪综合
http://tech.sina.com.cn/i/2018-01-11/doc-ifyqnick7174902.shtml

[7] “Waymo says it has logged 3 million miles of self-driving on public roads”, Chance Miller
https://9to5google.com/2017/05/09/waymo-miles-3-million-may/

[8] “Merkle tree”, Wiki
https://en.wikipedia.org/wiki/Merkle_tree

[9] “Filecoin”, Wiki
https://en.wikipedia.org/wiki/Filecoin

[10] “Proof of Replication Technical Report”, Protocol Labs
https://filecoin.io/proof-of-replication.pdf

[11] “Exponential function”, Wiki
https://en.wikipedia.org/wiki/Exponential_function

[12] “Cumulative distribution function”, Wiki
https://en.wikipedia.org/wiki/Cumulative_distribution_function

[13] “Proxy re-encryption”, Wiki
https://en.wikipedia.org/wiki/Proxy_re-encryption

[14] “NuCypher KMS: Decentralized key management system”, Michael Egorov, MacLane Wilkison, David Nuñez
https://www.nucypher.com/assets/whitepapers/english.pdf

[15] “Average US gas price jumps 3 cents to $2.54 for regular”, CNBC
https://www.cnbc.com/2018/01/08/aver-age-us-gas-price-jumps-3-cents-to-2-point-54-for-regular.html

[16] “Facebook's Mark Zuckerberg finally addresses Cambridge Analytica scan- dal”, Julia Carrie Wong
https://www.theguardian.com/technolo-gy/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica