



# A GLOBAL TRANSPORTATION DATA PROTOCOL WITH DECENTRALIZED APPLICATIONS

## **WHITEPAPER**

Version 4.0

Last Update: August 13 2018



## Table of Content

<b>Summary</b>	03
<b>The Disruptive Power of Connected Cars and Connected Car Data</b>	05
How Smart Devices and the Mobile Internet Are Changing the Automotive Industry	05
Accurate Data Modelling To Replace Traditional Data Analysis	05
Understanding the Connected Car Ecosystem and Its Potential	06
<b>The 4 Core Data Problems in the Connected Car Ecosystem</b>	08
Data Ownership - The Conflict Between Corporate Interest and Data Privacy	08
Data Incentives - Data Contributors Receive Zero Benefit	08
Data Value - Desensitised data Vs User-specific data	09
Data Allocation - Data for the Creation of Transportation Applications Is Nonexistent	09
<b>Core System Design</b>	11
CarBlock Architecture	11
<b>Data Collection and Storage</b>	14
Data Collection Method and Dimension	14
Data Storage and Optimization	15
The Importance of Valid Data	16
Mining and Proof of Work	17
<b>Data Exchange</b>	19
Data transaction flow	19
Smart Contract Template and Audit	20
<b>Data Security</b>	21
Data Storage security	21
Data Transaction Security	21
Privacy Protection Module	23
Copyright protection based on data watermarking technology	23
<b>The CAR Token Economic Model</b>	25
The Cost Analysis of CAR Token Mining	25
How CAR Tokens Will Circulate in the Real World	27
<b>The Formation of the CarBlock Ecosystem</b>	30
<b>Road Map</b>	33
<b>Disclaimer</b>	34
<b>Risk Assessment</b>	35
<b>Reference</b>	39



## 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.

The premise for CarBlock's inception is that from the beginning of the 21st Century, digitalization, networking, and big data have driven tremendous changes in the automotive industry and its peripheral industries<sup>[1]</sup>. CarBlock will be first incubated by the world's leading connected car device company, nonda (No NDA Inc) and then will later conduct its operation independently. The team behind CarBlock took nonda from a small Silicon Valley startup and grew it to being one of the world's leading connected device companies. The team firmly believes that traditional mindsets regarding the automotive and transportation industries will inevitably be disrupted. We will share more details about those insights later in the whitepaper.

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.
  - Car owners can earn token rewards for providing data and in return, receive a more tailored, or reduced, pricing based on the data they provide. This allows participants to enjoy more creative services and products built from the provided data.
  - Automotive and transportation companies can gain enormous amounts of data, which will ultimately drive competition and force companies to come up with better, more targeted, products and services built on the data received via CarBlock. Given that the data itself is sanitized (no personal data will be shared), CarBlock will serve as the bridge between businesses and users and become the most efficient platform from lead generation to order fulfillment.
  - All innovators will have to access to the data they've been longing for, and build more creative services and applications upon it. Actually, CarBlock team has already developed some creative services in the US market and received amazing feedback. We used tire pressure data and cross analyzed it with gas consumption to save millions of dollars of gas fee for our users. We created a tax deduction service based on drivers' mileage logs and helped them to save over \$1,000 in tax payment each year. We are further assured by these attempts that with the help from data, more amazing things will be created by innovators.

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

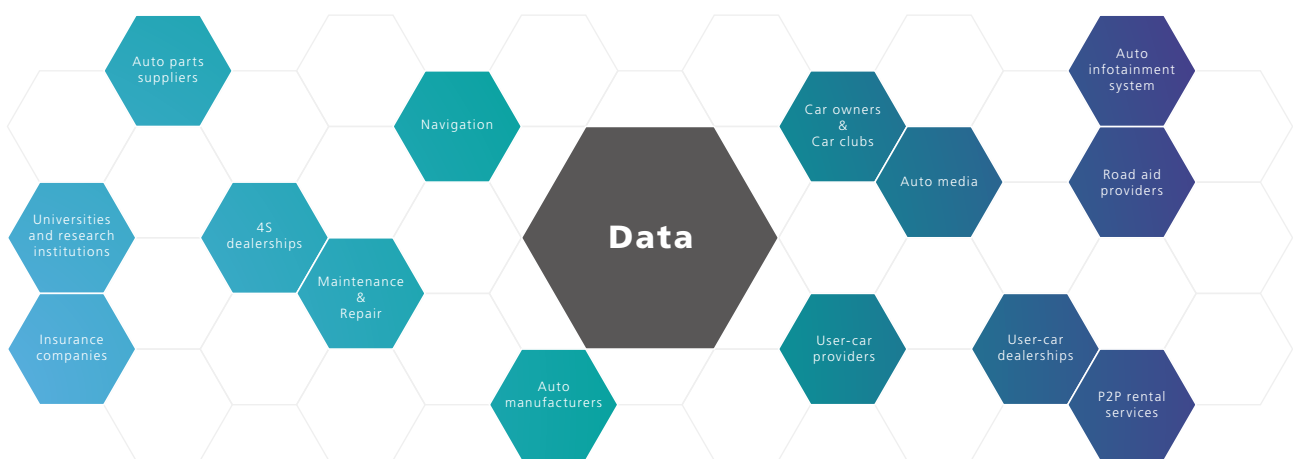
When it comes to vehicle data, traditional data analysis no longer appears adequate. We're currently seeing emerging trends in which connected car data modelling can more accurately represent a vehicle's real profile and therefore serve as a more reliable source of information for making decisions about 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<sup>[2]</sup> 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.

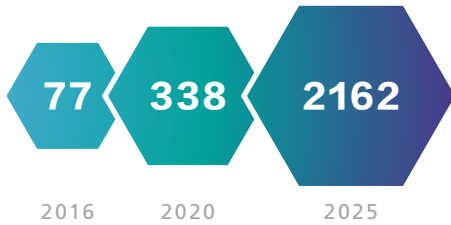


Connected Car Ecosystem

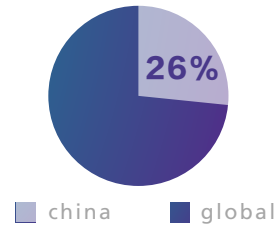
The connected car market holds immense potential. According to Accenture’s report<sup>[3]</sup>, the global connected car market will reach \$840 billion in 2025 (excluding car manufacturers) with China estimated to take up 26%<sup>[4]</sup> of that market.



### China connected car market size (unit: billion dollars)



### 2025 Global connected car market size

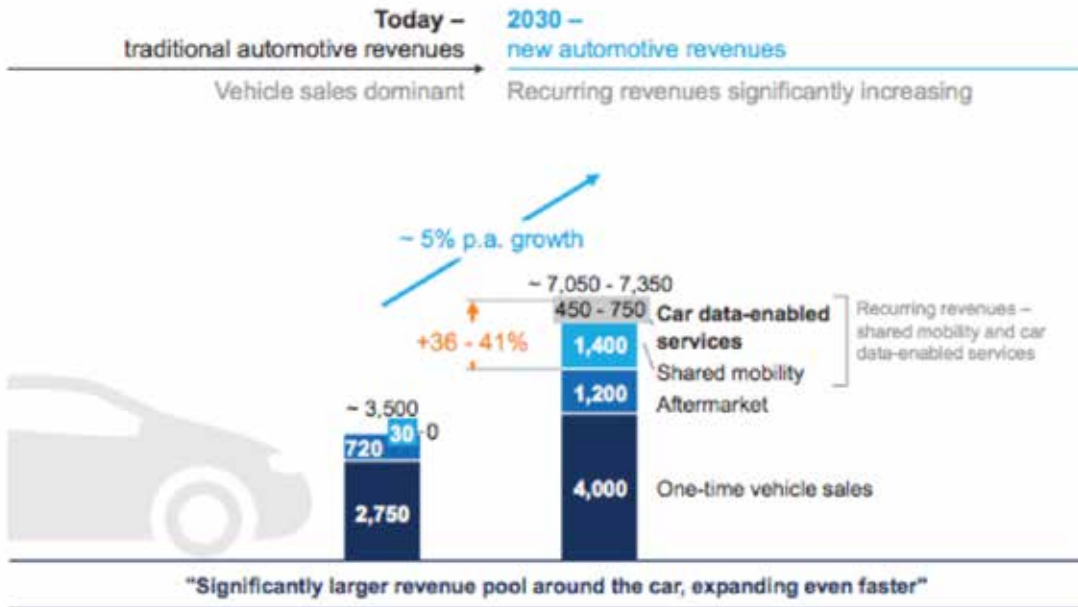


Accenture's report on the connected car market

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

### Car-generated data may become a USD 450 - 750 billion market by 2030

USD billions





# 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<sup>[5]</sup>.  
<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<sup>[6]</sup>.  
<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<sup>[7]</sup> 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.



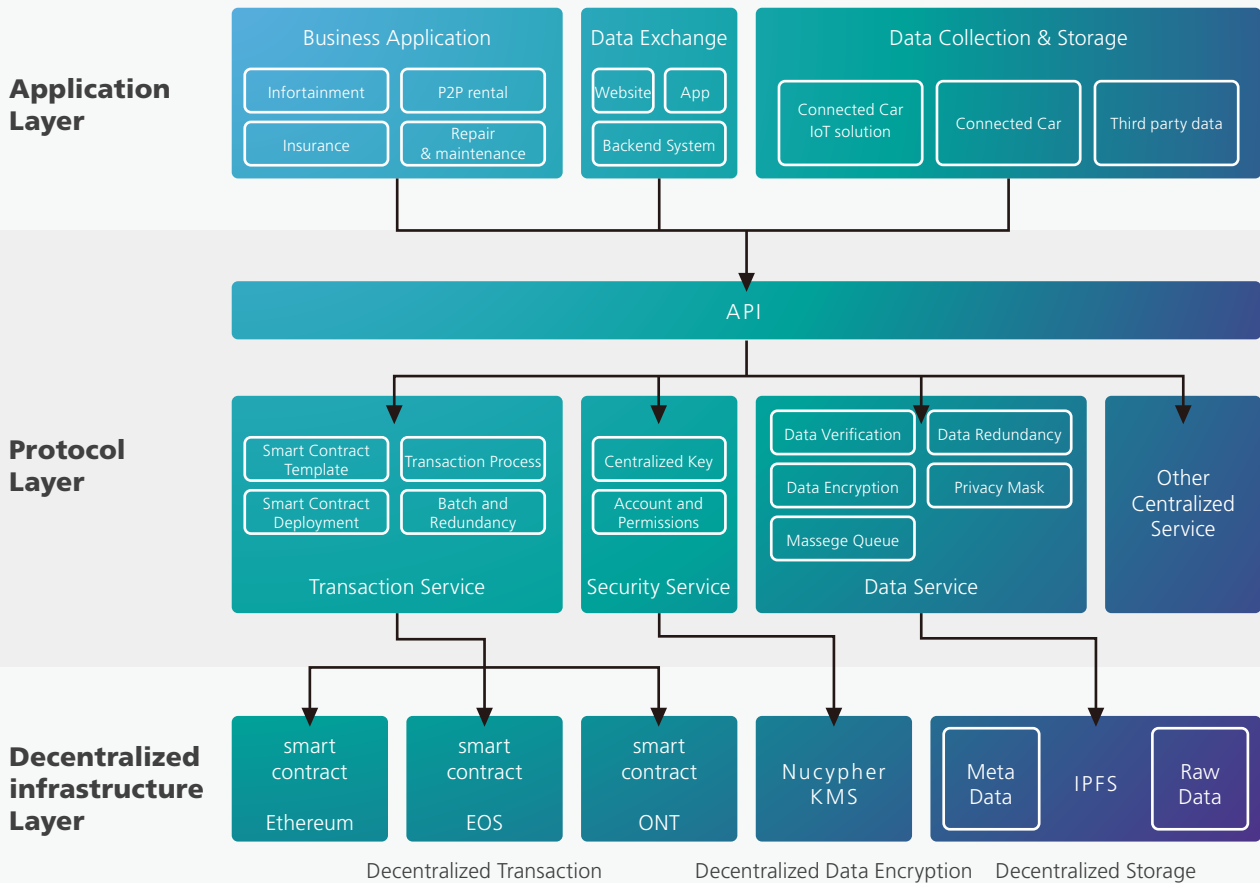
# Core System Design

## 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 infrastructure layer:** Different public chains have provided different decentralized infrastructures, like Ethereum's decentralized transaction, Nycypher'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 nonda smart device for data collection which serves as the bottom IoT and sensor layer. For instance, nonda ZUS smart Car Charger will collect ignition data and car battery data. OBD health monitor can collect engine related data, TPMS for tire pressure and temperature data. 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) <sup>[8]</sup>. Metadata will also contain some validation data. For example, data stored based on IPFS will use the same "copy proof" technology as Filecoin <sup>[9-10]</sup> 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 nonda products 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 IoT hardware and sensor module is the lowest layer of the CarBlock architecture. For example, nonda's ZUS Smart Car Charger can provide vehicle ignition/shutdown



data and battery voltage data. The Smart Vehicle Health Monitor can collect engine data and the Smart Tire Safety Monitor can track tire pressure and temperature. 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. Consequently, those who provide data will be rewarded in the form of CAR tokens (see the following chapter). When there are rewards, there is undoubtedly a possibility of cheating. Individuals may seek to game the system by generating huge amounts of fake data to earn tokens. 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.

### **Mining and Proof of Work**

As discussed already in the previous section, CarBlock's data providers (car owners) act as miners in the ecosystem. Like Bitcoin, CarBlock's miners compete with each other for token rewards. But unlike Bitcoin, CarBlock's miners prove their work by contributing connected car data. Mining efficiency is directly related to the value of the data contributed, which in turn provides valuable transportation data to data users and helps to improve transportation technology. This approach creates a strong incentive for miners and motivates them to collect as much vehicle data as possible and store them in order to share with data users.

In the CarBlock ecosystem, the miner community will receive a fixed number of tokens each day, and the main factors that determine each individual's gain are:

- Data dimension (v), the diversity of data provided by different types of sensors
- Time span (t), the time span that data is continuously supplied
- Data volume (x), the amount of data that a miner provides

When we are building the mining mathematics model, we think there is a very useful model available for both the Data dimension (v) and the Time span (t) parameters, which is the cumulative distribution<sup>[12]</sup> algorithm of the exponential function<sup>[11]</sup> as commonly used in artificial intelligence calculations. Specifically, there is a basic form of calculation, as well as a variant form as shown below:

The cumulative distribution function is given by

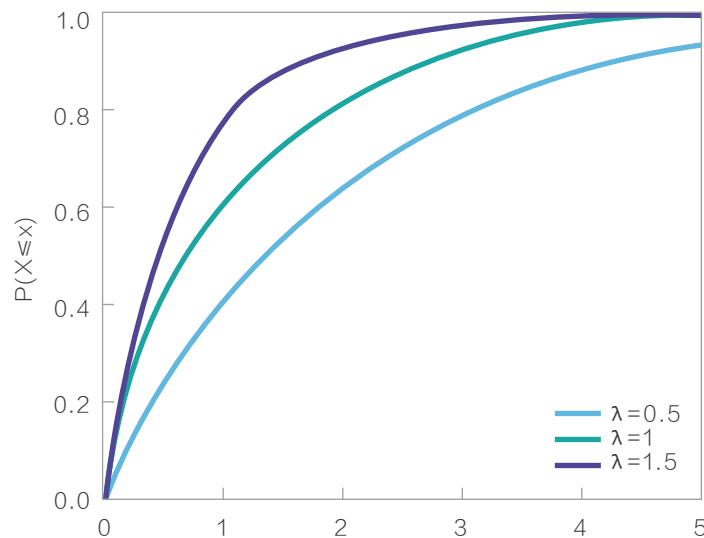
$$F(x; \lambda) = \begin{cases} 1 - e^{-\lambda x} & x \geq 0, \\ 0 & x < 0 \end{cases}$$



Alternatively, this can be defined using the Heaviside step function,  $H(x)$

$$F(x; \lambda) = (1 - e^{-\lambda x})H(x)$$

The purpose of the above calculation is: on one hand, users should be encouraged to keep contributing (e.g. purchase more sensor devices, and provide data for as long as they can); and on the other hand, the gain should decay after reaching a certain level, so that there are no big miners monopolizing the mining output, which is an issue in Bitcoin and other Blockchain communities, and more new miners will be welcomed to join the CarBlock ecosystem.



**Curves of Cumulative Distribution Function**

If the Data dimension ( $v$ ) and the Time span ( $t$ ) are considered as weighted parameters, the Data volume ( $x$ ) can be defined as the base value for the mining benefit, which is verified by the Data Validity process as previously mentioned. For the entire CarBlock ecosystem, assuming the number of daily output for tokens is  $L$  and the equation of total gains is  $f(x) = F(x, v, t)$ , the mathematical limit of the ecosystem can be calculated as:

$$\lim_{x \rightarrow \infty} f(x) = L$$

In practical programming, the system allocation ensures that  $f(x) = L$  will represent all the miners involved in mining on that day.



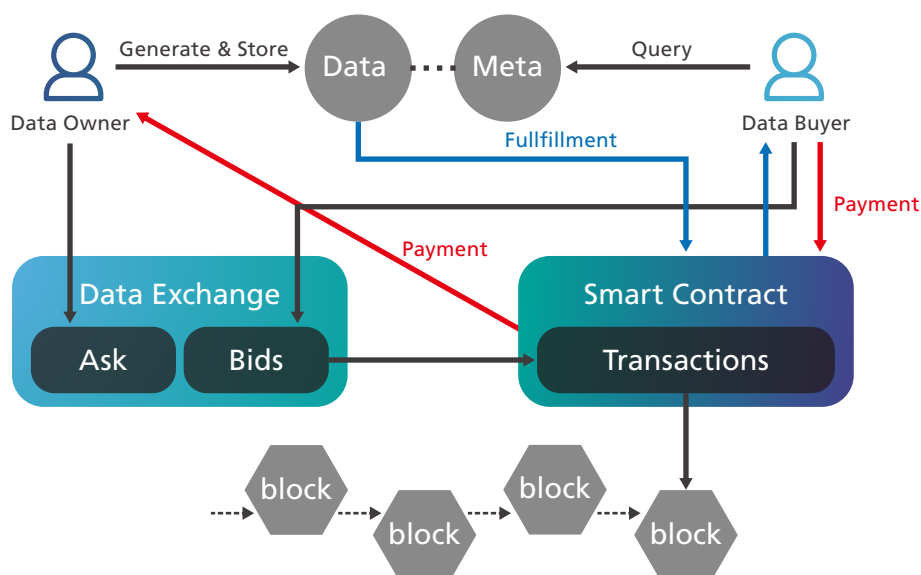
# Data Exchange

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 tokens to the data owner's wallet.



Example of Date Exchange Process



Taking the Ethereum public chain as an example, the data will be purchased by the buyer in the form of an ERC 721 independent token directed to a data link on the IPFS, which the buyer can access at any time during a time-limited period. The data stored on it has been encrypted by the buyer's public key and can only be decrypted by the buyer's private key to ensure data security. We will illustrate the data security issues in the transaction phase later.

Because current cross-chain technologies such as Cosmos and Polkadot are not mature yet, CarBlock does not consider cross-chain transactions for the time being, and data transactions will occur on the same public chain. We will also continue to focus on cross-chain technology advancements in the hope that we will be able to trade freely on multiple chains with a unified CarBlock Token in the future.

### **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 require 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, CAR token 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 through 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.

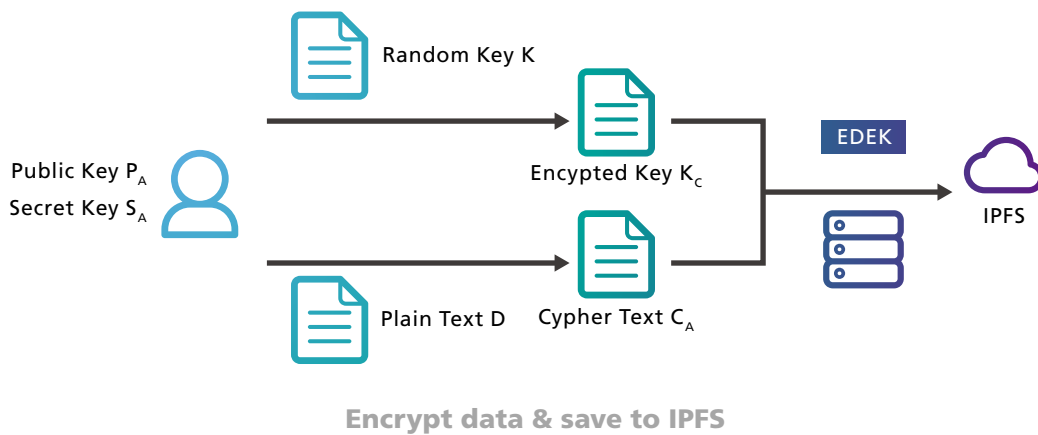


# Data Security

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

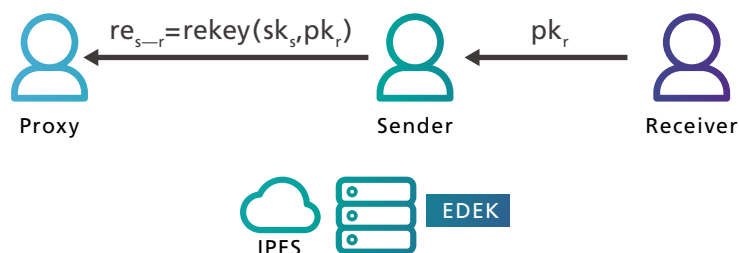
## Data Storage security

On the IPFS layer, CarBock will use Proxy Re-encryption<sup>[13]</sup> 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:



## Data Transaction Security

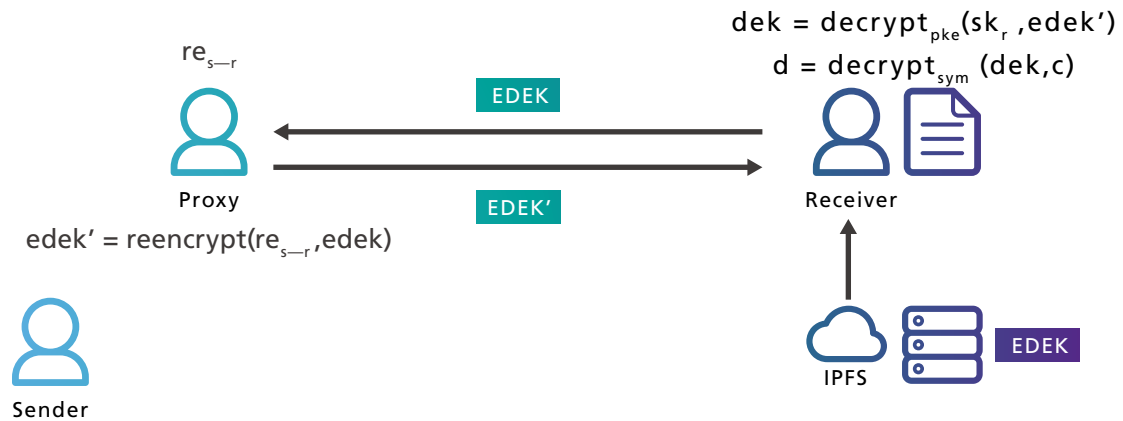
When data demander wants to access and decrypt the data, it needs to initiate a request to the data provider. If the data provider agrees, it will send a rekey to the Proxy. In this scenario, there can also be some third-party services, such as verifying the identity of requester, providing access log 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<sup>[14]</sup>. The CarBlock team can thus use the existing services and further ease the whole development process.

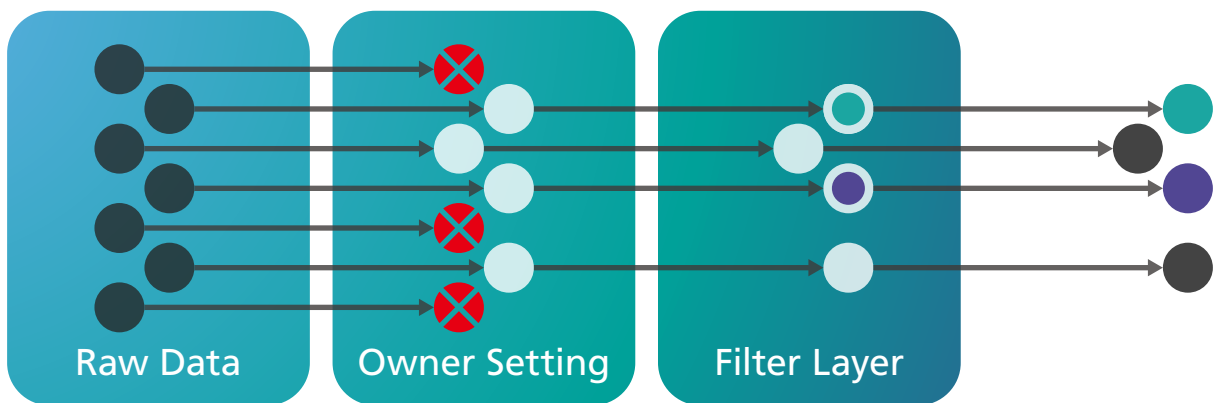


## Privacy Protection Module

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.





## The CAR Token Economic Model

### The Cost Analysis of CAR Token Mining

As previously mentioned, car owners, who are part of the CarBlock ecosystem, can earn CAR tokens by providing valuable car data, similar to a “miner” in the bitcoin ecosystem.

According to certain theories, the cost of mining typically is believed to have an anchoring effect on the intrinsic value of a token. Although we don't necessarily agree that the relationship between 'mining cost' and 'token value' is related in that way, we'd like to lay bare the cost of mining a CAR token, so that you have the information for your reference.

- From a fuel consumption perspective, the cost of mining 1 CAR token is equivalent to  $(\text{Number of drivers in the CarBlock ecosystem} * \text{average daily gas consumption} * \text{gas price}) / \text{Daily token pool}$
- According to a 2017 Motley Fool report, an American driver consumes on average 656 gallons of gasoline annually (1.8 gallons per day). For the sake of simplification, let's assume that this number remains constant.
- According to CNBC<sup>[15]</sup>, the average gas price in January 2018 in the United States was \$2.54 per gallon.
- nonda will recommend all its users to join CarBlock and adopt CarBlock's SDK in its next mobile app version that will enable token mining. In 2017, nonda's MAU (monthly active users) was over 400,000, so we will use 100,000 users as the base for our calculations.

Putting all these numbers into the calculations, and using the number of drivers in the CarBlock ecosystem as the variable, we get the following results:



Number of drivers	Cost of 1 CAR Token (in USD)	Cost of 1 CAR Token (in ETH)*
100,000	2.29	0.0035
400,000	9.16	0.0062
1,000,000	22.86	0.0352
10,000,000	228.60	0.3523

\*1ETH = \$650 (Price of ETH in March 2018)

We recognize that this is not the perfect way to calculate the intrinsic value of a CAR token. Time on the road is more valuable than fuel consumption. Secondly, fuel consumption is primarily for getting from point A to point B, while earning CAR tokens is just an additional benefit. Yet, the calculation still holds merit since it shows that if someone wants to abuse the system to earn CAR tokens, there is a substantial cost in the process.



## How CAR Tokens Will Circulate in the Real World

CAR will play an important role in the future of smart transportation as an utility token. To illustrate how CAR tokens can be earned and spent, we've combined several scenarios into the following diagram:



Figure 8. CAR circulation scenario

To illustrate the circulation of CAR tokens in the real world, we discuss a few sample applications below.

### ● Application #1: Insurance

Currently, the price of most insurance packages are set by static information such as the vehicle's model and age, and the driver's traffic violation history. Very few companies (like the aforementioned Metromile) have started to adjust insurance quotes based on people's driving mileage. What will happen if the CarBlock ecosystem comes into play?

- It is common to see two cars with the same model and age in totally two different conditions. With CarBlock, innovative insurance companies can create insurance packages based on a car's real conditions rather than general information about the vehicle's model and age. People who treat their car better deserve a better insurance quote.
- Certain driving styles and behaviors result in a higher likelihood of being in an accident. As a result, with CarBlock, companies can charge more accurate insurance quotes based on a driver's behavioral data rather than just his or her traffic violation history. Insurance companies can even create insurance packages based on an individual's driving habits.
- Moreover, insurance companies can combine information on a driver's typical



area of activity with climate/road analysis to further adjust insurance quotes and even notify drivers of potential hazards to lower the rate of accidents.

CarBlock has the potential to forever disrupt the auto insurance industry and enable the growth of new insurance services. The biggest disruption we foresee is the abandonment of an annual payment scheme. Why pay the same annual fees as someone who has a riskier driving behavior? Why can't we pay for auto insurance on a per usage basis like we do with flights? With CarBlock, companies can offer insurance to cover from the start of a trip to the end of a trip and adjust the price based on each trip's conditions in real-time.

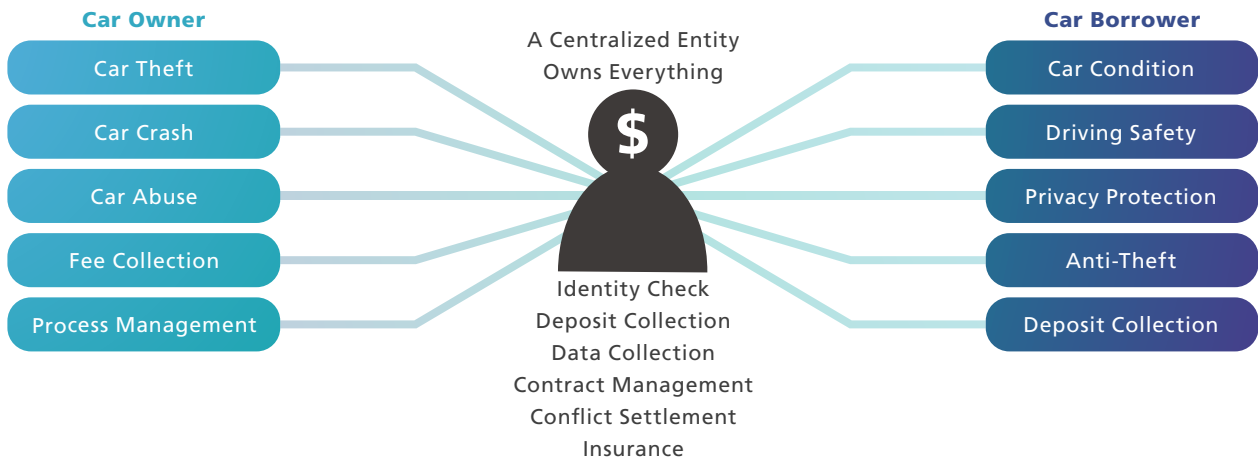
Another change we expect to see in the insurance industry is related to the car owner:

- Car owners with good driving behaviors and pristine car conditions can enjoy better insurance quotes and more discounts from the free market enabled by the CarBlock ecosystem.
- For drivers with poor driving behavior or whose cars are not in the best condition, a higher insurance price will be applied. However, third-party analysis companies can provide services to these drivers to coach them on how to drive better and take better care of their cars to prevent their insurance rate from going up. These services allow service providers to earn CAR tokens from car owners and the car owners to also benefit from becoming better drivers in order to avoid potential financial loss and accidents.

Overall, we firmly believe that CarBlock's open ecosystem will foster commercial cooperation that will create more win-win results than the status quo.

## ● **Application #2: P2P Car Rental**

Although the name P2P suggests decentralization, the P2P car rental business is in fact very much centralized. A central entity owns everything, leaving the car owner and the car borrower with information asymmetry and a sleuth of concerns.



### A centralized P2P rental scenario

In the CarBlock ecosystem, the P2P car rental will become truly decentralized:

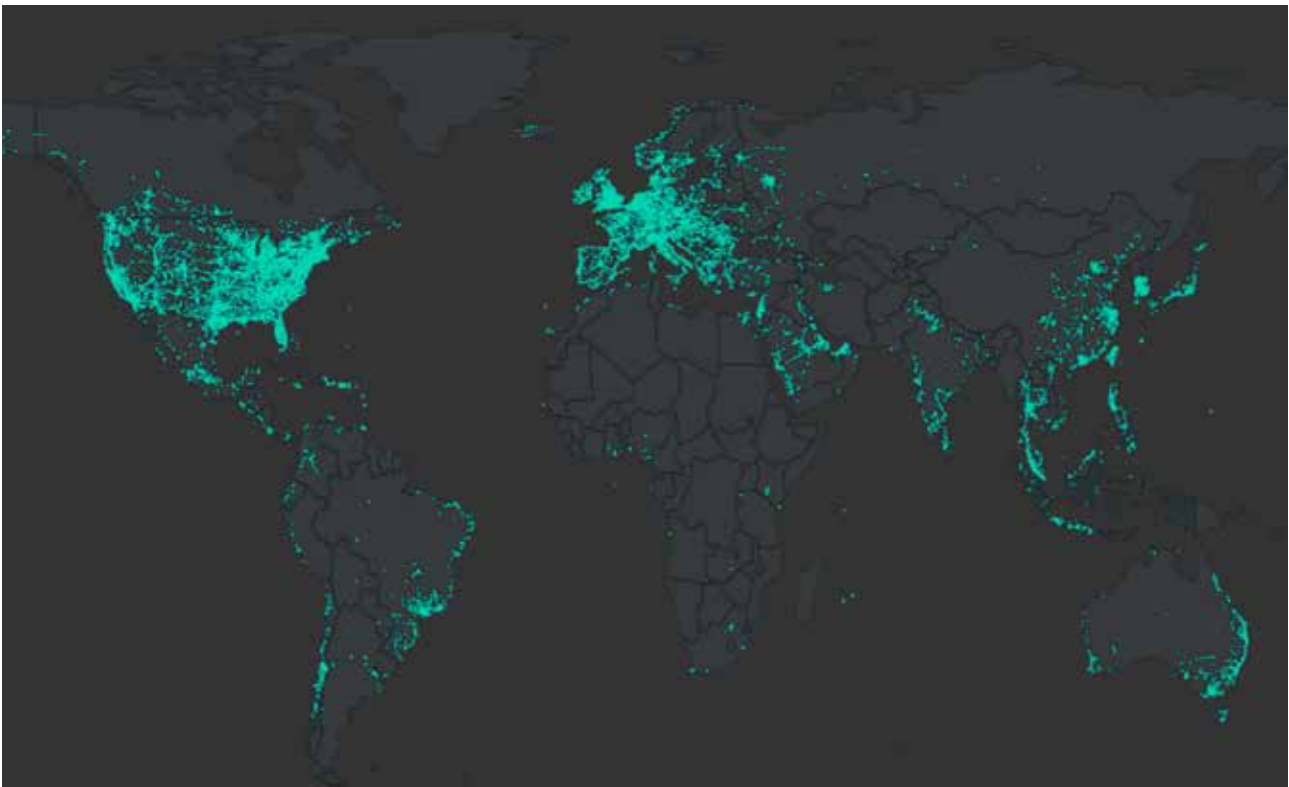
- As a true peer-to-peer business, each party can remain worry-free about privacy breaches. A blockchain based service is a perfect fit for this kind of transaction.
- Information on the car's condition and the vehicle usage by the car borrower will be transparent, accurate and fair.
- Payment will be based on a smart contract and will be automatically calculated from the start of the engine to the safe return of the car.
- Third-party services such as background checks, insurance, anti-theft, and roadside assistance can integrate seamlessly into the system without the involvement of a middleman.
- All car owners in the CarBlock ecosystem will be eligible to become car lenders to take advantage of the market demand.



## The Formation of the CarBlock Ecosystem

As stated in the beginning, CarBlock is a decentralized blockchain platform and ecosystem that serves the entire automotive and transportation industry. Through a standard open protocol, CarBlock will bring all transportation data into the ecosystem and build more innovative decentralized applications based on that. In this ecosystem, users can get more personalized products and services. Businesses can have a more precise cost analysis mechanism and therefore, offer more diverse services and reach their targeted users at a lower cost. Innovators will have a lower barrier to entry, bringing more innovative ideas to fruition via the ecosystem.

Through our collaboration with the leading connected car smart device company nonda, we have acquired a user base of around 500,000 car owners and a mature IoT solution for data collection. This has helped us to quickly kickoff the project and avoid the chicken and egg dilemma that every marketplace project would face at the very beginning. We will leverage nonda's user base, products, channels and brand image to facilitate the deployment of the application and better grow the ecosystem down the road.





The success of this ecosystem relies on:

1. An ample number of car owners joining the ecosystem and providing valuable car data, which attracts more businesses to the ecosystem.
2. An ample number of businesses (including innovators) joining the ecosystem and offering better and more personalized services, which in turn attracts more users.

In terms of initial user acquisition, CarBlock have the following advantages:

**For car owners:** CarBlock's vision is to give data ownership back to car owners and encourage businesses to create better services that are aligned with the public's interest. In addition, the token rewards provide further incentive for car owners to join the CarBlock ecosystem and contribute data.

**For nonda and other similar smart device & IoT companies:** Mining CAR tokens will be a huge boost to companies that are selling smart hardware devices. With nonda as a successful pilot, more companies will join the ecosystem and bring their existing users to CarBlock.

**For Car Manufacturers:** CarBlock will provide free data storage and encrypted data access. This free and open source solution will dramatically reduce the workload and cost for car manufacturers, while improving their capacity to innovate. Car manufacturers simply need to acknowledge that their customers should be the rightful owners of their car data. Then, every car owner can easily manage and control their data using a private key after joining the CarBlock ecosystem.

**For service providers:** Their users can get more tailored, competitive service after joining the CarBlock ecosystem. When the service providers innovate based on the data they get, they would help us to bring more users into the ecosystem simultaneously.

In terms of attracting businesses to join the ecosystem, CarBlock has several advantages:

Businesses will be able to offer products and services based on a targeted user profile and in-depth data analysis.



- CarBlock seeks to accelerate data circulation in the ecosystem, which will help businesses adopt a more data-driven model.
- CarBlock will also enable businesses to reach their potential users at a much lower acquisition cost through data-driven targeting, so that businesses can spend more resources on new product development and customer loyalty programs.

The nature of a token economy is such that it protects its users. An offense such as Facebook's Cambridge Analytica<sup>[16]</sup> scandal would unfold very differently in the CarBlock ecosystem. Simply put, CarBlock will spare no effort to hold the abuser accountable in order to serve the majority's interest in the ecosystem. Developers, innovators, and service providers in the CarBlock ecosystem will also be motivated to offer specific services and tools to help CarBlock strengthen data protection efforts and mitigate the risk of any data misuse.

Finally, CarBlock is an independent blockchain project. As the operating entity, we (CarBlock Foundation) don't need to pursue profits, and therefore can maintain a very open position with no conflict of interest towards our partners. To maximize the value of the entire ecosystem is to maximize our own interests. From a motivational point of view, CarBlock is by far the best entity to run such an ecosystem compared to traditional corporations. The experience and expertise our team has in the automotive industry, multinational business operations and the mobile internet further help us to create critical partnerships and develop the ecosystem.

Our confidence stems from everything mentioned above. We aim to build a new world with better efficiency, personalization and diversity through reinventing the current dynamics at play in the transportation industry.





## Development Roadmap

### 2018 Q1

Kickoff CarBlock officially

Build Core Team

### 2018 Q2

Finish CarBlock fundraising

Deliver first hardware product that supports CAR token mining

Deliver first application that supports CAR token mining

Verify infrastructure technical solution

### 2018 Q3

Deliver second hardware product that supports CAR token mining

Confirm proof of concept requirements for the application layer

### 2018 Q4

Complete proof of concept development for the application layer

Complete prototype test for the protocol layer

Complete First blockchain-based data transaction for real business application

### 2019

Expand and integrate more business partners

Complete multi-chain access for protocol layer

Launch insurance service in CarBlock ecosystem

Launch car maintenance and repair service in CarBlock ecosystem

Launch used car dealership service in CarBlock ecosystem

CAR token supports closed-loop transaction for real business application

### 2020

OEMs integrate with CarBlock and supports vehicle mining

CAR reaches full circulation for real business application

CarBlock supports multiple Dapp



## 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.

CAR is a digital token used, besides other scenarios, in the CarBlock ecosystem. CAR is not a investment target and we cannot guarantee the value of CAR, whose value may decrease under certain circumstances. Due to unpredictable factors, milestones listed in this white paper may be subject to change. While the CarBlock team will make the best efforts to implement all milestones stated in this white paper, all individuals and groups purchasing CAR shall bear the risks on their own. CAR does not represent the rights of ownership or control. Owning CAR does not provide ownership of CarBlock or other CarBlock associated applications. CAR does not confer any rights on any individual to exercise participation in, control over or decision making of CarBlock or other CarBlock based applications.



## **Risk Assessment**

As a new model of investment, investment in digital assets involves various risks. Potential investors shall discreetly assess the investment risks and their own risk tolerance.

### **Risk in Token Sales**

The environment of the token sales market is closely tied to the state of the entire digital currency market. In the case of a sluggish market or existence of other uncontrollable factors, the token price may be underestimated over a long period of time despite its positive underlying value.

### **Risk of Regulations**

To date, blockchain is still in its early stage of development. There are currently no laws or regulations in any country, including China, that stipulate requirements for precondition, transaction, information disclosure, and locking for ICOs. Also, it is still unclear as to how the current policies will be implemented. All these factors may bring uncertainty to the project's investment and liquidity. Blockchain technology has become the main target of supervision in major countries. If there is any intervention or exertion of influence by supervising authorities, CarBlock application or CAR may be affected. For example, if there is a legal limitation on the use and sale of the token, CAR or the development of CarBlock based applications may suffer restriction and obstruction and CAR may be directly terminated.

### **Risk of Competition**

With the advancement of information technology and the mobile internet, digital assets such as Bitcoin are increasing in value and various decentralized applications are emerging, heating up the competition. With the steady appearance and expansion of other application platforms, the community will face constant operational pressure and certain risks from market competition.

### **Risk of Talent Loss**

CarBlock has gathered a technical team and a group of renowned advisors, who



possess deep expertise in their respective professional sectors. Some of our advisors have a long history of active involvement in the blockchain industry. Our core team possesses decades of experience in the development and operations of an internet product. The core competitiveness of CarBlock lies in its stable core team and consultant resources, the loss of which may affect platform operations and project progress.

### **Risk of Development Abandonment or Failure Due to Funding Shortage**

If the price of tokens raised by the founding team drops or the development time is prolonged, the team may face a shortage of development funds and by extension, not have sufficient funds for all activities. If this were to happen, there is a risk that the intended targets may not be realized.

### **Risk of Losing Private Keys**

After the buyer extracts the digital wallet address for CAR, the only means to operate content contained in the address is via his or her secret key (private key or wallet passcode). Users are personally liable and responsible for protecting their secret keys, which will be used to sign transactions and to prove ownership of assets. Users understand and accept that if their private key document or passcode is lost or stolen, the CAR tokens associated with their user account (address) or passcode will be unrecoverable and permanently lost. The best method for securely storing the login document is to store the secret key separately in one or several places and avoid using a shared computer for this purpose.

### **Risk of Cybercrime**

There is a possibility that hackers, other entities, or nations may attempt to interrupt the CarBlock platform or CAR functionality with any methods, including but not limited to DoS attack, Sybil attack, guerrilla-style attack, malware attack, and homogeneity attack.

### **Risk of No Asset Insurance**

Unlike bank accounts or accounts with other financial institutions, CarBlock accounts or related blockchain networks generally don't have any insurance guarantees. For



losses under any conditions, no public or individual entity will be able to provide insurance.

### **Risk of Related Core Protocol**

The current CarBlock platform is developed based on Ethereum. In case of any defect, unexpected malfunction, or attack on Ethereum, CAR or the CarBlock platform may suffer a stop or a loss of function.

### **Risk of an Open Source System**

There are risks related to neglected critical defects in open source software or large scale failures of global network infrastructures. While some of the risks may drop over time due to bug fixes and breakthroughs in computation bottlenecks, other risks are still unpredictable, such as political factors or natural disasters that may interrupt part of the internet or the global internet as a whole.

### **Risk of Rapid Development in Cryptography**

The rapid development in cryptography and the advancements in science and technology such as quantum computing may bring about the risk of cracking the CarBlock platform, leading to possible CAR token loss.

### **Risk of Insufficient Interest**

There is a possibility that the CarBlock application may fail to be used by a large number of individuals or entities. This means that the public does not have enough interest in developing and improving the relevant distributed applications. This lack of interest may have a negative impact on CAR and CarBlock based applications.

### **Risk of Poor Acceptance or Lack of Participation**

First of all, CAR shall not be deemed as an investment target. Even if CAR may have value associated with it after a certain period of time, such value would be very minimal if CAR is not accepted by the market and therefore short on participants. There is a possibility that due to reasons including but not limited to failure in business relations or marketing strategy, CarBlock platform and all the future marketing efforts



supported with the raised funds may fail to achieve success. In such a scenario, there may be few to no supporters for the platform. Of course, this would be very unfavorable to the project.

### **Risk of Application Defects**

The CarBlock platform may fail to provide normal services due to defects caused by known or unknown reasons (e.g. large-scale Node crashes), and may even suffer losses of CAR tokens in extreme scenarios.

### **Risk of Application or Product Failing to Reach Specifications or Buyers' Expectations**

The CarBlock application is still in its development stage and major changes may be executed prior to the launch of the official version. During the development process, CAR or the CarBlock platform may not meet its original specifications or meet the expectations of buyers. This may result due to faulty analysis or any changes in design.

### **Other Unpredictable or Unforeseeable Risks**

Tokens based on cryptography is a completely new technology that has not be fully tested. In addition to risks already described in this white paper, there are other risks that may occur that are not yet mentioned or anticipated by the founding team.



## 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](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](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](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](https://en.wikipedia.org/wiki/Exponential_function)
- [12] “Cumulative distribution function”, Wiki  
[https://en.wikipedia.org/wiki/Cumulative\\_distribution\\_function](https://en.wikipedia.org/wiki/Cumulative_distribution_function)
- [13] “Proxy re-encryption”, Wiki  
[https://en.wikipedia.org/wiki/Proxy\\_re-encryption](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 scandal”, Julia Carrie Wong  
<https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica>