Roadmap for the mass urban aviation industry blockchain solution

Delivering the Terms of Reference in January 2018

Draft v.0.4

Proof-of-flight (PoF) is an algorithm for the blockchain.aero, where the creator of the next block is chosen as a consensus function of hash signatures of all wallets having been involved and signed the actual act of flight: passenger, vehicle, landing pad, charging station, dispatch organizer, air traffic control system.

Other options that exist for the consensus protocols in various systems.

Proof-of-work (PoW) system requires demonstrating processing time was spent by a computer.

Proof-of-capacity (PoC) solutions include proof-of-storage or proof-of-space (PoS), which apply the same principle by proving a dedicated amount of memory or disk space instead of CPU time.

Proof-of-bandwidth (PoB) approaches have also been discussed in the context of using cryptocurrency to reward nodes on the TOR network.

Proof-of-stake (PoS) is used when the creator of the next block is chosen in a deterministic (pseudo-random) way, and the chance that an account is chosen depends on its wealth (i.e. the stake).

Proof-of-ownership (PoO) aims at proving that specific data are held by the prover.

Proof-of-elapsed-time (Intel) works similarly to proof of work,

Use Case Description

You go out on the street and you have got some McFly tokens. Tokens are “flight itself”. You use them to order an aerial vehicle (electric vertical take-off and landing, autonomous or semi-piloted) to the nearest landing area or directly to your house roof and you use your mobile device.

At times, you will wish to vote to get priority service (for example, in case of a temporary lack of available vehicles in your area). Then you do it in two ways:

- With the number of tokens in your wallet (without spending them, this affects the "class of service").
- By consenting to a higher tariff determined by demand and supply ratio at the moment. (And the decentralized system allows you to see real-time changes in the current demand and supply of network capacity in your area and your fair trading will form the final flight price).

The aerial vehicle then arrives to take you to the desired destination and some tokens are transferred from the client’s wallet into the "current" (operational) wallet of the vehicle. From this wallet the vehicle autonomously settles all associated costs of the urban flight and its ecosystem and infrastructure:

- Battery recharge costs,
- Landing pad (vertiport) rent,
- Purchase of media content the passenger opted to enjoy
- Scheduled maintenance,
- Air traffic control,
- Insurance costs, etc.

The vehicle may even track cabin damage and other excessive use of its resources and issues additional bill to the passenger on the smart contract basis.

but consumes far less electricity, the algorithm uses a trusted execution environment (TEE) – such as SGX – to ensure blocks get produced in a random lottery fashion, but without the required work.

Proof-of-Replication allows storage providers to prove that data has been replicated to its own uniquely dedicated physical storage.

Proof-of-Spacetime allows storage providers to prove they have stored some data throughout a specified amount of time.

Upon landing the vehicle settles costs related to its resource consumption by transferring respective number of tokens into its internal “total flight” counter called "resource wallet". This is the life time “meter” of each vehicle, much like the odometer is used to measure the lifetime of the automobile. Tokens on the resource wallet represent the total flight that the vehicle has already performed. Therefore, capacity of the resource wallet is the indicator of the remaining life the vehicle has remaining. It is counterfeit-proof as the information is stored on the blockchain.

Total lifecycle of the Bartini 4-seater vehicle corresponds to 700,000 McFly tokens on the resource wallet, and of the 2-seater — to 500,000 tokens. As soon as this amount is reached the vehicle is recycled and tokens are then transferred to the manufacturer to pay for the new vehicle for the city.

The exact number of tokens to be transferred from the current wallet to the resource wallet for any particular trip is determined by an open calculation algorithm based on the usage rate of each technical component and of the whole vehicle.

General approach to the user profile analysis and users’ business demands to the system

Blockchain is a growing data ledger located on many users’ machines. The data contained in blockchains are:

- Checked for veracity, confirmed by consensus,
- Tamper resistant and protected against unauthentic records.

There are various types of blockchains for different usecases: for transfer of “coins”, for code executing, for protected records keeping, etc. The task of blockchain.aero is to work out a blockchain for implementation in the mass urban aviation industry.

The central fact to be kept in this blockchain, or the “transaction“, is the fact of the flight. The blockchain will record and and keep the network resource consumption in its ledger based on the factual number of performed flights. Within the system, a flight is a unit of measure of the overall load as experienced within every inner-city cluster belonging to the communal network. The network (a cluster) can perform some definite number of flights (minutes). To implement this function, parts of the infrastructure themselves make records in the ledger, thus becoming a part of the ledger, and through this reflecting the fact of the flight performance.

Composition of users and user requirements to the system

User	**Requirements to the system**
Passenger	Call an aerotaxi, pay the flight
Infrastructure party* (incl. service supplier in the broad sense)	Register elements of infrastructure, set rates and fees (rates scheduling), obtain payments

Aerial vehicle	Register flights (from call to landing), pay for the participating infrastructure elements (smart contract), register consumption of the available technical resource
Flight manager	Register acceptance and dispatch of aerotaxi calls, set fees, participate in trades for aerial vehicles calls and infrastructure elements
Manufacturer of aerial vehicles	Monitor the technical resource, register service and maintenance, provide new aerial vehicles in replacement of the worn-out ones
…	…

*) E.g., a user who rents out his material assets for the network, for instance, a roof for a landing pad, a fleet of several aerial vehicles; also a service supplier, for instance, insurer, media provider, etc.

Assessment Of The Performance Requirements: Speed and Storage

According to Uber's estimate for a full-featured urban aviation system for a city size of Dallas they would need 1000 aerial vehicles, which will operate on a schedule 15 mins of flight per every 5 minutes on the landing pad, and the daily utilization rate shall be fall between 20% and 50%.

This makes it possible to assess that at peaks the system has to sustain up to 1000 transactions per minute per one city of operation. Which makes it 1 million transactions per minute for a network of 1000 cities. That is only for the city operations — the business support system side. This should no longer be viewed as unattainable as the Bitshares blockchain is able to handle 6 million transactions per minute.

Which speed levels may be indeed required, for the OSS-side (operation support system), which has to reflect transaction happening on the component manufacturing, assemble, tests and handling, maintenance of the vehicles and the infrastructure.

As such we may establish that current technologies already allow speeds required for the blockchain.aero operations.

Turning to the data storage requirements, it may be feasible to design the system to store only hashes of data contents per each transaction to reduce the storage size requirements. It however may be feasible to design the system to be able to contain large portions of data, since the system is conceptualized with the purpose *not* to rely on any other database.

Additional properties of particular usecases

Each stage of providing and consuming the flight settles a number of tasks. When the infrastructure performs its work embodied in a definite flight, the fact of the flight and all relevant actions performed by the infrastructure have to be confirmed, reflected and protected by blockchain.aero.

This problem is the one to be solved by Proof-of-flight protocol.

Within the mass urban shared aviation network, Proof-of-flight designates not only the fact of an actual flight, but also the process of obtaining confirmation of the flight performance.

- A Passenger was transferred from A to B, and the part of the infrastructure, which was used in this flight, rendered its services. Respectfully, there are wallets in all devices of all parties to the flight:
- of the passenger and of the aerial vehicle (public and private keys of wallets);
- of a flight manager, which took part in the aerotaxi call to the location;

- of other passengers who used the same way of transfer;
- of key components such as batteries;
- of landing pads which allowed take of, from one side, and landing from the other one;
- of the recharge station (serving to recharge the the aerial vehicle's batteries)

The fact of the flight can be traced with devices where the wallets are installed, geolocation, with video records from cameras in aerial vehicles and landing pads. Besides, every participant has a key from his wallet, and it's the combination of these keys which forms an action meaning the confirmation of the fact of the flight - i.e. a Proof of flight accounting for a number of actions required for the flight and confirming that the flight took place, and that the technical, operational and financial network resource was spent during this flight.

In this system it is also worth mentioning the role of such actions as:

- Flight approval — a confirmation that the ground service cleared the flight and provided the route, and
- Flight order — a confirmation that the flight was called through one of the shared use systems.

A passenger can fly without a Flight approval and a Flight order if he uses an aerial vehicle reserved to him personally for a period of time (for instance, if the passenger has 700 K McFly in his wallet). However, such flight must be reflected in the blockchain anyway to record the fact of usage and transfer of its resource in the common network.

Immediate tasks for projecting of technological protocol Proof-of-flight and blockchain.aero

This concept is made as a compilation of requirements from Blockchain aero, based on which a process flowchart is to be made for every participant of the network. The flowchart will reflect actions performed within the framework and parameters of these actions.

The most important, the flowchart must reflect the way in which transactions with tokens (being also containers for the relevant records) in circulation on participating wallets of passengers and other parties to the flight form blocks in the blockchain.

McFly Tokens turnover reflects the changes in the network in correlation with the work performed by the network and components. This is simultaneously a basis for the maintenance and development of the network's technical state, and a basis for settlements according to rates depending on the demand within the network and its clusters during some definite period of time.

Understanding which process and in which way finds its reflection in the ledger, and how technical requirements to the software of the blockchain can be implemented, will consequently allow for various apps on blockchain.aero for various usecases. These apps will be able to compete with each other.