



A Peer-to-Peer Transportation System of Objects

Frederic VEDRUNES

Piloteo (former PassLfix)

Moscow, Russia

www.Piloteo.com / f.vedrunes@piloteo.com

Abstract—The Blockchain technology allows us to send assets in a Peer-to-Peer trustless way. So why not develop an Internet of Objects in the same way we developed an Internet of Information, an Internet of Communication and an Internet of Values?

Keywords: *Blockchain; Internet Of Things; smart contract; Ethereum; DAO; reputation system; DAPP*

I. INTRODUCTION

Our goal is to allow the transportation of objects in a decentralized and secure way using two emerging technologies:

- The Blockchain, which allows proving the transmission of assets in a Peer-to-Peer trustless way and without third party. Furthermore, Blockchain smart contracts allows managing the financial flows according to predefined and signed contractual terms and allows creating applications for distributed organizations.
- The Internet of Things, which allows sensing and controlling remote objects.

Let us see two use cases showing the interest of a decentralized and controlled transportation system of objects:

1) *You forgot your camera in your hotel before coming back from a remote country to your city*

Asking the hotel to send the camera would cause fee and delay without guarantee. You could probably find someone who will travel tomorrow from the same hotel to your city and ask him to take your camera. However, how can you prove the transmission, hold a deposit insurance, pay fee only after receiving your camera and check that the traveler has a good reputation ?

2) *Your company makes specific machines that other companies want to rent*

You could deliver the machine to the first renter who will use it and pay renting fee, then transfer the machine to a transporter for the next renter without necessity to return to the factory. In that case, you need to have guarantee that you will receive rental fee depending on the rental time, to know and be able to prove who has the machine at any time and to

track your machine with specific sensors for checking that the content and state did not change during the travel.

In this document, we propose a whole system of features, which if working together could give a solution to the above use cases changing the way we transport objects. The main features are:

- Self-executing contractual states (smart contracts)
- Localization and events tracking of luggage or/and postboxes
- A novel reputation system
- A deposit insurance
- A Distributed Autonomous Organization to serve delivery services

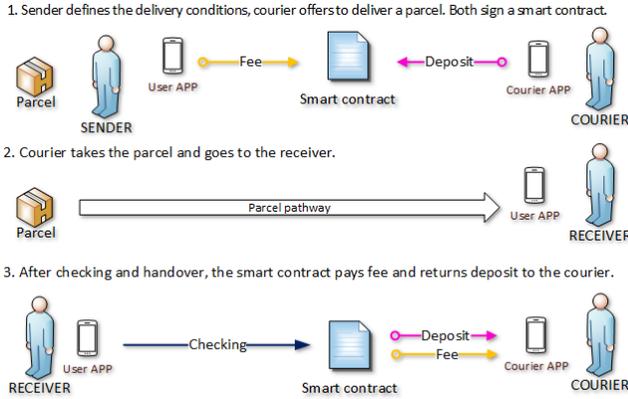
II. DELIVERY PROCESS DESCRIPTION

A. *Delivery Smart Contracts*

A delivery smart contract is a contract in the Blockchain created by a user who wants to transfer a parcel from one place to another, and signed by a courier or a transporter who proposes to execute the transfer according to contractual terms defined in the smart contract.

Though at the present time users and couriers have no legal obligation because of the smart contract, these can foresee contractual terms in a flexible, trustless and automatic way. For instance, the delivery contractual terms can foresee to reduce the return of deposit by 10% per day after a predefined date. The smart contract applies contractual terms with no need to go to court or make a complaint to an insurance company.

The next scheme shows the delivery process in case of a simple delivery from a sender to a receiver via one courier.



B. Transmission of objects

Before taking a parcel, the courier or transporter has to check that everything is legal. If there are illegal items, he does not have to take the parcel. In some countries, the legislation can allow a person-to-person delivery. In other countries, the legislation requires to be a professional service and even buy special equipment to check the parcel for instance in special checkpoints. The project is for responsible and authorized services.

Before transmitting the parcel, the sender can take a picture and send a hash of the picture to the Blockchain, which we use in that case as a proven timestamp. In case of dispute, the sender can prove that the photo was taken before the transmission date. When taking the parcel, the courier can see this photo and check that it corresponds to the content of the parcel.

Before closing the parcel, the sender can add connected devices with sensors inside the parcel.

Each delivery is identified by its delivery smart contract address on the Blockchain. A QR code is printed on stickers pasted on the parcel. The sender and the courier can close the parcel using smart stickers used for traceability, VOID tampering, sealing and authentication.

We prove the transmission of objects with the double signature of the sender and the courier. When the sender transmits a parcel to a courier, both sign the transmission using delivery smart contract methods with their mobile application. These methods automatically lock the fee and deposits in the smart contract until the delivery of the parcel or the predefined contract end date. It will take less than one minute to complete the proof of transmission on the Blockchain.

C. Delivery and reception of objects

The reception is established during the handover of the parcel after the double signature of the courier and the receiver defined in the delivery smart contract. When the courier transmits the parcel to the receiver, both sign the transmission using delivery smart contract methods with their mobile application. This automatically unlocks the fee and deposit from the delivery smart contract. It will take less

than one minute to complete the proof of transmission on the Blockchain.

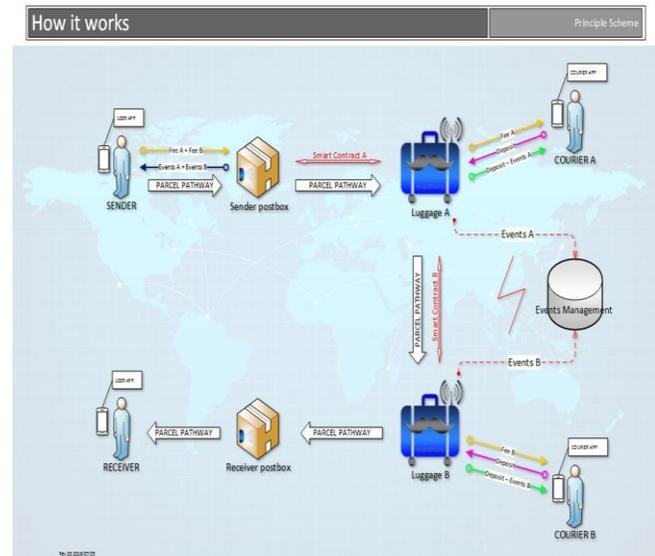
The delivery is possible to a private postbox and without the attendance of the receiver. In that case, the receiver can use a smart and connected postbox, which allows unlocking fee and deposit.

The parcel with its deposit can also be transferred to a local public postbox. In particular, this is the case if the courier cannot deliver the parcel to the receiver.

Lastly, the courier can transfer the parcel to another courier using the same process than for the transmission from the sender.

D. The case of a parcel delivered by several couriers

The next scheme shows how we can transfer parcels in a Peer-To-Peer way (without any server or central organization) using the Blockchain for registering the smart contracts and the Blockchain events, and using the Internet of Things for tracking luggage or postboxes. In this example, couriers A and B can belong to different delivery services.



III. TRACKING OBJECTS

We store in the Blockchain the delivery smart contracts and the proofs that can have an impact to the financial flows linked to the contracts.

Other events as pictures or data frequently sent from sensors are stored off-chain. For a secure and decentralized file system, we store files for instance into IPFS (InterPlanetary File System).

A. The IT Architecture

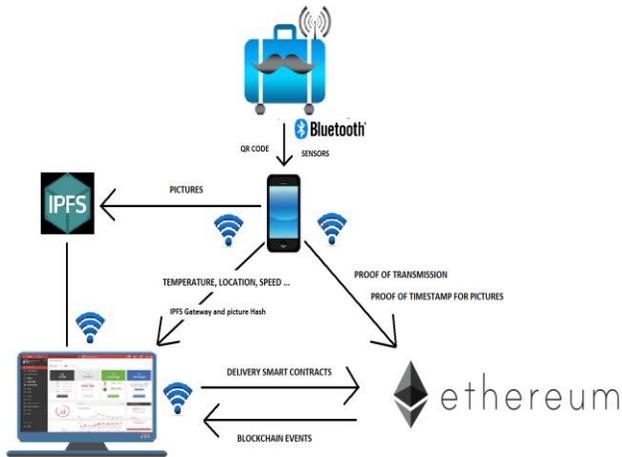
The easiest and cheapest way to track the parcel is to use the mobile phone sensors and the Internet connection of the courier. In mostly cases, a connection via mobile phone

should be enough and used by couriers, who need to develop and maintain a good reputation if they want activity and profit.

The mobile phone of the courier or transporter sends frequently package's sensors data and its GPS location to an off-chain data processor engine.

Furthermore, the mobile phones of participants in the delivery process contain an application linked to an Ethereum wallet, and which allows sending and signing messages to the Ethereum Blockchain.

The next scheme shows the IT architecture for a courier or transporter holding the parcel all the time during the travel.



B. The user web application

The web application is a distributed application (Dapp) allowing owners of objects creating delivery smart contracts and tracking parcels. The user can generate his private postboxes or select public postboxes when creating delivery smart contracts.

Events from the Blockchain allow the user knowing who has the parcel at any time. Charts and map allow visually following the parcel or looking back to the history of contracts or events received from the parcel or the Blockchain.

C. Smart luggage

In some cases, the user can prefer connecting the sensors directly from the objects. The electronic device can include the next features:

- Micro sensors (temperature, magnetometer ...)
- GPS module
- Microcontroller and Cryptographic Authentication
- Low-energy consumption and communication with a global network

At this time, we do not have a global network dedicated to the Internet of Things. However, some networks offer already a coverage growing quickly in the world.

D. Smart postboxes

A user who wants to send or receive a parcel without necessity to meet the courier can use a physical smart postbox with:

- A network connection
- A digital scale
- A camera
- An automatic unlocking system linked to the postbox smart contract

A smart contract is created for each postbox. For public postboxes, rental fee and maximum deposit can be predefined in the smart contract by the postbox owner.

IV. A REPUTATION SYSTEM LINKED TO A DEPOSIT INSURANCE

A. Reputation tokens

Reputation tokens named PASS are tokens used as a currency for the payment of deposits by the couriers or public postboxes. The services buy, on the market, tokens that they use for the payment of deposits when taking parcels. Couriers will be able to transfer only packages with input price less than the reputation tokens they can lose in case of not or bad delivery.

We can consider the PASS tokens as a license that delivery service buy in order to work. A developing service should buy tokens progressively as it grows and get reputation.

The reputation tokens of the couriers involved in parcels transfer are updated according to their accurate. If the courier delivers packages in good condition and on time, he will receive back all the deposit he paid when taking packages. Otherwise, he may lose it in accordance with the delivery conditions established and signed in the delivery smart contract. The deflation rate per minute or day can be set in the delivery smart contract and automatically applied when calculating the net deposit during the handover of the parcel. We can also apply a deflation rate linked to data from sensors as the temperature for fresh products or the acceleration for fragile items.

B. Analysis of the reputation

With the volume of tokens held, the amount of tokens used over a period and the amount of tokens lost, it is possible to evaluate the size, the turnover and the reliability of a delivery service. To this, we can add the appreciation given by the users of the service. The set allows new users to know among other things if the delivery service is reputed or not.

C. Disputes

With smart contracts, smart stickers and smart objects, disputes should be rare or easier to fix. However, the system cannot be entirely automatic, and we think that it is important to allow a mediation, arbitration and resolution of eventual disputes. This work is done by a DAO contractor

named mediator and who is incentivized to work fairly, as everything can be published.

Two cases are possible:

1) *The receiver does not want or cannot take the parcel*

The courier can leave the parcel in the nearest public postbox. If the delivery conditions were respected, the deposit should be given back to the courier even if the user does not take the parcel. In this case, the mediator examines the proofs and if they are evident, he makes a decision as to the return of the deposit to the courier. One of the proof is a picture that the courier and postbox can take during the transmission. The receiver can then take the parcel from the public postbox and unlock the deposit paid by the postbox to the delivery smart contract.

2) *The receiver takes the parcel*

In case of dispute during the handover about the content and its state, the courier can upload a picture and send a proof of timestamp in the Blockchain. When taking and signing the transmission of the parcel, the receiver approves the picture. For disputes during or after the handover, the deposit is given back to the delivery service but there can be an impact on the appreciation given by the users and therefore the reputation of the service. For this reason, a reputed delivery service should partially reimburse the user.

D. *Deposit insurance*

For the users, PASS tokens are their deposit insurance. If the receiver does not receive the parcel, the sender receives valuable tokens from the person(s) in charge of the transfer of parcel and which were hold as insurance deposit. With the development of delivery services using the system, the token price should reach stability and liquidity. We can also provide financial tools to have the deposit insurance backed to the currency defined by the user.

Of course, the fee paid by the user will depend on the deposit amount, which is linked to the risk the courier agrees to take. In this way, it will be more profitable for couriers to operate urgently or to transfer expensive parcels, but they will have more risk to lose some amount of their reputation tokens.

The system foresees that the courier and not the user should take an insurance in case of late train or plane for instance. This is a main difference with centralized postal services, which cannot give guarantee to users and are not incentivized to deliver on time.

V. PASS DAO

Pass DAO is a distributed autonomous organization created to serve delivery services. The DAO is not in charge of transferring objects but a global financial organization paying contractors, which serve responsible delivery services.

The organization belongs to its shareholders who decide together the future of the Organization: the services to develop, its contractors and how it works. A forum is used

to discuss the prospective proposals before submitting to the Blockchain.

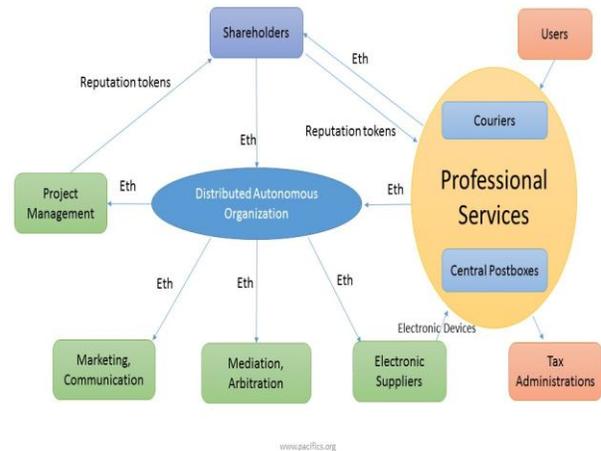
The DAO shareholders form a distributed global Community of persons who funded the DAO. The creation of new shares or PASS tokens is decided by the shareholders and limited for each funding. By allowing funding step-by-step and by limiting the funding amounts, we limit the amount of money in the DAO smart contract.

A. *Flow Diagram*

During the development phase, the organization pays contractors for project management, marketing and communication. PASS reputation tokens are rewarded to the shareholders of the organization when funding the work of the project manager. During this phase, Pass DAO will not collect and share any revenue from his contractors. On the other side, in case of success of the promoted services, the price of shares and PASS tokens (which will be sold to customers when launching a service) should raise.

During the exploitation phase, the delivery services and public postboxes buy from shareholders PASS reputation tokens. They pay fee to the organization for technical assistance, mediation and arbitration service with users or electronic devices if supplied by a DAO contractor.

The next diagram shows the flows between all actors during the development phase and during the exploitation phase. All the transactions are stored in the Blockchain. In this way, it is easy to calculate the profit of the couriers or central postboxes services.



B. *The DAO distributed application (DAPP)*

All the decisions regarding the organization are taken by the Community with voting procedures called committees and managed by the distributed application.

Anyone can submit a proposal. The only condition is to pay committee fee over a minimum, when submitting the proposal. This fee will be rewarded to voters depending on their share in the DAO. If the proposal is estimated (and not

necessarily approved), the creator of the proposal receives shares with an amount equal to the minimum committee fee. The shareholders should vote on contractor proposals, as it is the only way to receive their part of committee fee.

Prepayments to the contractors are done gradually. For each step, the shareholders decide by voting to continue or to stop ordering the work described in the contractor proposal.

VI. CONCLUSION

In this document, we described a novel way to transfer objects using delivery smart contracts and digital assets for the payment of fee or deposit. Sender does not need to make a prepayment and receiver can easily buy a specific local product from a remote region. Delivery smart contracts could potentially reduce frontiers in particular with rural regions or with regions where existing delivery services are expensive or without any guarantee of a delivery date.

Tracking objects during a travel and/or from postboxes improves the quality of the provided delivery service and is a way to avoid or solve many disputes. It gives also potential applications for the renting of objects. The easiest and cheapest way to track the parcel is to use the mobile phone of a courier or transporter, who travels all the time with the parcel. However, with the development of the Internet of Things, we can imagine that in a short future it will be possible to track objects located in containers, for a low cost and everywhere in the world.

The system aims to connect professional delivery services and central postboxes in a decentralized and distributed way. It is not necessary to be a global organization to transport or hold objects you do not own. However, if you are a responsible delivery service with a good reputation, it makes your service easier.

We link the reputation system with the deposit insurance provided to users. The system is not 100% autonomous, as we cannot always automatically determine who is responsible if a parcel cannot be delivered. However, we can have an effective and fair system with the help of mediators contracted by a decentralized organization.

The development of a Distributed Autonomous Organization allows providing services such as communication, mediation and arbitration everywhere in the world, democratically and without any possibility of downtime, censorship, fraud or third-party interference.

By serving any delivery service wishing to share work and economic values inside a growing network, we can potentially develop a global distributed delivery system of objects. This could help monetizing empty planes or cars driving around the planet with an important challenge for our environment.

GLOSSARY

Blockchain: a permission less distributed database that maintains a continuously growing list of data records secured from any tampering or revision.

DAO (distributed autonomous organization): transparent distributed autonomous organization where governance and decision-making system are immutably programmed in the Blockchain.

DAPP (decentralized application): an application, which has its backend code running on a decentralized peer-to-peer network. Furthermore, its frontend can be hosted on decentralized storage such as IPFS.

Ethereum: an open-source, public, blockchain-based distributed computing platform featuring smart contract functionality. It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. Ethereum also provides a value token called "ether", which can be transferred between participants and is used to compensate participant nodes for computations performed.

Hash: a hash function is any function that can be used to map data of arbitrary size to data of fixed size. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value.

Internet of Things (IoT): the network of physical devices that enable objects to be sensed and/or controlled remotely across existing network infrastructure.

IPFS (InterPlanetary File System): peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.

Peer-to-peer (P2P): A network in which each node can act as a server for the others, allowing shared access to data without the need for a central server.

QR code (Quick Response Code): machine-readable optical label that contains information about the item to which it is attached.

Smart contract: self-executing contractual states, stored on the Blockchain, which nobody controls and therefore everyone can trust. They are computer protocols that can make traditional contractual clause unnecessary. Furthermore, smart contracts reduce other transaction costs associated with contracting.

Smart stickers: adhesive sticker used to authenticate, secure, seal and trace a product. It can carry QR codes, opening detection with tamper evidence, temperature indicator...