# 2PS:
# A Proof-of -Ownership P2P file-sharing platform

Arthur MEUNIER
arthur.meunier@cpe.fr
www.2ps.io

**Abstract.** Files sharing is today relatively challenging regarding copyrights, ownership and property rights over original contents. Often, authors and media providers want to control and monetize the diffusion of digital files over the world wide web. 2PS is aiming to provide a trustworthy environment inside which files' ownership, distribution and monetization is fairly and securely managed.

By building a Proof-of-Ownership platform relying on a cryptographic file-encryption protocol, the integrity, diffusion and ownership of the files is preserved among all participants allowing to maintain their owner's rights at any time.

## 1. Introduction

Digital files' distribution on internet is facing multiple challenges since external actors have found ways to copy, reproduce and illegally redistribute digital contents. Today, the annual losses in sales generated by piracy in the United States only is estimated to be over $25 billion. Besides film, music and gaming industries, individuals are also impacted when sharing content online by sometimes losing control on them because of the fraudulent use made by some third parties or companies. Keeping track and ownership over shared content is consequently a need either for commercial or private applications.

What is needed is a safe operating environment into which files' reproduction and distribution is exclusively restricted to the owner of the original file who then can safely duplicate, distribute and monetize it with other participants and third parties. By encrypting each file with a unique and brute-force resistant password prior p2p transfer with a protocol only giving access to the file's final recipient, and by keeping the public hash of this key recorded into a decentralized public ledger, 2PS propose a solution to address this problem.

In addition, the creation of a user-friendly platform built on top of such environment allows to p2p-share and verify both the file's integrity and its legal ownership before any participant can open it (Proof of Ownership). Such ecosystem consequently ensures to have both a legitimate owner and a legitimate file at any time.

## 2. Review of existing file-sharing solutions

Today, popular file sharing platforms and related services are diverse and often specific to one particular sector (videos, music, documents or games). For almost all of the video streaming platforms (youtube, youku, dailymotion, Netflix…), third parties (software) exist and allow to download and duplicate contents. Itunes or QQmusic are by themselves allowing users to download music files that they can store and eventually diplicate and share with external and unsolicited parties (Family, friends, websites, p2p...). Besides, unauthorized streaming platforms fed by hackers flourish on internet, stolen pdf-newspapers are available sometimes even before the paper version is released and, similarly, new video games are quickly "cracked" and shared over the internet.

This illegal sharing-ability is amplified by unregulated p2p protocols such as BitTorrent which often denies responsibilities, arguing that any fraudulent use made of its platform (even if representing the majority of the files exchanged) is not of its concerns, as being a service provider. The lack of possibilities for regulations and the difficulty for user-tracking in such platform is made challenging. In an international context, it is particularly difficult for authorities to identify and convict involved individuals. First, because they are often physically or virtually (VPNs) out of their jurisdiction and second, because they are quickly replaced.

Building a trusted, decentralized and blockchain-enabled authentication protocol able to verify that the user has legitimate rights over the file before being able to play and/or open it would consequently be answering some of those problems. Here comes 2PS.

## 3. Built on EOS

2PS is built by taking advantage of the EOS ecosystem and its smart-contracts capabilities. EOS is chosen as 2PS main-net over other likewise solutions such as ETH or NEO for the following reasons (as of today):

- **Scalability:** EOS can process about 1 million transactions per second versus 10,000 for NEO and about 30 for ETH making transactions faster and providing higher reliability for projects requiring a potentially large traffic as 2PS.

- **DPOS (Decentralized proof of stake):** This consensus mechanism developed for EOS allows to minimize the hashing power needed to ensure transactions are valid and secure, while not requiring a particularly large coin's distribution to entrust the consensus compared to POW and POS respectively.

- **Developer friendly:** EOSIO software gives developers the possibility to use system languages such as C++ or JAVA for the development of higher complexity smart-contracts.

This environment also allows to link such smart contracts to the EOSIO software in the form of DAPPS (Decentralized applications) able to run autonomously off-chain.

For more information about EOS, please refer to Block.one whitepaper available on GitHub.

# 4. The 2PS Token:

### 1. First phase:

The 2PS token is created by opening a smart contract on the EOS blockchain (EOS itself was started as an ERC20 opened on ETH blockchain). By starting the 2PS project out of the EOS environment, the main advantages offered by the EOS mainchain (security, scalability, stability and existing user database) are leveraged for the project, which limits the initial coding work exclusively to the deployment of the 2PS platform and thus, leading towards a quicker release of the said platform.

### 2. Second phase:

In a second development phase, however, a separate 2PS main chain, optimized for its exclusive use (Thus allowing more flexibility for further improvements), is planned to be released as a hard fork of EOS with potential modifications of its source code and a conversion ratio from the initial 2PS token of 1:1.

2PS token is meant to be used as the main payment system through the 2PS platform in order to settle transactions quickly at low fees.

### 3. Supply and distribution:

2PS total supply has been fixed to 10,000,000,000 2PS with a sub unit of 10-9. Such a large supply is known to favor a wider distribution between users than lower amounts, helping to fight speculation and monopolies. The token is 90%* pre-minted (see 8.1) with an initial global distribution as follow:

- ITO (pre-sales in 3 rounds): 30%
- Airdrop to existing EOS wallets: 10%
- Further airdrops: 15%
- *Extra incentives for users to share resources: 10%
- Reserve for operations and marketing: 10%
- Project development and funding: 20%
- Developing team: 5%

# 5. A Multifunctional wallet: The 2PS platform

The 2PS wallet is designed not only to hold 2PS tokens but to assist users through the full usage of the 2PS environment. Being more than a usual wallet holding your private and public keys, this multifunctional tool is referred to as the 2PS platform. Natively, the 2PS platform has the initial following features, described separately and in detail in the following sections:

- File uploading: encryption and file ownership insertion into the blockchain;
- Ownership management (transfer and authorizations) within the blockchain;
- P2P sharing protocol;
- Marketplace: Controlled files' distribution, fees and monetization;
- Anti-piracy tools;
- User-to-user messaging;

# 6. Uploading files:

### 1. Original file: definition

The 2PS platform is built with AI and machine learning algorithms here to determine if an uploaded content is unique before publication on the platform. By comparing the file to online public databases, it seeks for existing similarities (Similar to what Shazaam is for music, google image for images, plagiarism algorithms for texts and documents and automatic verifications on YouTube for videos).

In other words, if the content is already present elsewhere else over the web, it won't be possible to upload it on 2PS, except by fulfilling special conditions leading to obtain a fully **verified official account (See 1.7)**.

### 2. Users verification:

As 2PS is not meant to be an anonymous platform but a place where authors and file's owners' rights are protected, users who want to upload content and consequently legitimately claim an ownership over digital files have to provide identity proofs (ex: picture holding passport or company registration number).

2PS uses automatic tools as passport scanning and facial recognition AI softwares to verify users faster. In case of conflicts, human verifications might occur. In such case, the 2PS team keeps the right to decline incomplete or suspicious applications at any time and at its discretion.

**Users whom do not use the uploading tool (buy only) do not require to register their identity on 2PS.**

**3. Initial "Proof of Ownership":**

Every file uploaded is recorded along its owner public identity (public key) into the blockchain and would consequently constitute the initial "Proof of Ownership" on the platform. 2PS is engaged to verify users and keep the record of their personal information offline once the account has been verified in order to protect users' identity and privacy.

Note that in this context, and in case of failure of the algorithm check, users who upload content on which they have no real ownership won't be protected against legal lawsuits from the file's legal owner. The later can eventually use the blockchain record as proof.

**4. Implications:**

Since the novelty and uniqueness of the content is something enforced by the 2PS platform in order to protect legal files owners, files that are already available online won't be able to be uploaded freely. If well-known artists, production companies and other recognized professionals and institutions will be able to quickly obtain a verified account (allowing them to bypass algorithms and upload files already available on other online platforms), it might not be the case for smaller artists, authors and editions companies. This point is discussed in 6.5 and 6.8

**5. As for patents:**

A patent application can be rejected on the basis that the invention is already publicly disclosed or present high similarities with another existing invention. It is the same general principle applied on 2PS platform for digital files' acceptation.

In this context, 2PS can be considered as a "patent registration application" for digital files. As for patents, users first deposit and go through the application process before making public use of their invention, digital files providers might want to protect their work by uploading it and going through the publication process on 2PS before uploading it anywhere else on internet.

**6. Benefits for users:**

Once the file has been uploaded on the 2PS platform (consequently into the blockchain), it is possible to claim its legal ownership disregarding on which other platform they share it afterwards, the 2PS blockchain's record accounting as a **proof of anteriority**.

Note that if files are protected against duplication inside the 2PS environment, content shared afterwards on other third party's platforms, which might not meet the same security standards, is not of 2PS responsibility in case of copy, duplication or theft.

### 7. Fully verified (trusted) accounts:

Content providers that already manage and monetize former content (published on the web prior 2PS launch) might also want to monetize them on the 2PS platform. In such situation, it would be possible to apply for a fully verified account implying a higher grade identity verification process (for example, but not limited to: company registration details, bank account information, legal representative contact).

### 8. Other accounts:

If a user is an original content provider but has already publicly shared the content somewhere on the web, this participant might not be able to pass the similarity check. In such case, the user has to contact the 2PS team and will be asked to provide extensive proof of his ownership over the content to be able to publish it. At any time, the 2PS team maintain its right to ask for extra documents or even decline the application.

## 2. File uploading: step by step guide

### 1. Uploading:

Users are able to drag and drop or upload files into the 2PS wallet's interface. By doing so, several mechanisms occur:

1) The file is hashed (MD5) which will serve its **Root Identity** on the 2PS network.

2) The file itself **and** its hash value (**Root ID**) are compared to existing databases for similarities using compatible algorithms according to their types (mp3/mp4/avi/doc…)

3) In case of success of the similarity check (no similarity found), the file is encrypted, and enters the edition interface. In case of failure, the file is rejected.

4) The user can edit the file on 2PS server: Title, short description, add a cover, provides links to a trailer… and **define permissions**: read only or ownership transfer (see 7)

5) Once step 4 is validated, a transaction (smart contract) is open on the EOS blockchain and the file's details are incorporated inside (**Subject to fees**).

6) The file becomes registered and available in the 2PS platform's P2P sharing interface;

### 2. Encryption (step 2.1.3)

The encryption process of the file consists at password-protecting it using the AES algorithm (Rijndael). The particularity of this encryption method is that it is a two-way algorithm (possibility to code and decode the message using the right keys).

Independently of the file encryption itself, a password for the file is set as being the hash value (SHA256) of the initial hash of the uploaded file (MD5sum root identity

described at 2.1.1) using the user's private and public keys securely stored (double password protected*) into the 2PS "wallet" (platform).

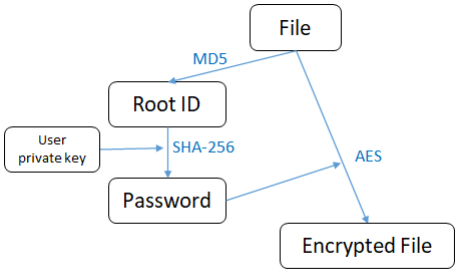



Figure 1: 2PS file encryption scheme

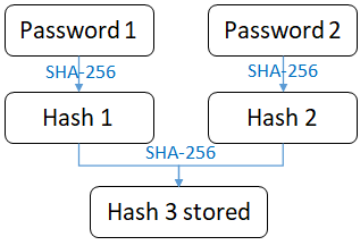



Figure 2: 2PS double password account protection

In fact, the encrypted file does not accept the password itself to decrypt the file but **any private key able to generate it from the Root ID**. Previous scheme was given to explain the main principle but is incomplete and can't work properly without the use of the blockchain:

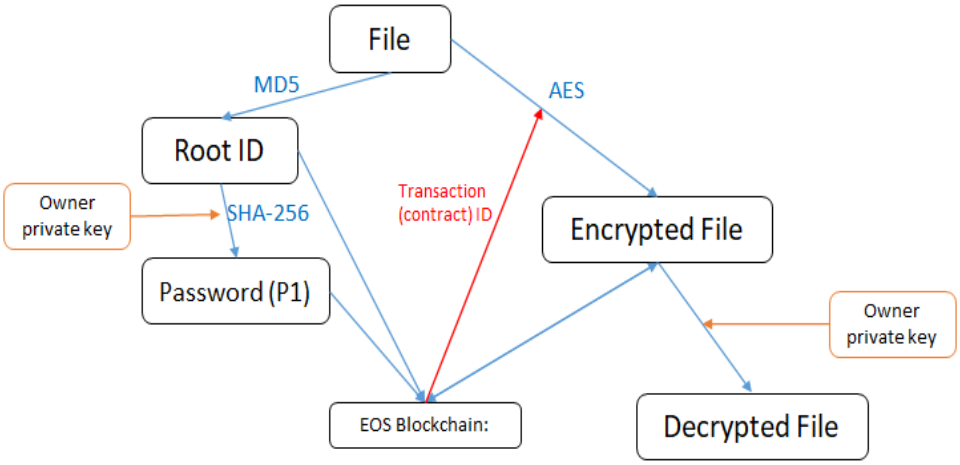



Figure 3: 2PS file encryption/decryption simplified scheme

In practice, the encrypted file refers to a transaction ID in the blockchain from which it will gather (using blockchain explorer) the required conditions to decrypt the file (the contract passed and stored inside the blockchain contains the conditions for which the file can be decrypted):

1. The Root ID of the file;
2. The password (P1) generated by the hash of the Root ID by its owner's private key;

When any user tries to open an encrypted file, the platform's program automatically interacts with the blockchain to access those information.

In order to read or open the file, the following condition must be satisfied: the user's private key is able to generate **PASSWORD = HASH(Root ID) = P1**.

In other words, the file will first require the 2PS platform to look after the last contract (transaction) passed by the user (identified by his public key) within the blockchain and regarding the file (identified by its Root ID).

The file encryption protocol, once connected to the contract will read the authorized password. If the user can provide the same password than the one in the blockchain by hashing the Root ID of the file with his private key, then the ownership is confirmed and the file can be opened.

If the condition is not met, the encrypted file and the 2PS platform will consider the user as not being a legitimate owner of the file and will decline the access.

## 7. Ownership management:

Since the 2PS platform is made to allow file transfers between users, 3 main cases are anticipated:

1. **Full transfer of ownership:** Previous owner lose rights on the file);
2. **Read only:** The file can be read as much as the user want but can't be exchanged (partial ownership);
3. **Temporary access:** Access is limited in time or by number of views.

Regardless of these 3 cases, the native owner of the file (the user who first uploaded it) **will always have the possibility to emit new copies of the file.**

It involves that, in the case of a full transfer of ownership, buyers can resell their copies of the file through the 2PS marketplace, and consequently, compete with the native owner.

Thus, it creates a possibility of a parallel economy for which content's price is influenced by the offer and demand for the files. This situation will be described in more details in the Marketplace section (See 10).

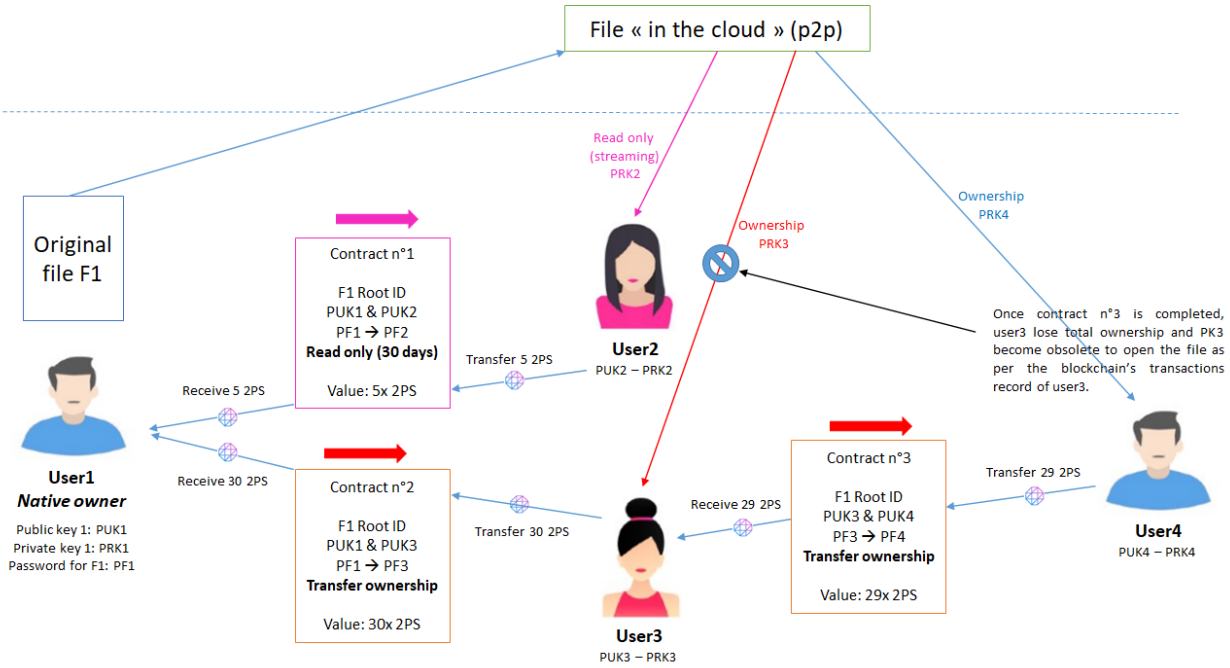
Regarding the technical management of authorizations and ownership's transfer through the blockchain, every transaction between a seller (native owner or not) and a buyer is settled by opening a smart contract into the blockchain:

1- The Seller define a price in 2PS token for the file and open a contract regarding the future rights on the file that will be given to the buyer (example: read only). This smart contract includes the public key of the seller and the Root ID of the file to be sold;

2- Once a buyer is agreed on price and conditions, said user is transferring the amount of 2PS token asked by the seller to the contract. The buyer's public key and the hash of the file's Root ID (made with his private key) is included on the contract which is then included into the blockchain.

3- The corresponding authorization over the file is then available to the buyer able to use his private key to unlock the file, as it is now recorded into the blockchain.

The following figure describes different situations of ownership transfer:




User3 bought full ownership through a smart contract from the file's native owner User1 for 30 2PS and has a full access for an unlimited time. At some point, User 3 decides to sell her rights over the file to User4 for 29 2PS. Once the smart contract is executed, User3 lose her rights over the file to User4.

User2 only bought a 30 days streaming (read-only) period from User1 for 5 2PS. She is not in the capacity to resell this contract after making use of the file (It might eventually become a possibility in a further update).

## 8. Files distribution and P2P sharing protocol:

P2P (Peer-to-peer) protocol is an exchange model where each entity of the network is simultaneously client and server. In the case of 2PS, each participant can be considered as an independent node of the network, sharing a portion of the files in use on the 2PS platform. To some extent, it is quite similar to staking when participants have to stay connected to the network in order to participate in the consensus.

In a situation for which only the native owner would broadcast the file(s) he owns, the availability of the file(s) for other participants is very dependent of this user's connectivity and availability, making the system potentially inefficient.

2PS offers the possibility for any user to allocate storage space (disk) and uploading bandwidth (emission) in order to serve the efficiency of the 2PS network in terms of files distribution.

### 1. Protocol:

In order to enhance file's availability and decentralization, once uploaded, files are divided into smaller parts (usually 60 but may depends on the file's size) using the Reed-Solomon (erasure correction) technology allowing to correct sampling errors even if files received are partially missing or corrupted.

Generated segments are encrypted separately using the AES protocol on the same basis than described previously. It is then randomly distributed between participants whom are sharing their disk storage among the network with a distribution ratio of 3:1 (meaning the files are hosted three times on the network or that 20 out of 60 segments allows to recover the file fully).

The distribution is managed by smart contracts to record where the different pieces are located on the network at any time. Such a system is designed to reduce dependency, increase file's distribution and minimize points of failure.

### 2. Incentives and remuneration:

As an incentive for users to share their hardware and connectivity, fees taken for uploading a new files or opening a 2PS smart contract (transactions) are distributed among these users sharing their resources according to the percentage shared compared to the whole network. Fees are calculated and redistributed automatically every 24h (UTC+0).

After the launch of the 2PS platform and over a period of 10 years, 10% of the total supply of the 2PS token will be released progressively with an increasing difficulty. It is designed to give extra rewards and incentives for people sharing their resources at the beginning:

| year | % | Yearly 2PS amount | Daily 2PS amount |
|---|---|---|---|
| year 1 | 5,00 | 500 000 000 | 1369863 |
| year 2 | 2,50 | 250 000 000 | 684932 |
| year 3 | 1,25 | 125 000 000 | 342466 |
| year 4 | 0,63 | 62 500 000 | 171233 |
| year 5 | 0,31 | 31 250 000 | 85616 |
| year 6 | 0,16 | 15 625 000 | 42808 |
| year 7 | 0,08 | 7 812 500 | 21404 |
| year 8 | 0,04 | 3 906 250 | 10702 |
| year 9 | 0,02 | 1 953 125 | 5351 |
| year 10 | 0,01 | 976 563 | 2676 |

### 3. Going offline issue:

If a sharing user is found offline for more than 10/24h or 6h in a raw, all incentives for this user are cancelled for the (24h) period. If the offline period reaches 7 days in a raw, files allocated to this user are duplicated and attributed to other nodes. This faulty user is also forbidden of sharing any files (and consequently get rewards) for 30 days following the situation.

# 9. 2PS Marketplace:

### 1- Organization:

The marketplace is a dongle on the 2PS Platform which is organized by sections (music, video, films, TV shows, books, cartoons…) with advanced research tools and filters (novelty, price, rating…).

### 2- User reviews:

Any user is able to submit comments and rating through the application. Both are recorded in the blockchain. Users are remembered of it since they will need to approve (sign) the review before posting it (considered as a transaction). Such a context may help to limit fake reviews and inappropriate comments.

### 3- Intellectual property and reclamations:

Abuse in regarding ownership rights are made through the marketplace. Any users finding and being able to provide evidences than another user is committing fraud, property theft or any piracy-related issue can submit a complaint to 2PS.

In such situation, 2PS will study the case regarding the information provided in the complaint and those at its disposal. In the case the complaint is justified, the fraudulent account can be frozen and its files deleted. Reporting user might be rewarded according to the severity (or punished with blocked functionalities if abusive use).

**Note**: During a first phase of deployment, full ownership transfer will be disabled and only streaming (read-only) will be possible. This is an attempt to protect real owners' rights and customers. Indeed, an illegitimate user who would have pass through the identity check with a fake ID and through the similarity check with a file not being his/her actual property won't be able to sell the file.

In the case 2PS has to froze/delete this account for copyrights infringement, no user would have bought the file's ownership from this account. Consequently, and in case of reclamation from the legitimate user, no sold copies representing a full ownership would be in circulation which makes it easier to settle potential conflicts of interest.

In a **second phase of deployment**, when the amount of verified users become consequent enough and the file-checking algorithms will have proven their efficiency, this feature will be activated.

**4- Fees:**

Opening a sharing (selling) contract for a file on 2PS is generating 2 kinds of fees:

1- **Storage fees:** When a contract is opened, the file's owner can determine a duration for it to stay valid. Indeed, the contract can't be open and hosted for free forever*. It also has to pay for the service given by hosts that borrow their resources to make the file available. These fees are taken as 0.01% of the contract value per day. It is also a way to keep only valuable content available to users.

2- **Transaction fees:** a transaction fee of 0.02% is taken by the platform once a contract between users is passed through the marketplace.

***Note:** Even if the user does not want to share or sell a file through the 2PS marketplace, he/she always has the possibility upload, hash and register his/her original file into the 2PS blockchain as a proof of her/his ownership over it (free service).

## 10. User-to-User direct messaging;

If the 2PS platform allows to sell files over its marketplace, it is also possible for users to transfer ownership or give files for free to their friends or acquaintances. A chat is used for this use with a simplified ownership transfer protocol with no fees directly through the chat interface.

Thus, a user can buy a file, read/listen/watch it and then "send" it to one of his/her friends using the 2PS platform (it involves an actual transfer of ownership). When a smart contract is opened with no 2PS amount to be paid, no fees are applicable. If an amount is specified, the platform automatically account for a 0.01% fee (Also in case of 2PS token transfer between users without any file exchanged).

## 11. Anti-piracy tools:

In order to fight piracy and illegal copies more efficiently on the 2PS platform, an extra bunch of tools is added to the software:

1. **Screenshot detection:** if a screenshot attempt is detected, the screen becomes black for the time of the shot.
2. **On screen video recording:** videos are paused if the software detects such an attack;
3. **Copy-paste:** documents are read only (appear like an image) disregarding the ownership state of the user. Thus, even if the owner has a full ownership over the copy he is not authorized to edit it or copy paste it.
4. **Screen pictures using smartphones or camera:** Unfortunately, 2PS has currently no perfect solution at hand to protect from this kind of attack. However, quality won't be as good as the original.

## 12. RoadMap:

We will take a snapshot of the EOS distribution the 11 May 2019 (GMT+0) which we will use to distribute 10% of the 2PS token total supply (1 Billion). The amount distributed to each EOS wallet will be estimated as a % of the EOS hold by the wallet compared to the total circulation.

The airdrop will happen by the end of May and users will have 2 months from the airdrop's date to claim their 2PS token. Unclaimed 2PS token after this period will be transfer to the incentive for users to share resources' balance (see 4).

Meanwhile, first pre-sale round will open on June 1th on the 2PS website (www.2PS.io) and will last one months. In July and August will be held the 2cd and 3d pre-sale round. For more information about the pre-sales, keep following us on Telegram (@2PS), Twitter (#2PS), Signal (2PS), Facebook or WeChat!

We will progressively reinforce the team after the first round of presales and should be able to release a functional beta version with limited features of the 2PS platform by the end 2019 for community review. We anticipate a **full deployment** for Q.2 2020 and a release of the full ownership contracts one year later (Q2.2021)

**IMPORTANT DISCLAIMER: This whitepaper represents the current idea the 2PS team is having of its product and is subject to change without notice. Nothing should be interpreted as a statement of fact or promise in any kind. It is released in order to give a general understanding of the 2PS concept.**