FILE**P**ROOF P-2-P VALIDATION PROTOCOL

ABSTRACT
V1.3

INTRODUCTION

What is FileProof

The main purpose of the FileProof protocol (and consequently tools using the protocol) is to prove the authenticity of validated digital files.

FileProof implies three majors components:

1. the issuer(s) and/or accredited validator(s) ID(s)
2. the body content
3. the holder(s) ID(s) - optional

FileProof definition

At a given time during the file editing phase, issuer(s) and/or validator(s) decide to close and to validate a given file, in conjunction with or not recipient(s)' consent (optional point 3. above).

FileProof primary core business is not to preserve the validated file but to allow anytime following the file validation (issuance) to check if a copy of the validated file is an authentic version or not (i.e checking if file has been altered following the validation) by means of FileProof first level services encompassing the file fingerprint seal into the blockchain. Other optional level services within the FileProof network can provide full data management including the file whole protection cycle.

What is NOT FileProof

- FileProof is NOT an organisation delivering validations, only users and/or their legitimate authorities agree to validate files in using the FileProof protocol according to their own policy and validation workflow.

PROTOCOL: Overview

Secured IDs *(for active users[1])*

- Required for Issuer (validator)
- Required for Recipient (holder)

Nota bene: the first range of proven files might be precisely validated IDs

Content

- Formats (any binary file)

Operations & Services

- Token operating: in any "transaction" users are either *clients* or *suppliers*
  (C) Client pays (S) Suppliers who receives a token incentive and (N) Network gets a fee on the transaction
  (C) can become a (S) e.g as the data holder especially when data are FileProof validated

Nota bene: in the contract use-case protagonists are clients and suppliers at the same time since they are both issuers and recipients. They can pay each other the same fee making the transfer void but fee to (N) still needs to be paid

Basic operations

- **Edit** (write right) C->S<->N (N can make a deposit to S when C is not in the loop yet)
- **Issue** / **Validate** (lock / seal) C->N - Blockchain seal
  - Fileproof container format (e.g hash + confidential once then hash again as the POW is done so far)
  - Hash

[1] *non-active users can access FileProof in using Proof token only, see Token Chapter*

- ➢ Timestamp and address

Standard Services

- ❖ **Access** (view - header - body) C->S->N
- ❖ **Check** C->N
  - ➢ Hash (according to Fileproof format)
  - ➢ Retrieval
  - ➢ Compare
- ❖ **Content management** C->N and/or S->N (option - see with doc.technology below). Access to FileProof container (header) information

Token (FileProofCoin ™ check website FileProofCoin.info)

- Modes work with a key = FileProofCoin token
- Active FileProof users needs token and ID
- Passive FileProof users needs only token

Implementation

- Token, Ops and Standard services (-> doc.technology)
- Accessibility (-> proof.chat)

FileProof TAG = FP#: when a file is validated and the corresponding fingerprint is sealed into the blockchain:

- FileProof container manages/archives
  - Blockchain Timestamp and embedded fingerprint address & information about the FileProof container format used to
  - IDs involved
  - Hashes (validated data Hash, FP random nonce, etc)
  - Pointer to validated data (data can be encrypted only)
- FP# / pointer to FileProof header container
  - To indicate the document is a FileProof i.e a validated doc
  - To retrieve the information stored on the FileProof service website and subsequently the path to make a full verification **Check** if requested

Concept & Definitions

Authenticity

To be authentified a document needs to be validated by the issuer if she / he / they can provide a secure justification about her / his /their identity, i.e in using an authentified and validated ID. The legitimate issuer can assign a validator to validate the document on her / his /their behalf. Identity requirements consistently apply to issuers and their delegated validators.

Assigning delegated validator(s) will involve authentified assignation document(s) validated by the issuer(s). Cascade of subsequent delegations are possible to vouch for legitimation. The legitimation of validators proof will be using the same FileProof system, ie a validator legitimation is a file validated by issuer (based on FileProof system) to allow the validator to validate file(s) on behalf of the issuer.

Identity (file)

An authentified document issued and/or validated by an authority. The identify file provides identification information about the person or the legal entity. The identification information are listed and stored in the authority ledger.

Centralized Authority

Authorities delivering official identification are generally national authorities, for example central database of:

- birth certificates
- Company / legal entity registration (company house)

Decentralized Authority

(this concept does not exist yet, still to be invented)

Identity (copy) validation

1. Assigned delegated validators by authority issuer
2. No assignment from issuer authority to validators

ID (key players)

Authoritative entities usually represent centralized registers such as the Company House or a national register of Birth

An Authoritative entity usually assigns official validators (police, notary).

3 ID categories:

1. Official ID, are IDs validated by an official authority
2. Temp ID, are IDs not validated yet by an official authority
3. Supra ID made only to create authorities IDs

FileProof plans to partner with ID key players. For example, FileProof will soon be interfaced with the Estonian ID-card system, what will allow to create FileProof ID systems and to officially validate them in connecting to the ID-card system using the Estonian certificate (validated by the EU).

Validation RULE

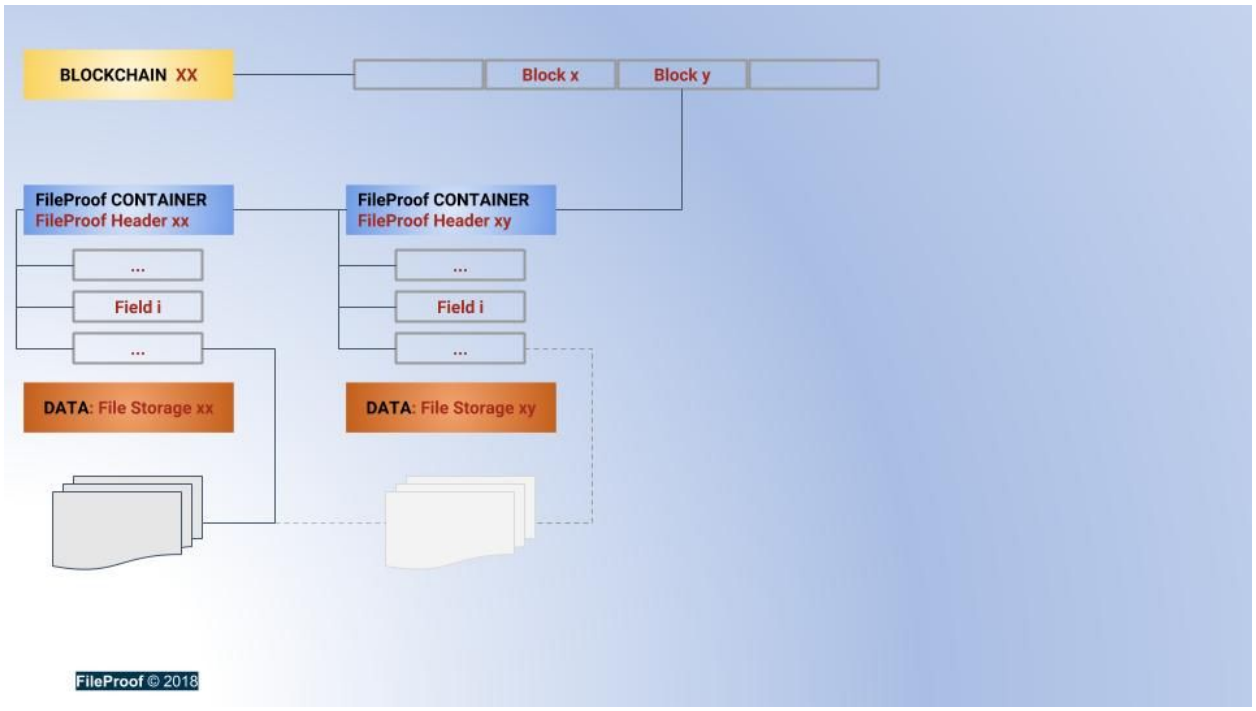
- Data binary must includes a string identifying the issuer
- The validation is only possible if the data (or binary) contains the Issuer identifier
- If the validator ID is not the Issuer, the container should point out the delegation assignment and we should retrieve a chain ending with the issuer ID

Issuer - validator x - validator y - validator z

PROTOCOL: Implementation

- TAG of validated file
- Validation fields
    - Recipient
    - Date
    - Location
    - Validation period
    - More sophisticated conditions (smart contract)
    - If validation involves validator(s) -> pointer to validated legitimation file assigning validator
- Programmatic verification: mechanism to automatically check files authenticity and validity

IMPLEMENTATION ARCHITECTURE



The 3 main layers

1. **Blockchain**. FileProof can be implemented in using any Blockchain to securely store the FileProof CONTAINERS Hash proofs.
2. **FileProof CONTAINER** system. A collection of fields for validating files. See FileProof JSON implementation & description file. The container architecture is generic and made to support static (one shot) but also recursive validations.
3. **DATA.** This layer stores the binaries which are validated. Some users might allow to store only encrypted data. FileProof plans to partner with distributed solutions in this domain such as Filecoin, Cryptyk, SIA, STORJ, others …