Timestamp Certificate

This timestamp was created with *Bitcoin*

originstamp

Timestamp	Nov-03-2018 00:07:36 UTC

Comment: test

Hash:
2c5d36be542f8f0e7345d77753a5d7ea61a443ba6a9a86bb060332ad56dba38e

Transaction:
aed3db9ef94953f65e93d56a4e5bcf234d43e27a1b3e7ce0f274cc7ed750d0e2

Root Hash:
5e92ec09501a5d39e251a151f84b5e2228312c445eb23b4e1de6360e27bad54b

Click here to verify your timestamp.

This certificate is only valid in combination with the original file and OriginStamp's open procedure. More information on https://verify.originstamp.com.

originstamp

Timestamp Certificate

Proof

The proof is necessary for the reproducibility of your document.


```
<?xml version="1.0" encoding="UTF-8"?>
<node type="key" value="5e92ec09501a5d39e251a151f84b5e2228312c445eb23b4e1de6360e27bad54b">
 <left type="mesh" value="7811e3130908fd2678eb2dd3928d245db7f3ed578c21f2ae4fbe680424dc735e">
  <left type="mesh" value="61f48c118002c0e7681e425a3b0e2396475fe0d037ebb0360231b95c2fd60c2f">
   <left type="mesh" value="54280d75669fb9f3ff976c66d03daefa02b691f1aa25558a85f86a5c60961c69">
    <left type="mesh" value="43e89c93c4247511a6eabfe24dfcd331453e04bdde13e688865bf73c3243280a"/>
    <right type="mesh" value="6c127084785466791190c1b4673635274d21e065b9ad9c70d246ef41ba960220">
     <left type="mesh" value="34789458c3010230cef61b6053626ee25f1d79762a76de3517ec5ac2e76ae2e9"/>
     <right type="mesh" value="f375cd66a5552b189a2bfe5f8be433236ff6829dea7bca710e611e98bc7baf0e">
      <left type="mesh" value="5e8d9839b88965971e8f8eb06d2d6bf2f72f75b16100ea175350179c6a82807e">
       <left type="mesh" value="55ed3f4915ab9f93e385f655a2c58c62a5fa2d0e7a4b741263102184e2b7a94f">
        <left type="mesh" value="c04c5bb97b65d009582feb32d88498880216aee8e3bda0c5a0f4ba12244aedb0"/>
        <right type="mesh" value="0bee8d27b7fd9129df599166751af1a9e82bf4e7ac91771f9c15ebf0cb05d74d">
         <left type="mesh" value="88369cb8594af97fb2ee465d5dc3a01e1e23924b8929faca6fdd7293f97e92be">
          <left type="mesh" value="d7ed34b6b74056df3cfb2836bfd55c4cd27b5237ad4a6641cf7003d21be76c88"/>
          <right type="mesh" value="af68501bb80cca4c0bc7d4df6aa2a0c347712e1f2cb1b687a0467e2e9aaf545e">
           <left type="mesh" value="debd8f8a4aa7af602faa9e8e08f5773c6decc29c9f65e80d70ee90a993170f69">
            <left type="mesh" value="8a477ae8ff3b601e709321b17f00117159a7efd861abc74286f7ee6479fe46ce">
             <left type="mesh" value="6a2368efa74c641f2f32d6be8f90a7b6ab5a3235d816faf4034d53d49ce5537c"/>
             <right type="mesh" value="2796b0a5986fe8f497057da457cdcf51ab9fc0ffb996445434bd08e2257b29e8">
              <left type="mesh" value="2c5838c92697fe3d5b8aa14e8f67f6fd2ff4c9e12d536332f57434ebcf0f0196"/>
              <right type="hash" value="2c5d36be542f8f0e7345d77753a5d7ea61a443ba6a9a86bb060332ad56dba38e"/>
             </right>
            </left>
            <right type="mesh" value="3d2466ee2746f818708f8f396649e0cc4d13738248e8ee051a767474ac2f87d3"/>
           </left>
           <right type="mesh" value="130921ae3e04ea13d237a9ed09e33c18574068e8db52e3d7d3d4855d7df3b3ce"/>
          </right>
         </left>
         <right type="mesh" value="8a5d691e559e95448c9aab2d92ba6d58ec9f814ee345e10aee81cf47790d7c2e"/>
        </right>
       </left>
       <right type="mesh" value="55562de568950252020816b6204cbc76820c7c9874c2a4672c99437d99068cf5"/>
      </left>
      <right type="mesh" value="f5fef74b0d216ca6221b024cc5f53d5aee7c9bc33f7289c529f465a0ff2969ea"/>
     </right>
    </right>
   </left>
   <right type="mesh" value="584d06e48bbfe9c5319495b7b3be9eaf7e11aa546ae777575e7e422aafa68fcd"/>
  </left>
  <right type="mesh" value="bf11a94cc0028fe2e0fe476d897da3417cc72777e523d6f0c030c5141bbeb75b"/>
 </left>
 <right type="mesh" value="a62eedb07080ce5a21ad26230bcd50ef37cac8cca43a2f1d946db2d1d47e1f94"/>
</node>
```

originstamp

Timestamp Certificate

Verification

OriginStamp is a timestamp service that uses various blockchains like the Bitcoin Blockchain to create tamper-proof timestamps for your data. Instead of backing up your data, OriginStamp embeds a cryptographic fingerprint in the blockchain. It is de facto impossible to deduce the content of your data from your fingerprint. Therefore, the data remains in your company and is not publicly accessible. All you need to do is send this fingerprint to OriginStamp via the interface. The integration of the RESTful API is very simple and convenient and allows all data to be easily tagged with a tamper-proof timestamp. This document shows the procedure and gives instructions for verifying a timestamp created with OriginStamp.

1. Determine the SHA-256 of your original file

There are numerous programs and libraries to calculate the SHA-256 of a file, such as MD5FILE. Simply drag and drop or select your file, to retrieve the SHA-256 of your file.

2. Validate your proof

First, it must be verified that the hash of the original is part of the evidence. In order to check this, the proof can be opened with a conventional editor and its content can be searched for the hash. If the hash cannot be found, either the file was manipulated or the wrong evidence was selected.

3. Determine the root hash

The Merkle tree is a tree structure, that allows to organize the seed more efficient than a plain-text seed file. The tree is built from the bottom to the top and follows a defined schema. The value of a node is determined by the aggregated hash of its children.

Left child =
a8eb9f308b08397df77443697de4959c156fd4c68c489995163285dbd3eedaef

Right child =
ab95adaee8eb02219d556082a7f4fb70d19b8000097848112eb85b1d2fca8f67

Node = SHA-256(a8eb9f308b08397df77443697de4959c156fd4c68c489995163285dbd3eedaefab95adaee8eb02219d556082a7f4fb70d19b8000097848112eb85b1d2fca8f67) =
47e47c96302eeba62ed443dd0c89b3411bbddd2c1ff6bdfb1f833fa11e060b85

This step is performed for all levels of the tree until the hash of the root has been calculated. If the hash of the root is identical as proof, the calculation was successful and the root hash is verified. The top hash corresponds to the root hash we embedded in the blockchain through a transaction. For a more detailed explanation of the Merkle tree, we want to refer to Wikipedia.

4. Determine the Bitcoin address

Having determined the root hash in the previous step, we can use this as a private key for a new Bitcoin address. The detailed steps to calculate the uncompressed Bitcoin address can be found here. Let's assume the private key is *4eac8a92f8846ea801669b5834aa733e5345cc5e90875152ea6b9f38c724701e*. The calculated Bitcoin Address is *1CV9tyNSdzrKFC2gtpx3Y5GU9rPWb81R4T*.

5. Check the transactions

Check the transactions. By using any blockexplorer for Bitcoin, you can search for the previously calculated Bitcoin address: *1CV9tyNSdzrKFC2gtpx3Y5GU9rPWb81R4T*. The first transaction for this address testifies to the proof of existence. The timestamp of the file corresponds to the block time of the first transaction.