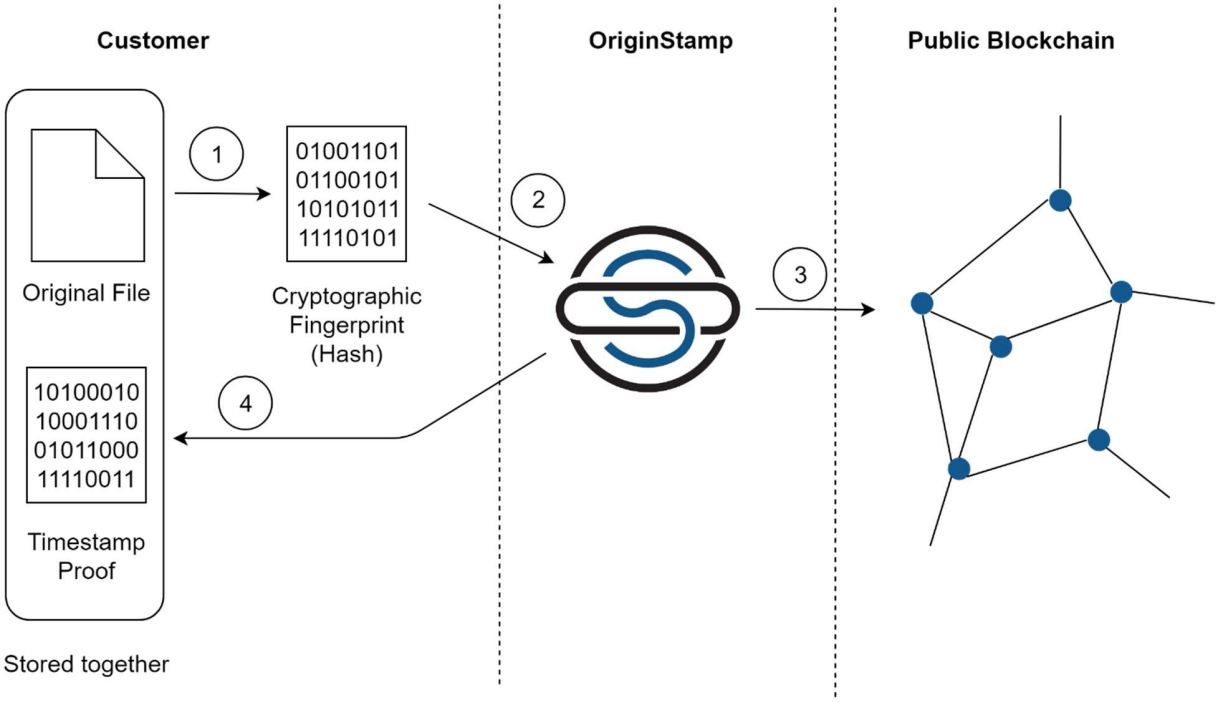
OriginStamp Whitepaper

22. Mai, 2019

OriginStamp AG, Rothausstrasse 1, 8280
Kreuzlingen, Schweiz

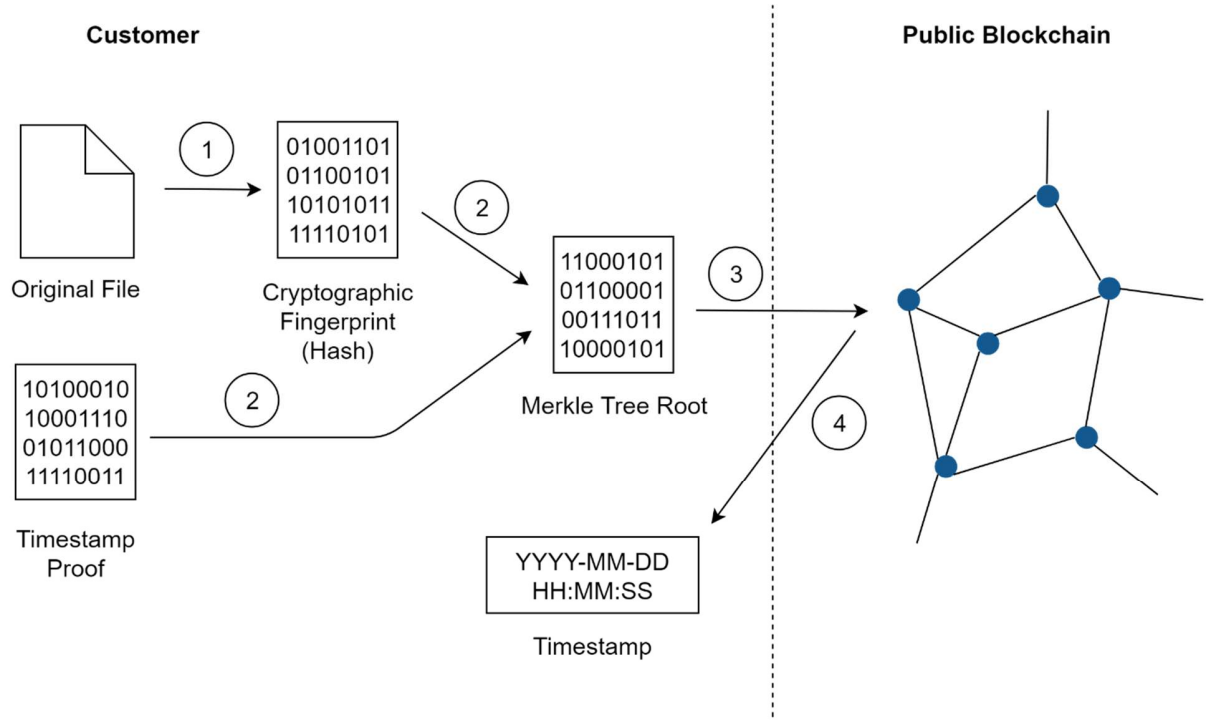
Inhaltsverzeichnis

Erstellen eines Zeitstempels



1. Der Kunde verwendet die öffentlich zugängliche SHA-256 Hashing-Funktion (https://en.wikipedia.org/wiki/SHA-2), um einen Hash der Originaldatei zu erstellen. Dies kann durch den Einsatz verschiedener Online-Tools oder durch den Aufruf von Bibliotheken für Computerprogramme erreicht werden.
2. Der resultierende Hash wird über die OriginStamp-API an OriginStamp übergeben. Dies erfordert einen gültigen API-Key.
3. OriginStamp sammelt in einem festgelegten Zeitintervall alle eingehenden Hashes von verschiedenen Kunden. Diese Hashes werden dann als Blätter in einem Hash-Baum (Merkle tree) behandelt (https://en.wikipedia.org/wiki/Merkle_tree). Die Wurzel dieses Baumes (Root Hash) wird dann in eine öffentliche Blockchain geschrieben. Die genaue Art und Weise, wie dies erreicht wird, hängt von den verschiedenen Blockchains ab (siehe unten). Der Zeitpunkt, zu dem die Wurzel des Hash-Baums in die öffentliche Blockchain geschrieben wird, ist der manipulationssichere Zeitstempel der Datei, deren Hash der Kunde übermittelt hat.
4. Schließlich gibt OriginStamp einen Beweis an den Kunden zurück, dass der Zeitstempel erstellt wurde. Der Beweis besteht aus einer Teilmenge des Hash-Baums, die benötigt wird, um den Zeitstempel unabhängig von OriginStamp zu überprüfen. Es ist wichtig, dass der Kunde die Originaldatei und den Zeitstempelnachweis zusammen speichert und dafür sorgt, dass sich beide Dateien nicht ändern.

Verifizieren eines Zeitstempels



1. Der Kunde verwendet die öffentlich zugängliche SHA-256 Hashing-Funktion (https://en.wikipedia.org/wiki/SHA-2), um einen Hash der Originaldatei zu erstellen. Dies kann durch den Einsatz verschiedener Online-Tools oder durch den Aufruf von Bibliotheken für Computerprogramme erreicht werden.
2. Der Kunde nimmt den zur Originaldatei gehörenden Zeitstempelbeweis und überprüft, ob der Hash der Originaldatei im Zeitstempelbeweis enthalten ist. Anschließend verifiziert der Kunde den Beweis, indem er die dort enthaltene Teilmenge des Hash-Baums verifiziert.
3. Der Kunde ruft das Datum und die Uhrzeit ab, zu der die Wurzel des Hash-Baums in die öffentliche Blockchain aufgenommen wurde. Die genaue Art und Weise, wie dies erreicht wird, hängt von den verschiedenen Blockchains ab (siehe unten).
4. Der Zeitpunkt, zu dem die Wurzel des Hash-Baums in die öffentliche Blockchain geschrieben wurde, ist der manipulationssichere Zeitstempel der Datei, welche der Kunde überprüfen wollte. Wenn die beschriebene Vorgehensweise fehlschlägt, kann der Zeitstempel nicht überprüft werden.

Eine detaillierte Schritt-für-Schritt-Anleitung finden Sie hier:
https://github.com/OriginStampTimestamping/originstamp-verification

Einreichen / Überprüfen eines Root Hashes

Der Prozess, wie die Wurzel eines Hash-Baums (Root Hash) in eine öffentliche Blockchain geschrieben wird, hängt vom der jeweiligen Blockchain ab.

Bitcoin

Für die Bitcoin-Blockchain wird die Wurzel des Hash-Baumes als privater Schlüssel interpretiert. Aus diesem privaten Schlüssel wird die entsprechende öffentliche Bitcoin-Adresse abgeleitet. Der Zeitpunkt der ersten Transaktion zu dieser öffentlichen Bitcoin-Adresse ist der manipulationssichere Zeitstempel. Die Sicherheit besteht darin, dass jede Änderung der Wurzel des Hash-Baumes zu einer anderen Bitcoin-Adresse führen würde.

Eine detaillierte Anleitung finden Sie hier: https://github.com/OriginStampTimestamping/originstamp-verification

Ein hilfreiches Werkzeug, um einen privaten Schlüssel in eine öffentliche Bitcoin-Adresse umzuwandeln, ist btcaddress-alpha:

https://casascius.wordpress.com/2013/01/26/bitcoin-address-utility/