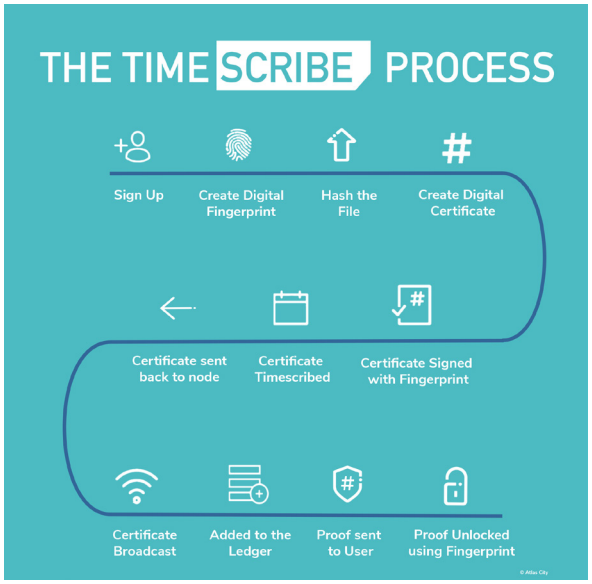
SECURE DOWNLOADED SOFTWARE WITH TIMESCRIBE

The Problem to be Solved

The infiltration into users' local devices via malware hidden in emails or downloaded software has become a large problem over the past two decades. Malware is the abbreviation of "malicious software" that includes viruses, worms or spyware that can hack a local device [1]. Malware can cause the user's data to become compromised, lost or stolen.

The expansion of the internet has provided malware the opportunity to reach more users. Initially, malware was hidden in Word files, then disguised in Outlook emails and multimedia content. This advanced into drive-by-downloads [2] or a "waterholing attack" [3]. The former method delivers malware to users via a downloaded file [1]. The latter method occurs when attackers gain user data to determine websites that they will surf and plant a drive-by-download attack.

Malware leads to the loss of data, excessive pop ups and possible internet theft [4]. However, users often cannot detect malware or validate the download before it infiltrates their local hardware [5] and prove that the software download was unintentional.



1. Sign in to your Timescribe account
2. Under the 'stamp' tab, choose downloaded software file that you wish to Timescribe
3. A timestamp will be created of the file by Ethereum
4. Download the certificate of the file and store securely
5. Share the certificate with relevant parties to verify authenticity and ownership of the content file

PROTECT YOUR COMPUTER WITH VERIFIABLE EVIDENCE OF DOWNLOADED SOFTWARE

The Timescribe Solution

Timescribe enables the authentication of downloaded software before the installation process occurs. This can prevent the download of illegitimate software.

The software provider should upload the original software package so that users can authenticate their downloaded software. The software provider should upload the original software file to create a unique hash, then Timescribe will timestamp it on Ethereum and the software provider will be provided a proof certificate. Individuals can then verify the downloaded file to ensure that their downloaded file does not contain any malware.

Get started at www.timescribe.io or email us at hello@timescribe.io for more information.