super computing systems

Decentralized Trusted Timestamping

Whitepaper

Author(s) Alain Brenzikofer

Reviewer(s) Thomas Meyer, Christof Sidler, Stephan Moser

Copyright reminder

Versions

Version	Date	Author	Changes
V.0.1	2016-12-20	AB	registered a proof of existence of a first description of idea in Bitcoin Transaction 2be8 3049 7ada d18f 439f 4330 4405 e227 2054 af3e 9e62 a70e 050d ee96 c628 4193
V.1 (hash:6967b1e5f4)	2017-01-17	AB	initial publication

Contents

1 Abstract

This whitepaper describes a concept to add trusted timestamps to sensor data based on a public blockchain. This allows to prove that (sensor) data has been captured at a specific point in time. Such a proof includes existence at certain time as well as prior inexistence, with a time precision of minutes. While it has previously been possible to prove that data existed *before* a certain point in time [3], this paper contributes a way to also prove that data only existed *after* a certain point in time. Such a proof of inexistence requires a trusted hardware platform.

2 Introduction

Trusting the timestamps and the integrity of sensor data can be a crucial requirement, i.e. for using surveillance camera footage as evidence in court. Thanks to Trusted Platform Modules [7], it is possible to provide trusted origin and immutability of sensor data as long as one can be sure that the hardware is not physically accessible to the adversary. However, timestamps remain difficult to verify as common time sources like GPS, GLONASS, Galileo and NTP can be spoofed. Blockchain technology such as Bitcoin [8] can be used to provide a "‘proof-of-existence"’ [3]: A document's hash can be stored in the blockchain as a payload to a transaction. This way one can later prove the existence of the hashed document before the corresponding transaction was included in a block on the blockchain. This proof relies on the immutability of a public blockchain and on the fact that it is very unlikely to know the hash of a document without knowing the document itself.
In the following section, a method will be introduced to complement proof-of-existence with a proof of prior inexistence.

3 Proof Of Origination

Proving the time of origination requires the proof of prior inexistence. While it is impossible to generally prove inexistence of something, we will assume the following in the case of sensors measuring physical quantities:

- the sensor is trusted hardware
- the software and and firmware are open source and can be verified by means of reproducible builds [1]
- the adversary has no physical access to the sensor hardware and has no possibility to

influence the physical quantities being measured.

Assuming the above, we can take advantage of the fact that the hash of the highest block in a public blockchain can't be known prior to that block having been mined. But the hash is publicly known and trusted ever after (or for as long as the blockchain is trusted). If we now enrich our sensor data frame with that hash before signing it using the Trusted Platform Module (TPM) [7], we have proven prior inexistence. If we then add the hash of our signed frame to a transaction on the same blockchain, we get a proof of origination (PoO). The combination of the two proofs results in a trusted time range of origination. Figure 1 shows a block diagram for such a platform.

The precision of this time range depends on the block time of the chosen blockchain. In the best case, the precision is the time between two blocks. This would be around 10 min in the case of Bitcoin or 1min in the case of Ethereum [4] but could be as low as 10s [6][5].

In order to be sure that the sensor data has really been handeled as described (and has not i.e. been buffered to delay the timestamp), it is necessary to open source both software and firmware and to have reproducible builds [1] running on the data acquisition hardware. This might need to be extended by using *Trusted Execution Environments* [2]. The security concept for the data acquisition platform is beyond the scope of this document however.

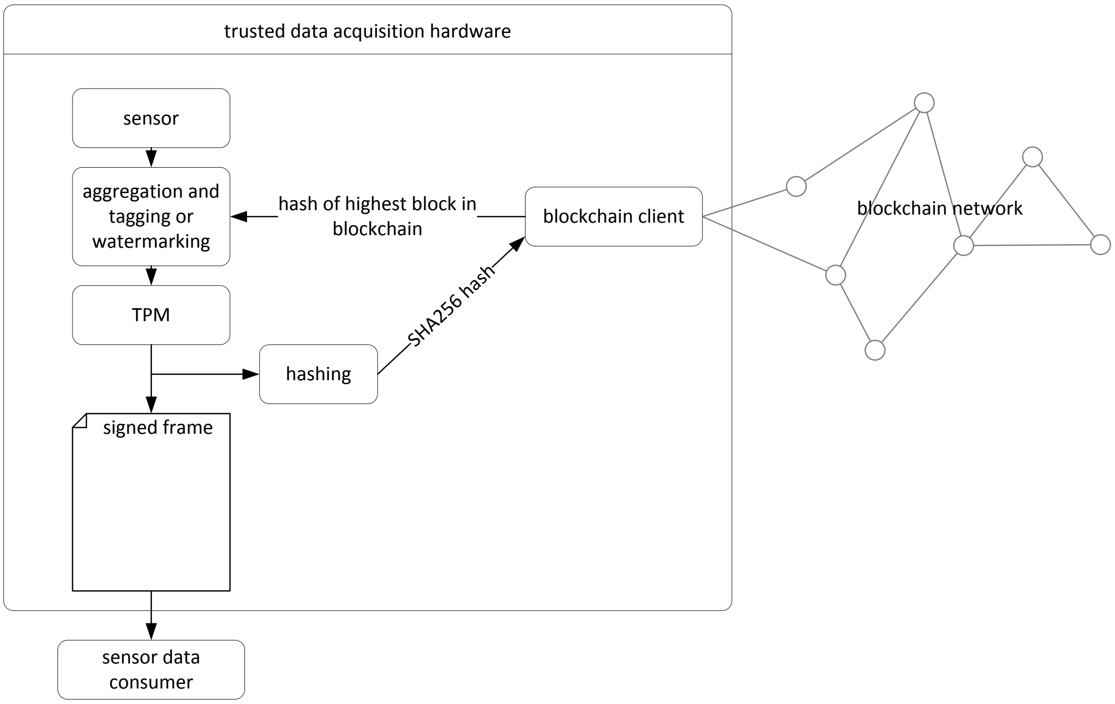
trusted data acquisition hardware
sensor
aggregation and tagging or watermarking
hash of highest block in blockchain
blockchain client
blockchain network
TPM
SHA256 hash
hashing
signed frame
sensor data consumer

Figure 1: Blockdiagram for a data acquisition platform featuring trusted timestamping.

4 About Supercomputing Systems AG

Supercomputing Systems AG is an engineering company in the fields of high performance computing systems, communication systems, algorithm development and big data solutions. Engineering expertise ranges from software design and development (enterprise solutions as well as embedded software), electronics development, design of distributed systems, to high-end measurement technology. SCS AG has 24 years of experience as an engineering company in different markets such as high performance computing, energy, public transportation, industrial application, automotive. The company has over 95 engineers in the fields of electrical engineering, software engineering, physics and data analysis.
Based on its experience Supercomputing Systems AG offers engineering services in this fast-growing field of blockchain technology.

References

[1] Reproducible builds. https://reproducible-builds.org/.

[2] Trusted execution environment specification. http://globalplatform.org/specificationsdevice.asp.

[3] M. Araoz and E. Ordano. http://www.proofofexistence.com, 2013.

[4] V. Buterin. Ethereum whitepaper, 2013.

[5] V. Buterin. Toward 12s block times. https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/, 2014.

[6] V. Buterin. On slow and fast block times. https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/, 2015.

[7] T. C. Group. https://trustedcomputinggroup.org/tpm-main-specification/, 2011.

[8] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.