Technical Disclosure Commons

Defensive Publications Series

October 30, 2018

ENSURING TRUSTWORTHINESS OF INCIDENT EVIDENCE DATA GENERATED BY THINGS

Jay Johnston

David White

Magnus Mortensen

Justin Muller

Recommended Citation

Johnston, Jay; White, David; Mortensen, Magnus; and Muller, Justin, "ENSURING TRUSTWORTHINESS OF INCIDENT EVIDENCE DATA GENERATED BY THINGS", Technical Disclosure Commons, (October 30, 2018)
https://www.tdcommons.org/dpubs_series/1619

ENSURING TRUSTWORTHINESS OF INCIDENT EVIDENCE DATA GENERATED BY THINGS

AUTHORS:
Jay Johnston
David White
Magnus Mortensen
Justin Muller

ABSTRACT

Techniques are provided that leverage blockchain technology to ensure that evidence that is recorded by things of an incident is saved and shared with interested parties in a method that ensures the trustworthiness of the evidence data. A thing, a local fog router, or a central integrity service might save evidence trustworthiness data to a blockchain. Complementary methods are also provided that bolster the solution's applicability to connected cities and other implementation opportunities.

DETAILED DESCRIPTION

Things (e.g., vehicles, traffic lights, Unmanned Aerial Vehicles (UAVs), rolling robots, caregiver robots, security cameras, etc.) have sensor capabilities and many of them are constantly active and recording. However, many have a limited amount of memory to save data recordings. These devices typically have some form of a rolling buffer which contains data for a predetermined amount of time. If some incident occurs, like a car accident, it is very important that all available sensor evidence from all available devices be saved to help investigate the incident for legal and technological reasons. This becomes the collection of facts around the time of the incident.

But providing the evidence is useless if the data cannot be trusted. The evidence must not be modified. The information cannot hold up in court if there is a dispute about what happened.

As described herein, multiple devices (owned by different entities) observe/record an incident to upload their data to a plethora of places, while also maintaining an open and trustworthy record of the request, the actual data, and where that data was stored. For example, a device that records evidence data (e.g., a camera on a street light, a dash-cam, etc.) can respond to a request for evidence data by uploading their saved evidence information to a location of their choosing. For instance, in the event of a crash, a driver's smart devices may upload their data to the data stores of the driver's insurance company, while the street light might upload data to the municipality's servers. A record of this request, the location of where the data is stored, and a hash of the data may be recorded in an evidentiary blockchain specified by the beacon. This allows multiple parties to verify the request and the source, as well as validate that the data has been unaltered.

Upon receiving a beacon request for evidence data about an event, things may then upload the relevant evidence data they have to a specific location. The authenticity of the data (e.g., timestamps, the device that generated the data, the evidence data itself, etc.) is ensured by the thing that generated the data writing metadata (including a hash of the data) to a public blockchain.

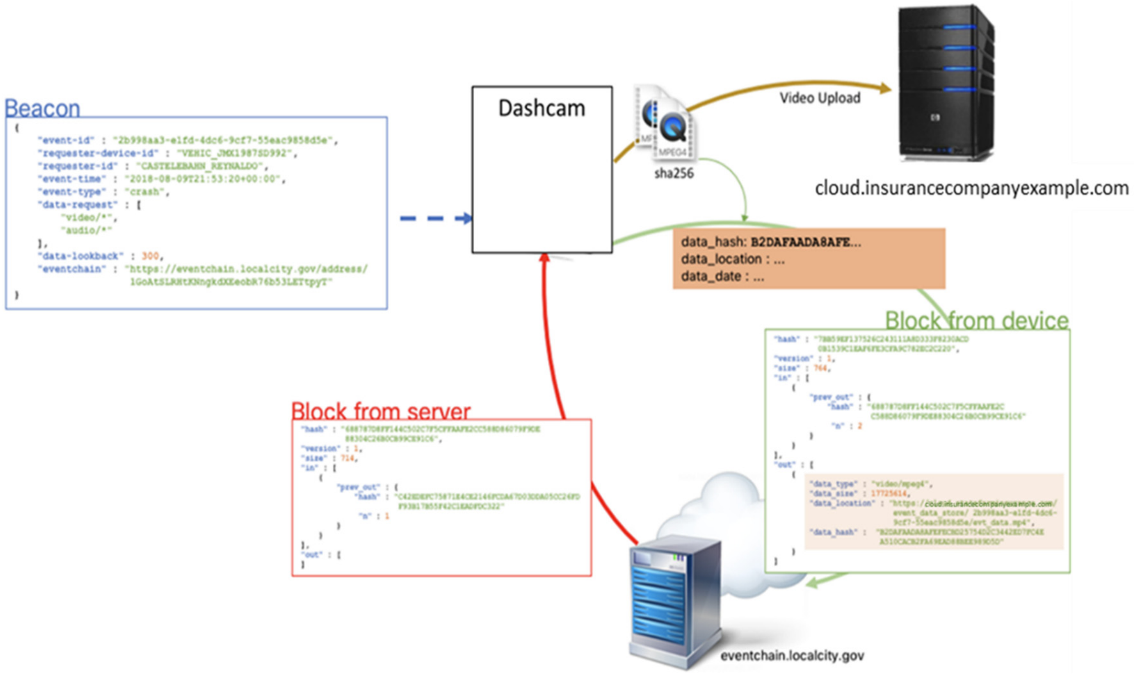
The uploaded data may optionally have a header or marking set on the traffic, thereby indicating to intermediary devices (e.g., devices on path from the device to the secured upload location such as routers, etc.) that they should update the blockchain as well. This indicates that they received and passed on the data.

In addition, or in a complementary fashion, a local fog device may receive the evidence data on behalf of the device and write it to the blockchain. The local fog device may broadcast the beacon requesting data. It may also relay the request for data to other beacons, allowing for the request for data to propagate throughout a connected city, for example.

The beaconing device that requests the data may be itself provisioned on the blockchain to help ensure the integrity of the request for data. This prevents malicious data requests (e.g., from unauthorized parties). Evidence for the same incident provided by different sources is consolidated by a central service that de-duplicates and weaves the evidence together to tell the story of what occurred and from different perspectives.

In a first example method, things that generate evidence save evidence authenticity information to the blockchain. When the beacon is announced requesting evidence, along with the metadata about the evidence request (type/time/location), the beacon includes the location of where to store this information on a blockchain for this event. In some instances this may be provided by the municipality in which the event took place (e.g., a smart city). If the device that receives the beacon is capable, it may directly write authenticity information to the blockchain. The data stored within the block may include an assortment of metadata about the evidence provided. Some examples may include the file type, size, date, and hash of the data being saved. By writing this data to the blockchain, the act of uploading the data is immutably logged along with key characteristics of that data. By also providing information about where to access this data, individuals with authority to access the data can obtain it as legally allowed.

Figure 1 below illustrates the first example method.



```
{
    "event-id" : "2b998aa3-e1fd-4dc6-9cf7-55eac9858d5e",
    "requester-device-id" : "VEHIC_JMX1987SD992",
    "requester-id" : "CASTELEBAHN_REYNALDO",
    "event-time" : "2018-08-09T21:53:20+00:00",
    "event-type" : "crash",
    "data-request" : [
        "video/*",
        "audio/*"
    ],
    "data-lookback" : 300,
    "eventchain" : "https://eventchain.localcity.gov/address/
                    1GoAtSLRHtKNngkdXEeobR76b53LETtpyT"
}
```

```
"hash" : "7B859EF137526C243111A80333F8230ACD
          0B1539C1EAF6FE3CFA9C782BC2C220",
"version" : 1,
"size" : 764,
"in" : [
    {
        "prev_out" : {
            "hash" : "688787D8FF144C502C7F5CFFAAFE2C
                      C588D86079F9DE88304C26B0CB99CE91C6"
             "n" : 2
        }
    }
],
"out" : [
    {
        "data_type" : "video/mpeg4",
        "data_size" : 17725614,
        "data_location" : "https://cloud.insurancecompanyexample.com/
                           event_data_store/ 2b998aa3-e1fd-4dc6-
                           9cf7-55eac9858d5e/evt_data.mp4",
        "data_hash" :  "B2DAFAADA8AFEFECB02575402C3442ED7FC4E
                        A510CACB2FA69EAD88BEE989050"
    }
]
```

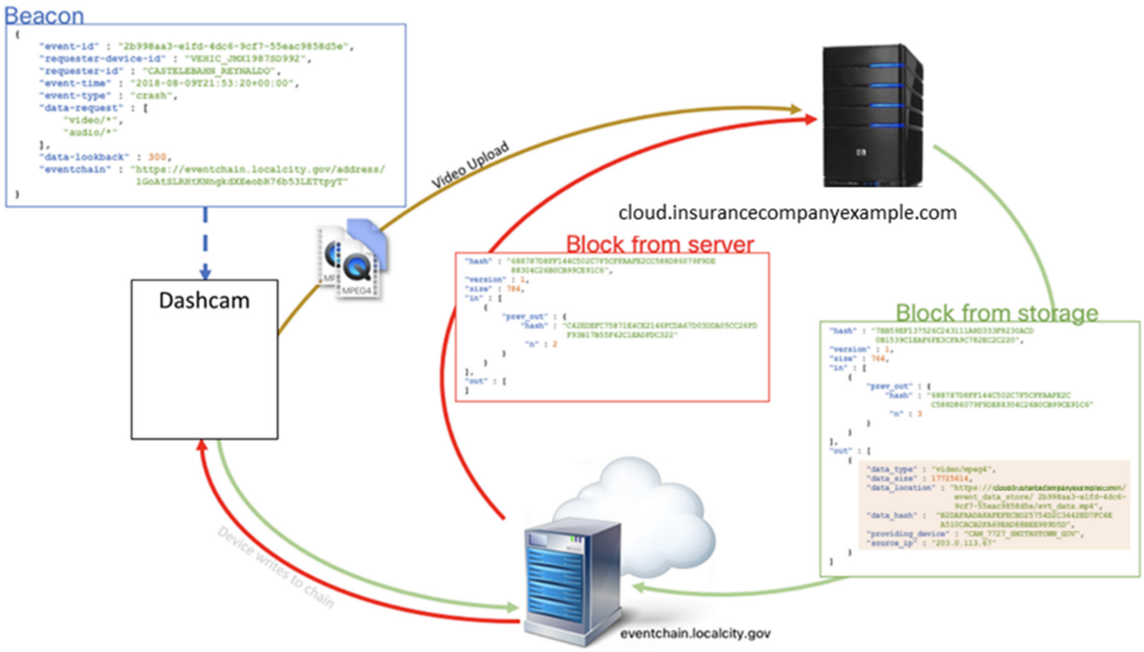
```
"hash" : "688787D8FF144C502C7F5CFFAAFE2CC588D86079F9DE
          88304C26B0CB99CE91C6",
"version" : 1,
"size" : 714,
"in" : [
    {
        "prev_out" : {
            "hash" : "C42EDEFC75871E4CE2146FCDA67D0300A05CC26FD
                      F93817B55F42C1EAD8DC322"
             "n" : 1
        }
    }
],
"out" : [
]
```

Figure 1

In a second example method, a central upload location acts as an integrity service by writing evidence authenticity information to the blockchain. In this situation, the device that receives the beacon has uploaded the data to its predetermined upload location. As part of that upload, the information about the beacon request, such as the event chain location, is also provided. In order to maintain the recorded chain of custody, the receiving server also writes data about the acquired evidence to the specific chain. The data stored within the block may include an assortment of metadata about the evidence provided including data about the device that provided that data. In addition to attributes similar to that mentioned in the first example method, key aspects of the device is logged such as the Internet Protocol (IP) address, serial number, Unique Identifier (UID), timestamp of data request, who made the data request, information on where that data was sent (the server) with timestamp information, etc. By writing this to the blockchain, the act of uploading the data is immutably logged as well as key characteristics of that data and its provider.

In addition, if there are multiple pieces of data being recorded to this blockchain for this event, the central upload location can also write additional metadata about the data it receives such as records of duplicate data, the rate of data, and/or diversity of the data (e.g., videos, audio files, photos, etc.). This central upload system may also leverage different algorithms and systems to derive an order of events that helps tell the story of what happened around a given event.

Figure 2 below illustrates the second example method.



```
{
    "event-id" : "2b998aa3-e1fd-4dc6-9cf7-55eac9858d5e",
    "requester-device-id" : "VEHIC_JMX1987SD992",
    "requester-id" : "CASTELEBANN_REYNALDO",
    "event-time" : "2018-08-09T21:53:20+00:00",
    "event-type" : "crash",
    "data-request" : [
        "video/*",
        "audio/*"
    ],
    "data-lookback" : 300,
    "eventchain" : "https://eventchain.localcity.gov/address/
                    1GoAtSLRHtKNngkdXEeobR76b53LETtpyT"
}
```

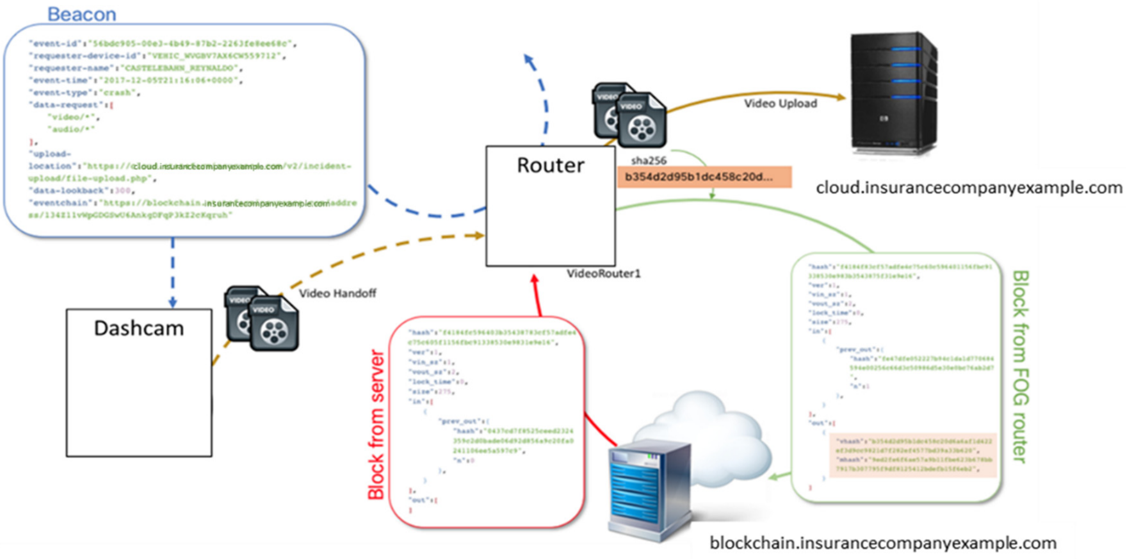
```
"hash" : "68878708FF144C502C7F5CFFAAFE2CC588D86079F9DE
          88304C26B0CB99CE91C6",
"version" : 1,
"size" : 784,
"in" : [
    {
        "prev_out" : {
            "hash" : "C42EDEFC75871E4CE2146FCDA67D0300A05CC26FD
                      F93B17B55F42C1EAD8DC322"
             "n" : 2
        }
    }
],
"out" : [
]
```

```
"hash" : "7BB59EF137526C243111A80333F8230ACD
          0B1539C1EAF6FE3CFA9C782BC2C220",
"version" : 1,
"size" : 764,
"in" : [
    {
        "prev_out" : {
            "hash" : "68878708FF144C502C7F5CFFAAFE2C
                      C588D86079F9DE88304C26B0CB99CE91C6"
             "n" : 3
        }
    }
],
"out" : [
    {
        "data_type" : "video/mpeg4",
        "data_size" : 17725614,
        "data_location" : "https://cloud.insurancecompanyexample.com/
                           event_data_store/ 2b998aa3-e1fd-4dc6-
                           9cf7-55eac9858d5e/evt_data.mp4",
        "data_hash" :  "B2DAFAADA8AFEFECBD25754D2C3442ED7FC4E
                        A310CACB2FA69EAD88BEE989050D",
        "providing_device" : "CAM_7727_SMITHSTOWN_GOV",
        "source_ip" : "203.0.113.67"
    }
]
```

Figure 2

In a third example method, a local fog device receives the evidence and saves the authenticity information to the blockchain. In situations where the evidence generating devices report back to other nodes (such as city wide security cameras connecting to fog routers), upon receipt of the beacon those local fog devices re-broadcast the beacon requesting data to nearby evidence gathering devices, effectively relaying the request for data to other devices, allowing for the request for data to propagate throughout a connected city, for example. As they handle actions related to the beacon (such as uploading data on behalf of the connected device, or relaying the broadcast beacon), these devices write to the provided blockchain information about what they do and the handled data. Fog devices may perform localized analysis of data to discard unneeded data. For example, if the request was to capture a red car during a time period, and that beacon was sent to every traffic camera in a geographical area, then the local fog router could request that data from every camera. Only the cloud service (and blockchain) data which matches the request may be sent in which a red car is spotted in the video footage.

Figure 3 below illustrates the third example method.



```
"event-id":"56bdc905-00e3-4b49-87b2-2263fe8ee68c",
"requester-device-id":"VEHIC_WVGBV7AX6CW559712",
"requester-name":"CASTELEBAHN_REYNALDO",
"event-time":"2017-12-05T21:16:06+0000",
"event-type":"crash",
"data-request":[
    "video/*",
    "audio/*"
],
"upload-
location":"https://cloud.insurancecompanyexample.com/v2/incident-
upload/file-upload.php",
"data-lookback":300,
"eventchain":"https://blockchain.insurancecompanyexample.com/addre
ss/134Z11vWpGDGSwU6AnkgDFqPJkZ2cKqruh"
```

```
"hash":"f4184fc596403b35438783cf57adfe4
e75c605f1156fbc91338530e9831e9e16",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":275,
"in":[
    {
        "prev_out":{
            "hash":"0437cd7f8525ceed2324
            359c2d0bade06d92d854a9c20fa0
            241106ee5a597c9",
            "n":0
        },
    }
],
"out":[
]
```

```
"hash":"f4184f83cf57adfe4e75c60c596401156fbc91
33853 0e983b3543875f31e9e16",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":275,
"in":[
    {
        "prev_out":{
            "hash":"fe47dfe052227b94c1da1d770684
            594e00256c46d3c50986d5e30e0bc76ab2d7
            ",
            "n":1
        },
    }
],
"out":[
    {
        "vhash":"b354d2d95b1dc458c20d6a4af1d422
        ef3d9cc9821d7f202ef4577bd39a33b620",
        "mhash":"9ed2fe6f6ae57a9b11fbe623b678bb
        7917b307795f9df8125412bdefb15f6eb2",
    }
]
```

Figure 3

The beaconing device that requests the data may be provisioned on the blockchain to help ensure the integrity of the request for data. This prevents malicious data requests (e.g., from unauthorized parties).

This solution derives a significant and unique benefit from incorporating blockchain technologies. Blockchain is critical because it removes the need to trust any one party. In this case, the data in question can be highly valuable and can be both created and stored by many different parties. The data is used to drive large financial decisions (e.g., insurance, city design, traffic management, etc.) and it may also be used during civil or criminal prosecutions. All of this added together means that there is both opportunity and, in some cases, a large incentive to falsify the data after it is created (e.g., from private companies).

One solution to this trust problem is to use blockchain technology. Effectively, rather than any one company owning the data, it may be widely published to many entities.

This demonstrates the immutability of blockchain: because everyone knows what the data is, no one party can change it.

Additionally, blockchain is also uniquely suited to solving this problem because of the element of time. In many cases, the fact that data on a blockchain is immutable does not really help, because there is no way to prove the quality of the data in the first place when it was put on the chain. If false data is uploaded to a blockchain, all the blockchain can do is make that false data immutable. However, applied to the techniques described herein, that lock into time is a significant advantage. This disclosure targets events such as car crashes that are by their nature unexpected. That means nearly all tampering and removal of data is expected to occur after the incident. In the moment of an incident, there is no time to track down all sensors and cameras in an attempt to alter data, and then a second later all that data is locked into that moment of the blockchain, and it becomes immutable. Effectively, the nature of the problem to be solved removes one of blockchain's greatest vulnerabilities.

Finally, by using blockchain, the burden of proving legal access rights to the data at the moment of generation is removed. This means that new and larger quantities of data may be both available and trustworthy. In one example, a crime is committed and only a private camera captures the event. At the time of the crime, the city might request access to the video recording, but the owner may refuse on privacy grounds. This means that the city has to obtain a warrant and spend time figuring out whether they have a legal right to the data. That time gap is a hole in the chain of custody, where the data may be altered or destroyed (due to being overwritten). However, with the blockchain solution, that video system may save a copy of the video locally or a location controlled by the private party, and send a hash of the video to the blockchain. That effectively locks the contents from undetected alteration, because if the video is altered the hash would change and no longer match the immutable hash on the blockchain. This gives the city the time they need to resolve the legal questions surrounding access to the data. If the city does obtain access, when the prosecutor views the video they will be able to check that the hash matches, and have proof that the video is unaltered. This may open the door to a whole new level of trusted access to data for the city.

Today, when a traffic accident or other disturbance occurs, city police may be dispatched to the scene. They may canvas the area and ask for eyewitness accounts. They might also identify any nearby cameras, and collect the recordings manually, if they can. The city is then legally responsible for maintaining the chain of custody of that evidence. This may be a resource intensive and costly exercise, as all the data collected must be accounted for and protected every moment. This process may be virtualized and allow the smart city offering to include the ability to both collect and guarantee the authenticity and chain of custody for all data. With this solution, all data can be generated and stored as normal, either on private or public servers. When accessing the data later, regardless of where it is stored, the city can have assurance that it has not been altered because the hashes on the public blockchain match. By simplifying the chain of custody process, and by opening up the possibility for data to be stored on private servers in a legally trustworthy way, costs for the city are reduced and new data opportunities become available.

For maximum effectiveness of the solution, the data may be added to the blockchain as close as possible to the moment of its creation. Ideally that means each device should write its own data to the blockchain. However, most of the devices do not have the required onboard compute power and flexibility to implement a system like this. Therefore, the next best option is to write the data to the blockchain the moment it leaves the device. When data leaves the device, it first touches the network. Therefore, the network itself is the best place for this solution to exist. Furthermore, by building the solution on the network, rather than on millions of different kinds of devices, a cost-effective and simple solution may be provided at a city level.

In summary, techniques are provided that leverage blockchain technology to ensure that evidence that is recorded by things of an incident is saved and shared with interested parties in a method that ensures the trustworthiness of the evidence data. A thing, a local fog router, or a central integrity service might save evidence trustworthiness data to a blockchain. Complementary methods are also provided that bolster the solution's applicability to connected cities and other implementation opportunities.