### Blockchain as a warehouse for medical data in emergency situations with biometics based access

### Abstract

This paper discusses how the use of Blockchain advances healthcare emergency services, and proposed system architecture and data structures to build this system. ONC, PMI and PCOR can review this proposal for their interoperability needs.

### Intro

The patient can be delivered to an emergency room significantly damaged, unconscious and without documents. For example, they can be victims of car accidents, wounded police officers or militias, firefighters, etc.

 And in emergency needs, it is vital to obtain information about the patient quick and from a trusted, high-available source, and access to this source must be unlocked only If patient body is presented in the medical facility.

In this article the public blockchain is proposed to store critical emergency medical data, and retrieve it by biometric credentials.

### What is critical emergency information?

This information is needed for emergency help, and can save lives. This will not give away personal name or employment history. This is only info about blood group, allergies to antibiotics or pain relief drugs (like Novocain), and so on. In addition, there can be reference (url, phone) to source, which can be used to provide additional or personal information by request.

In another words – this information helps save life and provide emergency service, but do not disclose personal private information.

Personal private information can be requested by a reference, provided among the emergency data.

### Why biometric access?

Patients can be delivered to an emergency room unconscious, without documents or witnesses. Therefore, there is impossible to obtain trusted emergency information, which is critical. Medical stuff must have ability to get this info by body presence only. So, biometric is the ideal solution to gain access. We assume the best biometric method is toe fingerprint, but there are other possible solutions, too.

Why is toe fingerprint?

* Usually toes are better protected, than fingers, so there’s a better chance to use them in an emergency.
* Toes aren’t shown as commonly as fingers, so there is a lesser chance of info being leaked, such as it was here: https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

### Why blockchain?

Blockchain is a world-wide trusted distributed database with high availability. Trust is provided by the consolidated efforts of independent miners. The following is a list of the advantages of this solution:

* **World-wide availability.** Patient able get help anywhere in the world.
* **High availability.** Data can be retrieved quickly and efficiently anywhere in the world.
* **Fault tolerant, Independent from external sites and services.** Data retrieval can be performed from a local blockchain copy, even if any external servers or even if the Internet connection is down.
* **Trust to a blockchain is independent.** It is supported by the consolidated efforts of independent miners, and data cannot be altered or blocked by some authority or malicious actors.

### Implementation

We propose to store the medical data in the public blockchain in encrypted form. Biometric data will be used for retrieve medical data and decrypt it. Thus, the retrieval process will be executed in following stages:

1. Collect biometric data (toe fingerprint, or another)
2. Compute decrypt key [1] (using cryptographic hash function, i.e. sha256)
3. Compute search key [2] (using cryptographic hash function, i.e. sha256)
4. Search associated record in the blockchain by key[3] and retrieve it
5. Decrypt medical data from the record [4] by the key [2]
6. Use medical data to help patient, or get reference to retrieve additional data.

Using this mechanism, all other users will be unable to retrieve medical data without biometric info, as blockchain analysis will be ineffective. In addition, since the hashes are not reversible, any attackers will be unable recover the decrypt key [2] from the public search key [3].

Each piece of medical data is recorded in the blockchain as a “key->value” pair, where:

* Key: search key [3]
* Value: Medical data, encrypted with key [2].

These records will be stored in the Name-Value Storage (NVS) of the Emercoin public blockchain.

### Why Emercoin?

* Emercoin contains a built-in Name-Value Storage (NVS) subsystem, which allows the storage of blockchain pairs “key->value”. See details: <http://emercoin.com/DNS_and_Name-Value_Storage>
* Emercoin is a mature blockchain for industrial applications, with priority in security and reliability.
* Compatible with industry security standards: X.509, PKCS#11, PKCS#12, RFC2818
* NVS interface is a standard JSON RPC, and is compatible with standard Bitcoin applications and samples. Sp, this is easy integrate it into medical infosystems using standard libraries.
* The Emercoin Group is the author of this proposal, and will provide any needed assistance to implement this solution into your infosystems.

### Medical data format

Medical data is in text file, containing key=value pairs, for example:

**BloodGroup=AB**

**Allergy=Penicillin, Novocaine**

**Disease=HBV, HIV**

**Tel=+1-555-555-5555**

**Url=https://www.meddata.gov?md=%s**

In this example, field **Url** contains the template to retrieve full patient info. An authorized medical facility can extract it secure using emcSSL authorization mechanism: http://emercoin.com/EMCSSL

Optionally, this record can be signed with DPO signature of some authorized medical institute, which can also be included into medical data. See details: http://emercoin.com/content/EMCDPO.pdf

For example:

**Signer=dpo:Holy\_Cross\_Hospital**

**Signature=IBf2SnBGQHQwwCR1XCc6bzhXkQOpdpfCecmDahfiACP/aC5T6jmw2UOBgZQ/8**

The file is compressed with gzip and encrypted with program openssl. Proposed algorithm is **salted AES CBC** – as same as used in EMC InfoCard records. Binary data is uploaded into Emervcoin NVS. It is possible to use other cryptoalgorithms and block chaining method, as described in the FIPS\_81 specification: <http://csrc.nist.gov/publications/fips/fips81/fips81.htm>