doi:10.20396/revpibic2620181094

XXVI Congresso de Iniciação Científica Unicamp
17 a 19 de outubro Campinas | Brasil

On-block certs: Blockchain-based lightweight digital certificates

Nícolas F. R. A. Prado*, Marco A. A. Henriques.

Abstract
The current method for verifying the status of digital certificates relies on the user checking it against a list provided by the Certification Authority (CA). This verification can fail due to problems on the CA's site or attacks against it. We developed a proof-of-concept for a system that stores and retrieves a lightweight version of digital certificates from the Ethereum blockchain. By doing that we created a tight link between certificates and their status and also reduced their size by taking advantage of the blockchain transaction structure.

Key words:
blockchain, digital certificate, Ethereum

Introduction

Digital certificates[1] are used daily to provide security over the internet. Nevertheless, the current system requires checking certificates against a Certificate Revocation List available on the Certification Authority (CA), which makes the process cumbersome and subject to failures. By using a blockchain, it is possible to store the certificates along with their status in a distributed and more tamper-resistant manner[2].

We propose a system where the user's information is stored in the data field of a transaction on the Ethereum's blockchain[3], sent from the Certification Authorities address to the user's. By doing this, we can make the certificate lighter, by omitting the CA's signature and the user's public key, since the first is present in the transaction's structure and the second can be associated to the user's blockchain address. Furthermore, the status of the certificate is stored in the balance of the address, facilitating the process of checking the revocation status. This lightweight version of a standard digital certificate, that is based on the structure of a transaction of the blockchain is what we call an on-block cert.

Results and Discussion

To provide a full proof-of-concept, the following use cases were established for the system:

1. Key pair generation
2. On-block cert creation
3. On-block cert query
4. On-block cert revocation
5. Message signing
6. Message signature confirmation

The first use case is responsible for generating a new cryptographic key pair, which will be used in the other use cases for generating an address for holding the on-block cert as well as signing messages and verifying the signatures.

Cases 2 and 3 correspond respectively to storing and retrieving the on-block cert from the blockchain. The first creates an on-block cert with the user's information, an operation that is guaranteed by the CA and that is coupled with the user's address on the blockchain, while the second checks for a given address and returns whether or not it contains an on-block cert. In case it does, it also returns the user's information and the certificate status and validity.

The fourth one is to be used in case the private key of the key pair is compromised. It updates the status of the certificate to be revoked by altering the address' balance, which makes it no longer valid,

Case 5 is for signing a message. It uses the private key from the generated key pair to produce a signature for the message, which guarantees its authenticity. The message is supplied by a file which can be of any type, and the generated signature is stored as a separate .sig file.

On the other hand, case 6 is responsible for verifying the signature of a message. It does that by interfacing with the blockchain and checking if the address associated with the key that signed the message has a valid on-block cert.

Conclusions

This system shows that, by using on-block certs instead of the standard certificates, it is possible to have lighter certificates, tightly coupled with their status and with integrity assured by blockchain's transactions and distributed nature. Moreover, as the on-block certs can be obtained from and/or verified securely at any one of the many blockchain network nodes, the proposed system is more robust and fault tolerant than a single CA network site.

As future works, we can point out the integration of this certification scheme with different kinds of software that can benefit from digital signatures as, for example, e-mail clients, pdf editors and word processors.

Acknowledgement

This research was funded by the PIBIC program, created and maintained by CNPq.

---

[1] Paar, C. and Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners;* Springer, 2010

[2] Antonopoulos, A. M. *Mastering Bitcoin: unlocking digital cryptocurrencies,* 2nd ed.; O'Reilly Media Inc, 2017

[3] Wood, G. *Ethereum: A secure decentralized generalized transaction ledger.* http://gavwood.com/Paper.pdf (accessed Jul 12, 2018)