

Replacing Public Key Infrastructures (PKI) by blockchain IoT devices security management

Auteur : Champagne, Loïc

Promoteur(s) : Leduc, Guy; 12788

Faculté : Faculté des Sciences appliquées

Diplôme : Master en sciences informatiques, à finalité spécialisée en "computer systems security"

Année académique : 2020-2021

URI/URL : <http://hdl.handle.net/2268.2/11608>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.



MASTER THESIS SUMMARY

Champagne Loïc: "Replacing Public Key Infrastructures by blockchain IoT devices security management."

Supervisors: Prof. G. Leduc, E. Tychon (Cisco)

M.sc. in Computer Science

University of Liège

Academic year 2020-2021

On the Internet, Public Key Infrastructure (PKI) is the most advanced credential management system. However, the standard PKI relies on certificate authorities (CAs) which have delivered certificates to the wrong people in the past for questionable reasons. Indeed, these CAs represent a corruptible central point that this work aims to remove. This was done by adapting the PKI to a decentralized framework based on blockchain smart contract. This solution is essentially targeted toward the Internet of Things (IoT) that currently lacks a scalable system for managing keys and identities (i.e., a standard PKI framework). Unlike CA-based PKIs, our framework delivers auditability natively which provides a proof of the framework integrity. In order to adequately test our solution, we designed and implemented a proof of concept. The smart contract was written in solidity and is deployed on the Kovan test net. After testing our solution on an Ubuntu core virtual machine, we found that the solution has a very small footprint and is therefore adapted to the IoT ecosystem.

Keywords: IoT, PKI, Decentralized, Smart contract, Blockchain, Authentication, Security.