REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHECHE SCIENTIFIQUE

Centre de Recherche Sur l'Information Scientifique et Technique

MEMOIRE

Présenté en vue de l'obtention du diplôme de Post Graduation Spécialisé en Sécurité Informatique

Thème

Application de Blockchain pour la sécurisation des données de santé

Présenté par :

- M. ABBAS Samir
- M. OUIKHLEF Rabeh Mohammed

Devant le jury composé de :

- M. DJEDJIG Nabil **Président**
- M. HADJAR Samir **Examinateur**
- M. AMIRA Abdelouahab **Examinateur**

Promotion : 2017/2018

Résumé

La protection des données de santé personnelles est devenue un enjeu majeur pour garantir le respect de la vie privée. Et par là, se prémunir de tout risque de monnayage des données, de ciblage ou de discriminations économiques et sociales. Ces risques sont accentués par la prolifération des systèmes d'e-santé intégrant les technologies de l'Internet des Objets, du Cloud et des bases données distribuées. S'ajoute à cet environnement, le risque porté par le degré de confiance à accorder aux fournisseurs de services, en termes de capacité technique à assurer la sécurité des données mais également en termes de responsabilité morale, ceci, même dans un contexte législatif de plus en plus contraignant. L'un des moyens de réduire ces risques est centré sur des processus de protection et de contrôle d'accès aux données centré sur le propriétaire des informations. La blockchain offre des possibilités prometteuses dans ce sens, néanmoins, ces approches font encore face à beaucoup de défis pour arriver à des solutions réalistes. Notre travail est destiné aux spécialistes de la technologie de l'information, et à tous ceux qui travaillent sur ou avec les technologies de contrôle d'accès, et qui sont curieux d'en savoir plus sur la blockchain et son impact sur le contrôle d'accès au données personnelles.

Mots clés: Vie privée, E-santé, Blockchain, Contrôle d'accès, Ethereum, Hyperledger, Smart contracts.

Abstract

The protection of personal health data has become a major issue to ensure respect for privacy. And by doing so, protect against any risk of data monetization, targeting or economic and social discrimination. These risks are exacerbated by the proliferation of e-health systems integrating Internet of Things, cloud and distributed database technologies. In addition to this environment, there is the risk of the degree of trust to be placed in service providers, in terms of technical capacity to ensure data security but also in terms of moral responsibility, even in an increasingly restrictive legislative context. One way to reduce these risks is to focus on protection processes and data access control focused on the information owner. The blockchain offers promising opportunities in this direction; however, these approaches still face many challenges in arriving at realistic solutions. Our work is aimed at information technology specialists, and at all those who work on or with access control technologies, and who are curious to know more about blockchain and its impact on access control to personal data.

Keywords: Privacy, E-Health, Blockchain, Access control, Ethereum, Hyperledger, Smart contracts.

Table des matières