

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
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 | Examineur |
| - M. AMIRA Abdelouahab | Examineur |

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 aux données personnelles.

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

Abstract

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.

<i>Table des matières</i>	
Remerciements	II
Résumé	III
Abstract.....	IV
Table des matières	V
Liste des figures.....	VIII
Liste des tableaux	X
Terminologie	XI
Introduction générale.....	1
Chapitre I : Contrôle d'accès au DMP	3
1. Introduction	3
2. Définition d'un DMP	3
2.1. Les modèles de DMP	4
2.2. Les avantages des systèmes DMP	5
2.3. Les défis des systèmes DMP	5
2.4. Les différents types de dossier médical	5
3. Sécurité du DMP	6
3.1. Propriétés de sécurité.....	6
3.2 Moyens de sécurité.....	7
3.2.1 Contrôle d'accès.....	7
3.2.2 Contrôle d'accès dans les cas d'urgences	8
3.3. Protection des données personnelles du DMP	8
3.3.1. Définition.....	8
3.3.2. Spécificité des données personnelles relatives au domaine de la santé	9
3.3.3. Protection des données personnelles et législation.....	9
3.3.4. Protection des données personnelles et Confidentialité	10
3.3.5. Propriétés de la protection des données personnelles.....	10
4. Modèles classiques de contrôle d'accès	10
5. Le Consentement	11
6. Conclusion.....	11

Table des matières

Chapitre II : Principes de la technologie Blockchain.....	12
1. Introduction	12
2. Définition.....	12
3. Caractéristiques de la blockchain	13
4. Fonctionnement	15
5. Concepts de la blockchain	16
5.1. Structure d'une chaîne de block	16
5.2. Structure d'un bloc	18
5.3. Entête du bloc.....	18
5.4. Arbre de Merkle	19
5.5. Transaction	20
5.6. Horodatage	22
5.7. Minage.....	23
5.8. Réseau de la blockchain	24
5.9. Preuve de travail.....	24
6. Types de blockchain.....	29
6.1. Publique	29
6.2. Privée	30
6.3. Choix de la bonne blockchain	32
7. Mécanismes de consensus	33
7.1. Généralités.....	33
7.2. Consensus utilisés dans les blockchains publiques.....	33
7.3. Consensus utilisés dans les blockchains privées.....	36
7.4. Étude comparative.....	42
8. Smart contracts	43
9. Opportunités de la Blockchain au contrôle d'accès des ressources	44
10. Applications de la Blockchain.....	45
11. Plateformes blockchain Ethereum&Hyperledger.....	47
11.1. Ethereum	47
11.1.1. Présentation.....	47
11.1.2. Protocole	48

Table des matières

11.1. 2.1. Comptes.....	49
11.1. 2.2. Nœuds	49
11.1. 2.3. Transactions et Messages.....	50
11.1. 2.4. Fonction de transition d'état Ethereum.....	51
11.1. 2.5. Exécution de code	52
11.1. 2.6. Minage.....	53
11.1. 2.7. Applications	54
11.1. 2.8. Systèmes de jetons	54
11.1. 2.9. Smart contracts.....	54
11.1. 2.10.DApp (Decentralized Application)	56
11.1. 2.11.DAO (Decentralized Autonomous Organization).....	57
11.2. Hyperledger	57
11.2. 1. Présentation.....	57
11.2. 2. Protocole	59
11. 2.1. Comptes.....	59
11. 2.2. Nœuds	60
11. 2.3. Transactions	60
11. 2.4. Minage.....	61
11. 2.5. Smart Contract	63
11.3. Comparaison entre Hyperledger&Ethereum	64
12. Conclusion.....	65
Chapitre III : Etude et annalyse des solutions existantes	66
1. Introduction	66
Partie I: Etude des solutions existant dans la littérature	67
1. Solutions.....	67
2. Tableaux comparatif.....	89
Partie II: Analyse et résultats.....	92
Conclusion.....	99
Conclusion générale.....	101
Bibliographie.....	103
Webographie	107