جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes
Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THÈSE DE DOCTORAT

Monsieur Khalid MRABET

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Samedi 11 Novembre 2023 à 10h30 au Grand Amphi à l'ENSIAS/l'ENSAM de Rabat

Intitulé de la thèse

Cryptographic Protocols and Blockchain for Establishing Trust and Security in Decentralized Networks

Devant le Jury composé de :

Président :

Pr. Hanan El Bakkali, PES, ENSIAS, Université Mohammed V de Rabat.

Directeur de thèse :

Pr. Faissal El Bouanani, PES, ENSIAS, Université Mohammed V de Rabat.

Co-Encadrant:

Pr. Hussain Ben-Azza, PES, ENSAM, Université Moulay Ismail, Meknès.

Rapporteurs :

Pr. Abdellatif Kobbane, PES, ENSIAS, Université Mohammed V de Rabat.

Pr. Moayad Aloqaily, Associate Professor, Mohamed bin Zayed Univ. of Artificial Intelligence, UAE

Pr. Omar Khadir, PES, FST-Mohammadia, Université Hassan II, Casablanca.

Examinateur :

Pr. Khalid El Makkaoui, PH, FPN, Université Mohammed Premier, Oujda.

UNIVERSITE MOHAMMED V - RABAT
ENSIAS

Résumé: Les primitives cryptographiques jouent un rôle essentiel dans l'assurance des communications sécurisées et la préservation des informations sensibles. Elles facilitent l'interaction et favorisent la coopération au sein des réseaux en offrant une protection contre l'accès non autorisé, l'usurpation d'identité et les atteintes à la vie privée. Leur rôle est d'autant plus important dans l'environnement de réseaux décentralisés, où l'autorité centrale chargée de surveiller le comportement des utilisateurs et d'appliquer la politique de sécurité fait défaut.

Ces primitives cryptographiques englobent des techniques telles que le chiffrement, la signature numérique, les fonctions de hachage, l'échange de clé et le partage de secret entre autres pour contrecarrer les accès non autorisés, garantir l'intégrité des messages et permettre la vérification d'identité. Il est important de souligner, cependant, que la cryptographie ne peut garantir l'exactitude des messages échangés ou leur véracité. Même les messages chiffrés et parfaitement authentiques peuvent contenir des informations erronées ou trompeuses. Par conséquent, la cryptographie, en elle-même, ne peut garantir la qualité des données transmises.

Pour remédier à cette limitation, les systèmes de gestion de réputation entrent en jeu, évaluant la fiabilité des sources de données et la véracité des informations transmises en fonction du comportement et des actions passés de ces sources. Les systèmes de réputation jouent ainsi, un rôle essentiel dans la réduction du risque de diffusion d'informations fausses ou trompeuses et dans le soutien à la prise de décisions éclairées.

De plus, les systèmes de réputation fonctionnent également comme des mécanismes de responsabilisation des utilisateurs au sein des communautés en ligne. Ces systèmes calculent la réputation d'un utilisateur en fonction des retours de la communauté sur ses actions. Au cas où l'utilisateur recevrait plusieurs retours négatifs, sa réputation diminuera, et peut faire l'objet de sanctions allant jusqu'à l'interdiction d'accès au réseau.

Un défi notable des systèmes de réputation réside dans la réticence des utilisateurs à fournir des retours négatifs en raison des craintes de représailles potentielles. Problème auquel les systèmes de réputation respectueux de la vie privée offrent une solution en calculant la réputation sans révéler les retours individuels. Ainsi, ces systèmes protègent la vie privée des utilisateurs tout en évaluant leur réputation. Il est à noter que de nombreux systèmes de réputation respectueux de la vie privée existants reposent sur des constructions centralisées et par conséquent ne sont

pas compatibles avec les environnements décentralisés. Certains de ces systèmes sont limités à des plates-formes spécifiques ou dépendent de tiers de confiance, ce qui peut être désavantageux. De plus, certains systèmes de réputation respectueux de la vie privée ne fournissent pas une protection suffisante dans des modèles adverses stricts ou nécessitent des ressources informatiques substantielles.

Dans cette thèse, nous étudions la sécurité des communications au sein de réseaux décentralisés et présentons des protocoles de gestion de réputation respectueux de la vie privée à l'échelle globale du réseau qui ne nécessitent pas de plates-formes spécialisées ni de tiers de confiance. De plus, ces protocoles préservent la vie privée dans divers modèles adverses et démontrent une efficacité pratique. Nous parvenons à cela grâce à l'utilisation du Blockchain et d'une gamme diversifiée de techniques cryptographiques, notamment le partage de secrets, les crypto-systèmes homomorphes additifs, le calcul multipartite sécurisé et les preuves Zero-Knowledge. Les résultats empiriques témoignent de l'efficacité des protocoles proposés.

Mots-clés : Blockchain, Calcul Multipartite Sécurisé, Confiance, Partage de Secret, Réputation, Système de Gestion de Réputation, Vie Privée.

Abstract: Cryptographic primitives are essential in ensuring secure communication and preserving sensitive information. They enable safe interaction and promote cooperation among network users by protecting against unauthorized access, identity theft, and privacy breaches. Their role becomes even more significant in decentralized network environments where a central authority for monitoring user behavior and enforcing security policies is lacking.

These cryptographic primitives encompass techniques such as encryption, digital signatures, hash functions, key exchange, and secret sharing, among others, to prevent unauthorized access, ensure message integrity, and enable identity verification. It is important to emphasize, however, that cryptography cannot guarantee the accuracy or truthfulness of exchanged messages. Even encrypted and perfectly authenticated messages can contain erroneous or misleading information. Therefore, cryptography, by itself, cannot ensure the transmitted data quality.

Reputation management systems come into play to fill this gap by assessing the reliability of data sources and the truthfulness of transmitted information based on past behavior and actions of these sources. Reputation systems help mitigate the risk of

disseminating false or misleading information and aid in making informed decisions.

Reputation systems also serve to hold users accountable in online communities. These systems calculate a user's reputation based on community feedback. If a user consistently receives negative feedback, his reputation will decline, and he may face penalties such as being banned from the network.

However, one challenge in reputation systems is the reluctance of users to provide negative feedback due to the fear of potential retaliation. Privacy-preserving reputation systems address this problem by calculating reputation without revealing individual feedback. These systems protect the privacy of users while still evaluating their reputation. It is worth noting that many existing privacy-preserving reputation systems rely on centralized constructs and, as a result, may not be compatible with decentralized environments. Some of these systems are limited to specific platforms or depend on trusted third parties, which can be disadvantageous. Additionally, some privacy-respecting reputation systems may not provide sufficient protection in strict adversarial models or require substantial computational resources.

In this thesis, we investigate communication security within decentralized networks and introduce global privacy-preserving reputation protocols that do not require specialized platforms or trusted third parties. Furthermore, these protocols preserve privacy in various adversarial models and demonstrate practical efficiency. We achieve this using blockchain and diverse cryptographic techniques such as secret sharing, additive homomorphic cryptosystems, secure multiparty computation, and zero-knowledge proofs. Experimental results testify to the effectiveness of the proposed protocols.

Keywords: Blockchain, Privacy, Reputation, Reputation Management System, Secret Sharing, Secure Multiparty Computation, Trust.