**Authentification des documents à l’aide de la blockchain**

**RESUME**

*Mots clés : authentification, sécurisation, document, blockchain, cryptographie, decentralized application*

1. **INTRODUCTION**

La fiabilité de certains documents administratifs est de plus en plus controversée car il est maintenant fréquent de retrouver des documents falsifiés ou d’origine douteuse sur l’espace numérique public, mettant ainsi en déroute, bon nombre de citoyens. Cela pourrait être dû en partie, au développement et à l’exploitation malsaine des multiples outils basés par exemple sur l’Intelligence Artificielle (IA).

En effet, le phénomène de documents falsifiés contribue à ternir l’image de leur légitime auteur qui pourrait être le gouvernement, créant ainsi une crise de confiance entre celui-ci ses usagers-clients. Pour faire face à ce phénomène grandissant, des auteurs et destinataires de documents effectuent parfois des opérations d’authentification de ceux-ci, moyennant l’utilisation de coûts et temps énormes qui pourraient baisser leurs rendements à terme.

Dans ce contexte où la Blockchain est également une technologie novatrice en pleine croissance, elle semble prometteuse pour résoudre efficacement le phénomène de falsification documentaire.

L’objectif de notre travail est de proposer une approche d’authentification de documents à l’aide de la blockchain, et d’implémenter une application décentralisée (DApp) basée sur cette approche. Notre solution offre la possibilité de vérifier l’authenticité de documents en temps réels, de manière sécurisée, transparente et sans passer par une autorité centrale de vérification.

1. **ÉTAT DE L’ART**

La technologie blockchain, propulsée par l’avènement en 2008 de la crypto-monnaie bitcoin de *Satoshi Nakamoto* [10], est en pleine croissance ces dernières décennies. La Blockchain est une technologie numérique permet de stocker chronologiquement et de transmettre des informations sous forme de blocs reliés les uns aux autres de manière sécurisée (par forte usage de la cryptographie) et sans autorité centrale.

Selon *Imran Bashir* [14], les blockchains de la 3e génération sont applicables, au-delà de l'industrie des services financiers, dans divers domaines sociétaux à usage général tels que les médias, la santé, le gouvernement, etc. Outre Bitcoin, il existe plusieurs blockchains (Solana, Ethereum, Cardano, Avalanche, ...) parmi lesquelles nous adoptons Ethereum pour la présente expérimentation.

1. **Blockchain Ethereum**

La blockchain publique Ethereum dont le mécanisme de consensus est passé du Proof of Work au Proof of Stake en 2022 [26], a connu plusieurs mutations depuis son lancement par Vitalik Buterin le 30 juillet 2015 [29].

1. **Authentification et sécurisation de** **documents**
2. **Méthodes existantes d’authentification de** **documents**
3. METHODOLOGIE
4. EXPERIMENTATION DE LA SOLUTION
5. Outils
6. Simulations

**Conclusion**

**REFERENCES**