

Université Benyoucef Benkhedda- Alger1

Faculté des Sciences

Département de Mathématiques et Informatique

Spécialité : Ingénierie des Systèmes Informatiques Intelligents



RAPPORT

Mise en place d'une interface de gestion d'une Blockchain

Réalisé par :

- MARREF Kawter

Enseignant : Mr ABBAS

Module : Cryptographie

Groupe : 01

2019/2020

Table des matières

Introduction :	2
1. Blockchain :	2
Type de blockchain	2
Blockchain publique	2
Blockchain privée	2
Fonctionnement :	3
Cas d'utilisation	4
2. Le rôle de la cryptographie dans une blockchain :	5
3. Les défis de la Blockchain	6
4. Application	6
Application décentralisée de vote (DApp) :	7
Processus de vote :	7
Smart contract :	7
Outils utilisés :	8
Interface du DAPP :	9
Conclusion	11
Références	12

Introduction :

En 2008, une thèse scientifique sous le nom de [« Bitcoin : A Peer-to-Peer Electronic Cash System »](#) a été partagée par une personne (ou une équipe) sous le nom de Satoshi Nakamoto. Dans cette thèse Nakamoto a démontré l'application de blockchain sur la première cryptomonnaie appelée Bitcoin, elle permet d'envoyer de l'argent sans intermédiaire c'est-à-dire sans autorité centrale de contrôle, cette avancée technologique ouvre la voie d'un nouvel internet. Dans ce rapport, nous allons voir le fonctionnement de blockchain et son intérêt, explorer à quels domaines cette technologie peut s'appliquer et enfin créer une application décentralisée de vote à l'aide d'Ethereum Blockchain.

1. Blockchain :

Blockchain est un outil de stockage et de transmission d'information d'une manière fiable, transparente et sécurisé.

Fiable : on y retrouve l'historique (registre ou Ledger) de toutes les transactions effectuées depuis que le genesis block (Block#0) a été miné, elle est aussi **immutable** c'est-à-dire elle n'est pas éditée, on peut seulement ajouter de nouveaux blocs liés au bloc précédent.

Transparente : elle est partagée par tous ses utilisateurs sans aucun intermédiaire donc on peut facilement vérifier sa validité.

Sécurisé : s'appuie fortement sur la cryptographie pour assurer la sécurité des données (coin24, s.d.).

Type de blockchain

Deux types de blockchain circulent en ce moment, publique et privée, la différence est que sur l'un tout le monde peut participer, sur l'autre l'accès est restreint.

Blockchain publique

Une blockchain publique est ouverte à tous d'une façon anonyme, elle est décentralisée donc aucune entité de contrôle, ses données restent tout de même très sécurisées grâce à son fonctionnement.

Blockchain privée

Une blockchain privée est plus confidentielle, seuls les membres autorisés peuvent l'utiliser ou participer. Hyperledger est un portefeuille de projets de DLT qui encourage les entreprises à adopter cette technologie pour améliorer la performance et la fiabilité des systèmes actuels.

Tableau comparative :

	Publique	Privé
Accès	Accessible à tous	Seulement les membres autorisé
Identité	Anonyme	Connu
Vitesse de transaction	Lente	Rapide
Immutabilité	Elevé	Faible
Réseau	Décentralisé	Décentralisé partiellement

Tableau 1 Comparaison entre blockchain publique et privé

Fonctionnement :

Blockchain comme son nom l'indique, c'est une chaîne de blocs, chaque bloc est constitué d'un ensemble de transactions effectuées entre les utilisateurs du réseau. Un bloc doit être validé par les nœuds (ordinateurs) appelés « mineurs » du réseau en utilisant un mécanisme de **consensus** qui assure que lorsqu'un message malveillant est envoyé une règle de consensus l'étouffe, il existe deux principales méthodes : (Loignon, 2017)

- ❖ La preuve de travail (Proof Of Work) : fiable mais lente et coûteuse en énergie
- ❖ La preuve d'enjeu (Proof Of Stake) : plus pratique, moins énergivore mais à la fiabilité plus contestée.

Une fois le bloc validé, il est horodaté et ajouté à la blockchain.

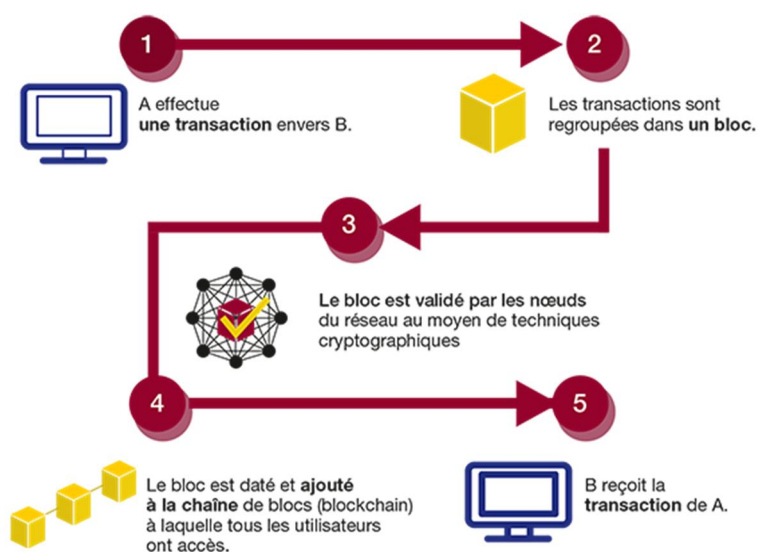


Figure 1 Etapes de transactions dans une blockchain (coin24, s.d.)

Cas d'utilisation

Grace à sa transparence, sa sécurité et son caractère décentralisée, cette technologie prometteuse de modernisation peut tout à fait être utilisé dans d'autres domaines autre que le domaine monétaire. On peut classer son utilisation en trois catégories :

- ❖ Les applications pour **le transfert d'actifs pair à pair** (cryptomonnaie, titres, votes...).
- ❖ Les applications de la blockchain en tant que **registre** (notarisation) : elle assure une meilleure traçabilité des produits et des actifs par l'enregistrement et la vérification d'informations datées et sanctuarisées, comme si elles étaient passées entre les mains d'un notaire.
- ❖ L'exécution automatique de contrats (**Smart contracts**) : c'est des programmes autonomes qui permettent d'exécuter automatiquement des commandes selon les conditions fixées par le contrat sans l'intervention d'une personne (Loignon, 2017), (Blockchain France, s.d.).

Parmi les domaines auxquels la blockchain peut être appliquée sont :

- **Domaine bancaire** : elle révolutionne la façon d'échanger et de sécuriser les transactions éliminant presque tous les risques d'hacking.
- **L'immobilier** : en plus des avantages du blockchain, elle simplifie les démarches et accélère le processus qui prend en moyenne 20 minutes (d'après une première vente immobilière blockchain en Brésil en juillet 2019) au lieu de 60 à 90 jours (en France) (Pagès, 28).
- **Chaîne de production alimentaire** : les projets blockchain alimentaires se développent partout dans le monde dans le but de moderniser les chaînes de production (Supply chain) du secteur agroalimentaire et de la grande distribution afin d'assurer la traçabilité et la transparence des chaînes de production alimentaire mondiale de confiance, une des solutions leader aujourd'hui est « IBM Food Trust ».
- **Gestion des identités et des accès (GIA)** : l'utilisation du Zero-Knowledge Proofs, une méthode d'authentification qui permet de prouver une information sur une personne sans divulguer les données qui apportent des preuves à l'appui, on a comme exemple « Yao's Millionaires problem » : deux millionnaires Alice et Bob veulent savoir qui est-ce le plus riche sans divulguer combien d'argent ils ont (Tykn, 2019).

2. Le rôle de la cryptographie dans une blockchain :

La blockchain dépend fortement de la cryptographie pour assurer la sécurité de ses données, c'est pour cela qu'elle utilise plusieurs types de cryptographie.

- a. **Fonction d'hachage** : Dans une chaîne de blocs, le hash de chaque bloc est créé à l'aide du hash du bloc précédent plus les données du bloc (comme illustré ci-dessous), cet hash qui est l'identifiant unique du bloc assure la sécurité du blockchain et l'immuabilité.

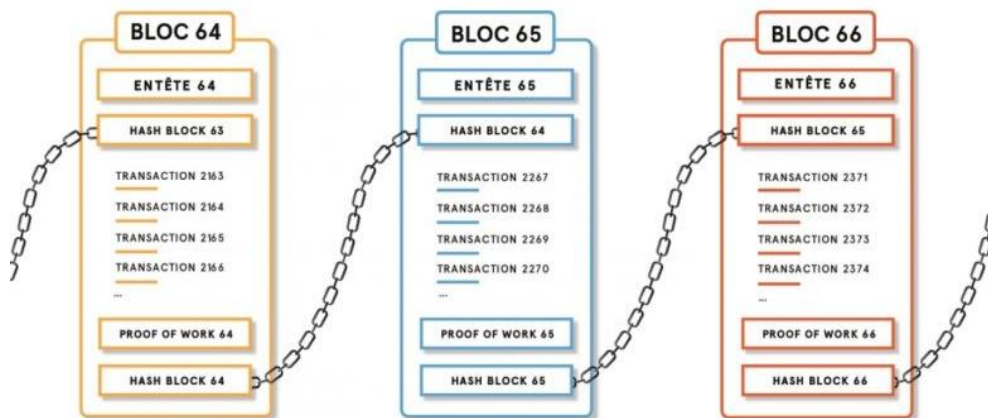


Figure 2 Fonctionnement du Blockchain (coin24, s.d.)

- b. **Cryptographie asymétrique** : utilisé pour la validation des données et l'authentification des utilisateurs en utilisant une combinaison de la clé publique et la clé privée de l'utilisateur via une infrastructure à clés publiques ou PKI (Public Key Infrastructure).
- c. **Zero Knowledge Proof** : prouver les conditions d'un message sans divulguer le contenu.
- d. **Merkle Tree** : est une façon de structuré les données pour valider les transactions d'une manière plus efficiente et rapide (HIMSS, 2019).

3. Les défis de la Blockchain

« La blockchain, pour le moment, est un peu comme Arpanet à l'égard d'Internet. La technologie n'est pas encore utilisable à grande échelle, on n'a pas encore trouvé l'équivalent pour la blockchain de TCP/IP », compare Gilles Babinet le représentant de la France sur les questions numériques à la Commission européenne (Loignon, 2017).

Comme toute nouvelle technologie plusieurs obstacles sont identifiés, ils doivent être d'abord surmontés pour qu'elle soit applicable à grande échelle, parmi lequel on trouve :

Les défis techniques

- Par rapport à la confidentialité, rapidité et sécurité

Les défis de marketing

- Consistant à trouver des modèles économiques rentables, tout en respectant ce qui fait la valeur de la blockchain

Transformer l'emploi sans le détruire

- La blockchain renforce le vaste mouvement d'automatisation ce qui entraîne une grande perte d'emploi, cela devra être compensé par la création de nouveaux métiers

Réglementer sans freiner l'innovation

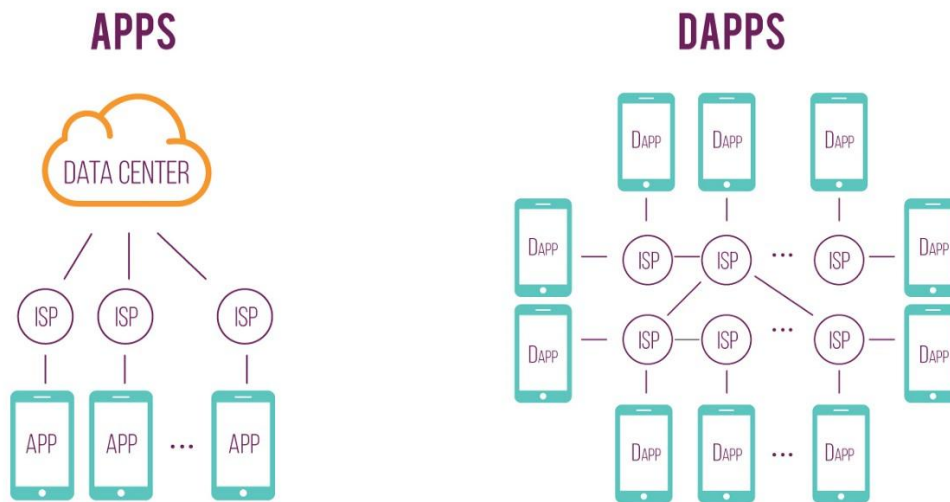
- La complexité et le manque de compréhension de cette technologie par les législateurs les freinent à entreprendre des actions

Figure 3 Les défis de la blockchain (Loignon, 2017)

4. Application

Une application web est une application accessible via un navigateur internet, le code et les données se trouvent dans un serveur web, dans le cas où on veut construire une application qui comporte des *données sensibles* comme dans une application de vote, on s'expose à de réels risques de sécurité car les données et le code peuvent être altérés et même supprimés à tout moment, cela crée un vrai problème de confiance chez les utilisateurs tel qu'on ne peut pas savoir si notre vote a été compté ou non si les élections ont été truquées. Avec une application décentralisée on assure un bien meilleur niveau de transparence et sécurité.

La figure ci-dessous illustre la différence entre les applications web classiques et les applications décentralisées :



Source: towardsdatascience.com/what-is-a-dapp-a455ac5f7def

Figure 4 App vs DApp

Application décentralisée de vote (DApp) :

C'est une application open source qui fonctionne sur un réseau décentralisé et utilise un token ou une cryptomonnaie, les données sont stockées d'une façon chiffrée et transparente sur une blockchain comme Ethereum.

Une DApp hérite de tous les avantages de sécurité d'une blockchain, elle sera très utile pour la construction d'une *application de vote*. Tous les comptes connectés au réseau auront une copie des données et le code sur la blockchain, ils participent aussi à s'assurer que toutes les copies distribuées sur le réseau sont les mêmes, on garantit ainsi que chaque vote est compté.

Processus de vote :

Pour qu'une personne vote, elle doit avoir un compte sur une blockchain -dans notre cas- Ethereum avec un montant de cryptomonnaie appelé Ether, il faut savoir que la lecture d'une blockchain est gratuite mais l'écriture ne l'est pas, donc pour voter il faut payer les frais de transaction appelé Gas, afin que les mineurs soient payés pour leurs services.

Smart contract :

Le smart contract est responsable de la lecture et l'écriture sur la blockchain, il contient le code de l'application programmé avec le langage Solidity. Il est important d'exécuter des *tests* sur le contrat car une fois la DApp est réellement déployée sur la blockchain elle devient immuable. On vérifie donc que :

- Le smart contract a été initialisé avec le même nombre de candidats 3.
- Les données des candidats sont correctes.
- On peut voter qu'une seule fois.
- Tous les votes sont comptés.
- Les votes pour des candidats invalides sont erronés.




Pour exécuter les tests on utilise la commande « truffle test »

```
20.04.13 01:52:19 304 GET /js/bootstrap.min.js
✓ initializes with three candidates (109ms)
✓ it initializes the candidates with the correct values (315ms)
✓ allows a voter to cast a vote (695ms)
✓ throws an exception for invalid candidates (679ms)
✓ throws an exception for double voting (1486ms)

5 passing (4s)
```

Figure 5 Exécution des tests

Outils utilisés :

- Ethereum : est une blockchain qui permet de créer des applications décentralisées, elle vise à bâtir un nouveau web où il n'existe pas d'intermédiaire entre client et service. Les participants du réseau Ethereum ne valident pas seulement les transactions monétaires mais ils exécutent le code provenant des applications décentralisées aussi, ce qui diffère de Bitcoin qui est centrée sur le domaine monétaire (Blockchain France, 2016).
- Ganache : est une blockchain personnelle pour le développement Ethereum, elle est utilisée pour déployer des contrats, développer des applications et tester. Il vient avec 10 comptes sur notre blockchain locale remplis de 100 faux Ether chacun (Ganache).
- Metamask : est une extension pour accéder à des applications Ethereum sur le navigateur Chrome.
- Solidity : est un langage de haut niveau pour l'implémentation de smart contracts. Il a été influencé par C++, Python et JavaScript. Conçu pour la machine virtuelle Ethereum EVM (Solidity).

Interface du DAPP :

L'utilisateur doit être logger à son compte Metamask pour voter, une fois qu'on clique sur le bouton « vote » une notification arrive sur Metamask pour confirmer le paiement de frais afin que le vote soit compter et les statistiques sont mis à jour automatiquement.

Voting DApp

Home

Vote

Stats

Candidates

Trust us with your vote

Select Candidate

Candidate 1


Vote

Your Account: 0x9b977e425ed16c01dc3e46ad44a151a6bbf50bf


Stats

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	0
3	Candidate 3	0


Get To Know The Candidates



Lorem ipsum donec id elit non mi porta gravida at eget metus.



Lorem ipsum donec id elit non mi porta gravida at eget metus.



Lorem ipsum donec id elit non mi porta gravida at eget metus.

Voting dapp made with blockchain and brought to you by [Ethereum](#)

Figure 6 Page d'accueil

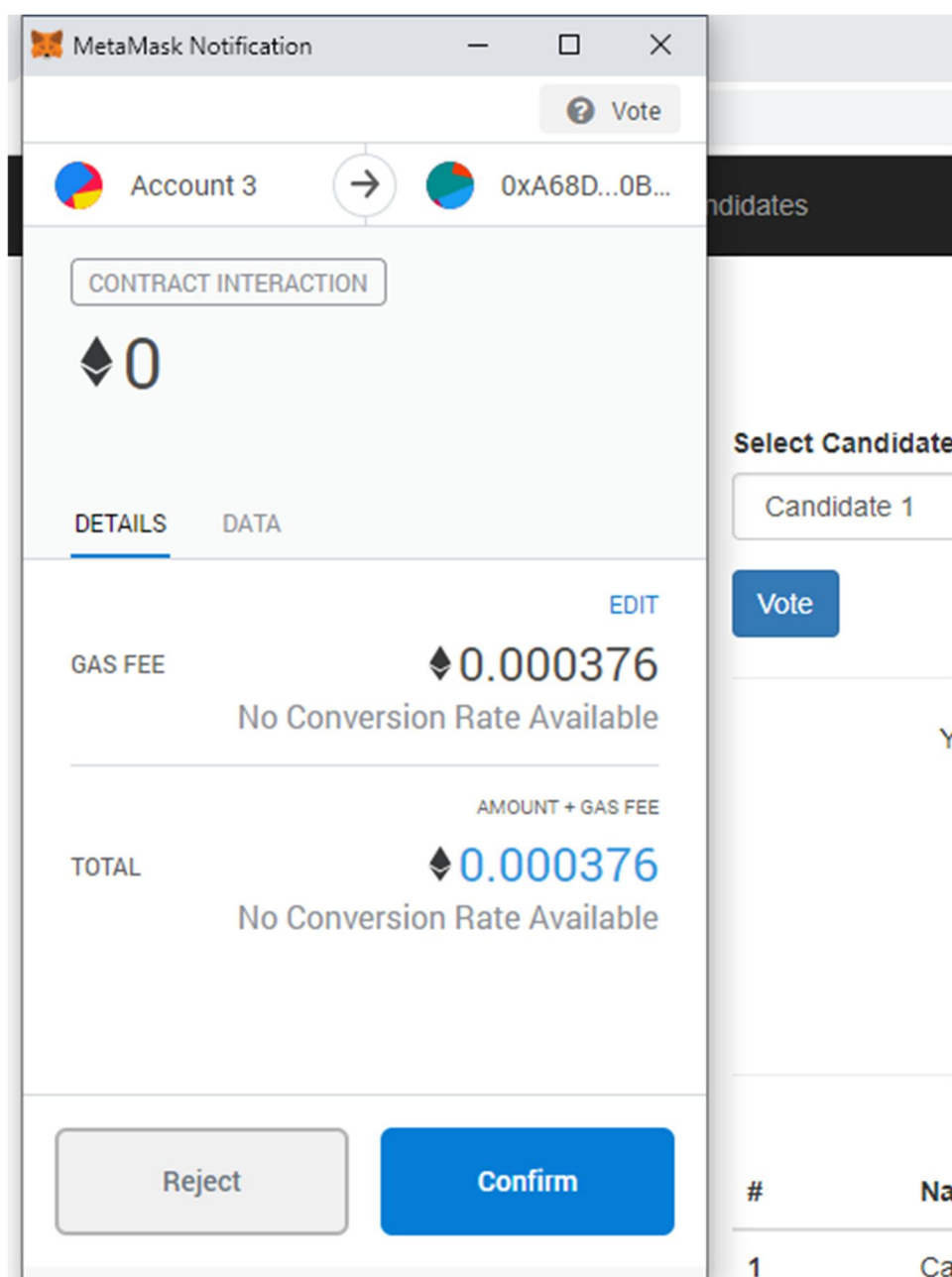


Figure 7 Confirmer le paiement pour voter

Conclusion

Blockchain est la nouvelle technologie de la confiance, sans autorité centrale, elle incarne la transparence et la collaboration, de grandes entreprises ont déjà commencé à adopter cette technologie, elle ne tardera pas à s'introduire dans notre vie quotidienne et pourquoi pas à la transformé pour le meilleur.

Références

- Blockchain France . (2016, Mars 4). *Qu'est-ce qu'Ethereum ?* Consulté le Avril 14, 2020, sur <https://blockchainfrance.net/2016/03/04/comprendre-ethereum/>
- Blockchain France. (s.d.). *Qu'est-ce que la blockchain ?* Consulté le Avril 10, 2020, sur <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>
- coin24. (s.d.). *Comment fonctionne la blockchain ?* Consulté le Avril 9, 2020, sur <https://coin24.fr/dictionnaire/blockchain/>
- Ganache. (s.d.). *TRUFFLE SUITE*. Consulté le Avril 14, 2020, sur <https://www.trufflesuite.com/docs/ganache/overview>
- HIMSS. (2019, Janvier 28). *Cryptography in Blockchain*. Consulté le Avril 12, 2020, sur <https://www.himss.org/resources/cryptography-blockchain>
- Loignon, S. (2017). *BIG BANG BLOCKCHAIN, La seconde revolution d'internet*. Paris: Éditions Tallandier.
- Pagès, A. (28, Novembre 28). *Avec la blockchain, l'immobilier devrait enfin passer à l'ère numérique*. Consulté le Avril 11, 2020, sur <https://korii.slate.fr/tech/blockchain-immobilier-cryptomonnais-futur-revolution-transactions>
- Solidity. (s.d.). *Solidity*. Consulté le Avril 14, 2020, sur <https://solidity.readthedocs.io/en/v0.4.21/>
- Tykn. (2019, Mars 13). *Identity Management with Blockchain: The Definitive Guide (2020 Update)*. Consulté le Avril 11, 2020, sur https://tykn.tech/identity-management-blockchain/#What_is_Identity_Management