



MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA
RECHERCHE SCIENTIFIQUE

UNIVERSITÉ ABDELHAMID IBN BADIS - MOSTAGANEM



Faculté des Sciences Exactes et d'Informatique

Département de Mathématiques et informatique

Filière : Informatique

MEMOIRE DE FIN D'ETUDE

Pour l'Obtention du Diplôme de Master en Informatique

Option : **Réseaux et Systèmes**

Présenté par :

BELKACEMI Rachid

OULD-BADJA Yacine

THEME :

Sécurisation des données dans un GDSS

Soutenu le :

Devant le jury composé de :

Mr. LAREDJ Mohammed Adnane

Université de Mostaganem Encadrant

Mr. Bessaoud Karim

Université de Mostaganem Encadrant

Année Universitaire : 2022-2023

Resumé

Les GDSS sont des systèmes informatiques conçus pour aider les groupes à prendre des décisions en temps réel. Ils offrent de nombreux avantages, mais la sécurité des données est un aspect crucial à prendre en compte. Les organisations doivent mettre en place des mesures de sécurité appropriées pour protéger les données contre les menaces potentielles.

Les blockchains par exemple peuvent être utilisées pour assurer la sécurité et l'intégrité des données stockées dans le contexte du GDSS, en garantissant que toutes les données sont sauvegardées de manière décentralisée et immuable. Les blockchains peuvent également être utilisées pour créer des contrats intelligents entre les membres d'un groupe, permettant des normes de gouvernance explicites et ouvertes pour la prise de décision.

Les blockchains offrent également une grande transparence et une grande fiabilité puisque chaque transaction est enregistrée sur la blockchain et peut être confirmée par tous les membres de l'organisation. Cela favorise la confiance collective, qui est nécessaire pour une prise de décision réussie et équitable.

Mots-clé : Systèmes Interactif, SIAD ,GDSS , Sécurité , Blockchains ,Ethereum,système de vote en ligne ,contrat intelligent

Table des matières

	Page
1 Décision et aide à la décision	3
I. Introduction	4
II. Décision	4
1. Les étapes de la décision	5
2. Le processus de décision	5
3. L'aide à la décision	6
4. Les acteurs de l'aide à la décision	7
III. Les systèmes Interactifs d'aide à la décision (SIAD), (DSS)	8
1. Définition :	8
2. Les différentes architectures des SIAD	8
3. Classification des SIAD :	10
4. Conclusion	12
2 Aide à la décision des groupes	13
I. Introduction	14
II. Définition	14
III. Caractéristiques des GDSS :	15
IV. Architecture des GDSS	15
V. Les composantes du GDSS	17

VI. Les avantages des GDSS	17
VII. Facteurs qui affectent le GDSS	18
VIII. Exemples de GDSS	20
1. Microsoft Teams :	20
2. ThinkTank :	22
3. Lucid meetings :	23
IX. conclusion	26
3 Sécurité de GDSS	27
I. Introduction	28
II. Généralités sur la Blockchain	28
1. Définition	29
2. Caractéristiques	30
3. Types :	31
4. Protocoles de consensus	33
5. Domaines d'application de la Blockchain :	36
6. défis de la Blockchain :	37
7. conclusion	38
4 conception et réalisation	39
1. Introduction	40
2. Processus unifié(UP)	40
3. Langage de modélisation unifié (UML)	41
4. Identification des besoins	42
5. Diagrammes de séquence	43
6. Outils de développement et langages utilisé	45
7. Configuration d'environnement	47

8.	Présentation des interfaces pour le vote	48
9.	Perspectives :	51
10.	Conclusion :	51

Table des figures

1.1	La prise de décision [12]	4
1.2	Modèle du processus de décision de[1]	6
1.3	– Modèle IDC (Intelligence, Design, Choice) [4]	6
1.4	Architecture en réseau d’un S.I.A.D	9
1.5	Architecture centralisée d’un S.I.A.D	9
1.6	Architecture hiérarchisée d’un S.I.A.D	10
1.7	Classification Selon les outils d’aides à la décision [12]	11
2.1	Architecture centralisée[1]	15
2.2	Architecture décentralisée [1]	16
2.3	Architecture hybride [1]	16
2.4	l’interface de Microsoft Teams [14]	21
2.5	l’interface de Microsoft Teams [14]	22
2.6	l’interface de ThinkTank [15]	23
2.7	l’interface de lucid meetings [16]	24
3.1	Histoire de la Blockchain[22]	29
3.2	les types de la Blockchains[27]	33
3.3	Domaines d’application de la technologie Blockchain. [30]	36
4.1	Le Processus UP [36]	41
4.2	Diagramme de séquencer lancer le vote	43
4.3	diagramme de séquence voter	44
4.4	Structure de répertoire election.	47
4.5	Connexion à la blockchain	48
4.6	Espace électeur	49

4.7	Transactions (Ganache)	50
4.8	confirmer la transaction	50

Liste des tableaux

- 3.1 Caractéristiques de différents Blockchains 31
- 3.2 un tableau comparatif des types de la Blockchain [28] 33
- 3.3 Comparaison entre les différents algorithmes de consensus [30] 35

Liste des abréviations

DSS : Décision Support Système

SIAD : systèmes Interactifs d'Aide à la Décision

GDSS : Groupe Decision Support System

ODSS : Organizational Decision Support Système

EIS : Systèmes d'information exécutifs

TB : tableaux de bord

URL : Uniform Resource Locator

AWS : Amazon Web Services

LDAP : Lightweight Directory Access Protocol

PoW : proof of work

PoS : proof of stake

DPOS : Delegated prof of stake

P2P : Peer-to-Peer

UP : Processus unifié

UML : Langage de modélisation unifié

NPM : Node Package Manager

Remerciements

Avant toute personne, je tiens à remercier ALLAH le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir travail.

Je tiens à exprimer ma sincère gratitude à notre encadrants **Mr. LAREDJ Mohammed Adnane & Mr. Bessaoud Karim**

pour ses conseils et ses encouragements tout au long de ce projet.

Je tiens à exprimer toute ma gratitude à tous les membres de jury, pour avoir bien voulu juger notre travail.

Je veux aussi adresser mes sincères remerciements à tous les enseignants du département de l'informatique de l'université de Mostaganem qui ont contribué à notre formation.

Aussi à mes parents, ma mère et mon père, qui m'ont toujours soutenue et encouragé tout au long de mon cursus.

Par crainte d'avoir oublié quelqu'un, que tous ceux et toutes celles à qui je suis redevables se voient ici vivement remerciés.

BELKACEMI Rachid

&

OULD-BADJA Yacine

Introduction Générale

Le concept de Systèmes Interactifs d'Aide à la Décision (SIAD) s'est formalisé dans la littérature dans les années 70 . Ce sont des outils spécifiquement développés pour supporter la prise de décision. La conception de tels systèmes implique l'utilisation de techniques issues de divers domaines comme l'informatique, la recherche opérationnelle, l'intelligence artificielle, l'ingénierie logicielle, l'interaction homme-machine et les télécommunications. Les SIAD s'avèrent particulièrement utiles pour aider à trouver une solution appropriée à des problèmes complexes, de grande dimension et ayant des objectifs fortement dépendants des préférences de l'utilisateur. La plupart des problèmes d'optimisation font partie de cette catégorie de problèmes.

parmi les systèmes interactif on à le GDSS ,Les systèmes d'aide à la décision de groupe ce sont des systèmes informatiques qui aident les groupes à faire des choix en temps réel. Ils permettent à un groupe de personnes de collaborer à une même activité en échangeant des informations et en discutant des difficultés à l'aide de technologies de communication et de collaboration.

Les GDSS présentent plusieurs avantages, Les membres d'un groupe peuvent collaborer plus efficacement en utilisant des outils de visualisation et d'analyse des données pour appréhender les différentes parties du problème (Lucid par exemple).

La sécurité des données devient un problème sérieux pour les entreprises . Les informations communiquées dans un GDSS pouvant être secrètes et sensibles, des mesures de sécurité appropriées doivent être mises en place pour les sécuriser. Pour garantir la sécurité des données dans les GDSS, en peut adopter des restrictions d'accès, des mesures de sécurité des communications, des sauvegardes fréquentes des données et des protocoles de gestion des incidents de sécurité, tels que les Blockchains.

L'objectif de ce mémoire est de rendre compte sur

- **Chapitre 1:** Dans ce chapitre, nous nous adaptons à Les systèmes d'information d'aide à la décision plus précisément les système inteactif d'aide à la decision ,les décideurs dans leurs activités de prise de décision,processus de décision, classification des systèmes d'information d'aide à la décision.

L'objectif de ce mémoire est dans le chapitre suivant,Il existe cependant diverses sortes de systèmes d'aide à la décision. Ce système est généralement utilisés dans les réunions. Nous présentons dans le chapitre 2 le GDSS.

-
- **Chapitre 2:Aide à la décision des groupe** qui est Un système informatique intégré composé d'un sous-système de communication et d'un SIAD orienté-modèle, pour soutenir la formulation du problème et de la solution potentielle des décisions non structurées dans une réunion de groupe.
ensuite présentés dans le chapitre 3 comment le?(GDSS)
 - **Chapitre 3:Sécurité des GDSS** pour cela on à adopté les Blockchains comme methode de sécurité,les blockchains peuvent être utilisées pour garantir la sécurité et l'intégrité des données stockées
 - **Chapitre 4:Conception et Réalisation** Ce chapitre explique les étapes essentielles de la conception, de la modélisation et de la réalisation d'un système de vote en ligne basé sur la technologie blockchain. Le processus de conception repose sur Unified Process (PU) en utilisant Unified Modeling Language (UML) comme langage de modélisation , en mettant l'accent sur les aspects techniques et les interfaces utilisateur.

Chapitre 1

Décision et aide à la décision

I. Introduction

Action d'aider quelqu'un, de lui donner une assistance momentanée ; appui, soutien :

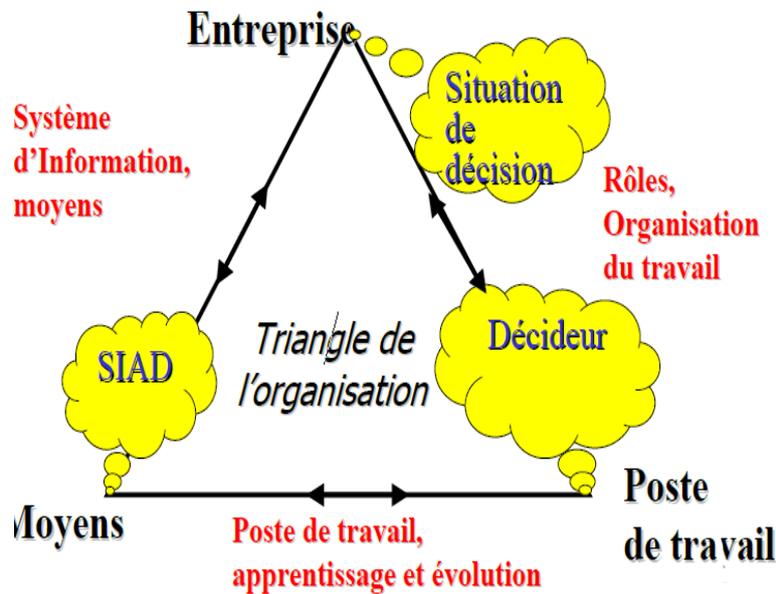


FIG. 1.1 : La prise de décision [12]

Avec votre aide, je réussirai. Aider quelqu'un dans son activité

II. Décision

Une décision est une action qui est prise pour faire face à une difficulté ou répondre à une modification de l'environnement, c'est à dire pour résoudre un problème qui se pose à l'individu, ou à l'organisation » [1].

« On présente souvent la décision comme le fait d'un individu isolé (le "décideur") exerçant librement un choix entre plusieurs possibilités d'actions à un moment donné dans le temps. Sans nier toute pertinence à cette conception de la décision, il faut admettre qu'elle ne rend que très imparfaitement compte de la façon dont sont prises les décisions dans la plupart des organisations » [2].

« Une décision c'est le résultat d'un processus mental qui choisit une parmi plusieurs alternatives mutuellement exclusives » [3].

D'après ces définitions, il est clair que la prise de décision consiste à choisir un plan d'action à partir d'alternatives pour atteindre un objectif prédéterminé.

1. Les étapes de la décision

La décision est un processus de résolution de problème qui met en oeuvre des connaissances de natures très variées, la décision simple correspond à la classe de « problèmes relativement bien défini » [5].

Un problème existe si [5] :

- Le décideur perçoit un état interne ou externe non désiré A ;
- L'état de départ A non désiré doit être transformé en état de but B ;
- Le décideur ne sait pas au départ comment parcourir le chemin qui va du point de départ A vers le point de solution B.

Le décideur doit transformer la perception peu précise du problème en problème plus précis et mieux structuré.

- Les buts de la décision doivent être précisés.
- Le problème doit être transformé en sous problèmes abordables.
- Chaque sous problème peut être résumé par un but à atteindre Pour chaque sous but, il s'agit de trouver des heuristiques (opérateurs) qui permettent de le résoudre. – La poursuite des sous buts doit être coordonnée stratégiquement. Il s'agit aussi de résoudre des conflits entre sous buts.
- Une fois que tous les sous-buts ont été atteints, il faut évaluer si le but général a été atteint.[5]

2. Le processus de décision

2. **1. phase d'intelligence (investigation)** : il s'agit de recenser l'ensemble des informations utiles et prioritaires dont le décideur aura besoin lors de la prise de décision (objectifs ou priorités, définition du problème à résoudre).
2. **2. phase de modélisation (conception)** : concerne la génération et le développement des différentes alternatives (ou scénarios). Cette étape peut nécessiter une recherche d'information complémentaire.
2. **3. phase de choix (sélection)** : le décideur évalue les différents scénarios réalisés pendant la phase de conception pour en retenir un seul. Il s'agit de déterminer les critères

d'évaluation des différentes solutions possibles et de mesurer les conséquences de chaque alternative.[4]

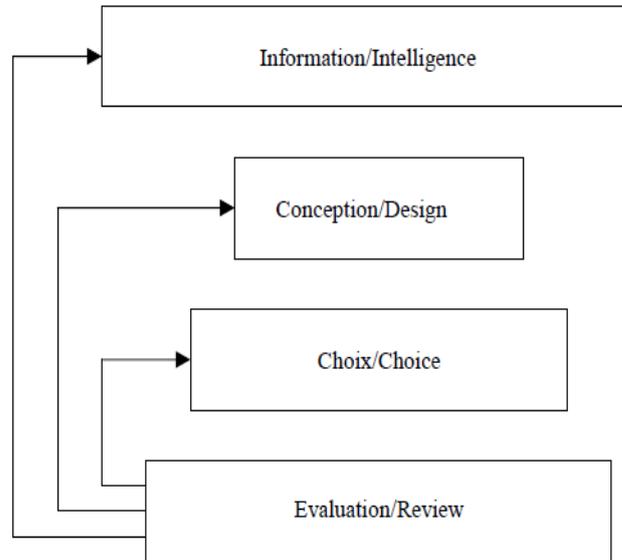


FIG. 1.2 : Modèle du processus de décision de[1]

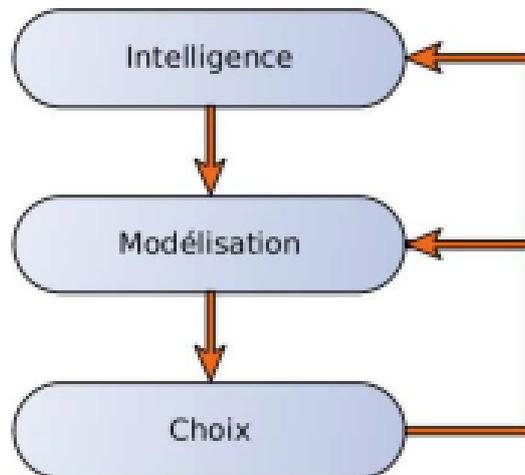


FIG. 1.3 : – Modèle IDC (Intelligence, Design, Choice) [4]

3. L'aide à la décision

L'aide à la décision est l'activité de celui qui, prenant appui sur des modèles clairement explicités mais non nécessairement complètement formalisés, aide à obtenir des éléments de

réponses aux questions que se pose un intervenant dans un processus de décision, éléments concourant à favoriser, un comportement de nature à accroître la cohérence entre l'évolution du processus d'une part, les objectifs et le système de valeurs au service desquels cet intervenant se trouve placé d'autre part.[2]

4. Les acteurs de l'aide à la décision

un acteur de l'aide à la décision est « tout individu intervenant dans le processus d'aide à la décision ».

On distingue plusieurs acteurs dans un processus d'aide à la décision.[6]

1. **Le décideur** : la personne (ou les personnes) assistée(s) par l'aide à la décision et qui est aidée pour mieux exprimer ses préférences vis-à-vis une situation donnée.
2. **Les intervenants** : ceux qui, de par leur intervention, conditionnent directement la décision en fonction du système de valeurs dont ils sont porteurs.
3. **Les agis** : ils sont concernés par les conséquences de la décision. Ils interviennent indirectement dans le processus par l'image que d'autres acteurs se font de leurs valeurs et plus concrètement de leurs systèmes de préférences.
4. **Les demandeurs** : ils demandent l'étude et allouent les moyens.
5. **L'homme d'étude (l'analyste)** : est un individu ou un groupe d'individus, qui a pour rôle d'établir un système de préférences, de définir le modèle d'aide à la décision, de l'exploiter afin d'obtenir des réponses et d'établir des recommandations pour conseiller le décideur sur les solutions envisageables. L'homme d'étude est à distinguer du négociateur et du médiateur.
6. **Le négociateur** : mandaté par un décideur en vue de faire valoir la position de celui ci dans une négociation et de rechercher une action compromise.
7. **Le médiateur** : intervient en vue d'aider les décideurs (ou les négociateurs) à rechercher une action compromise.
8. **L'arbitre (juge)** : intervient en se substituant aux acteurs dans la recherche d'une action compromise.

III. Les systèmes Interactifs d'aide à la décision (SIAD), (DSS)

1. Définition :

En raison de la complexité et de l'importance des conséquences engendrées par une décision, il faut déterminer des informations pertinentes pour garantir une meilleure prise de décision [3] tout en minimisant les coûts d'erreurs, et en suivant une stratégie de changement de l'environnement qui nous entoure. L'utilisation des systèmes d'aide à la décision (SAD), permet d'évaluer de telles situations relativement à diverses alternatives et leurs impacts.

Les SAD constituent des solutions très adaptées et très avancées dans ce domaine. Ces derniers permettent au décideur d'améliorer sa capacité de prise de décision en tenant compte des différentes contraintes [6] .

Le concept de système d'aide à la décision (DSS, Décision Support Système) est extrêmement vaste et ses définitions dépendent du point de vue de l'auteur. Un DSS peut Information Conception Choix Évaluation , prendre de nombreuses formes et peut s'utiliser de diverses manières. Certains définissent un DSS d'une façon générale comme étant :

« Un système informatique qui facilite le processus de prise de décision »[10] . D'une manière plus précise, d'autres définissent un DSS comme étant ; « Un système d'information informatique, interactif, flexible et adaptable, spécialement développé pour aider à trouver une solution à un problème de gestion non structuré, en vue d'une meilleure prise de décision. Il utilise des données, offre une interface conviviale et permet au décideur d'apporter ses propres idées »[18].

2. Les différentes architectures des SIAD

- Architecture en réseau :

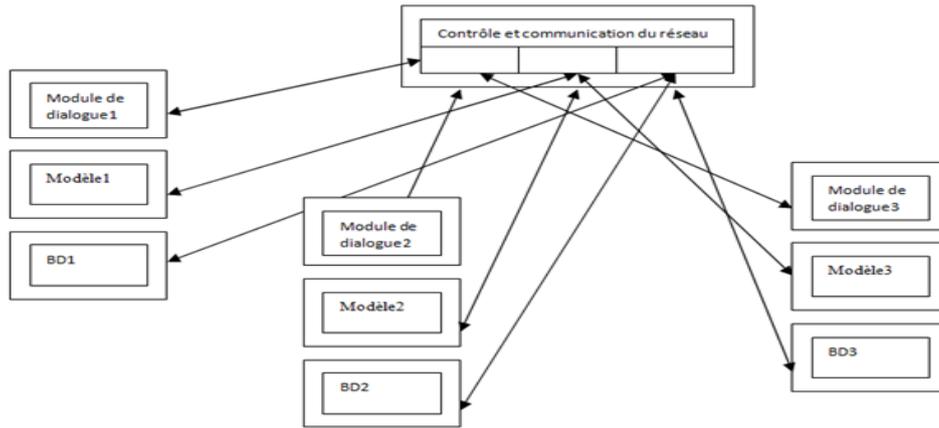


FIG. 1.4 : Architecture en réseau d'un S.I.A.D
[12]

- Architecture centralisée :

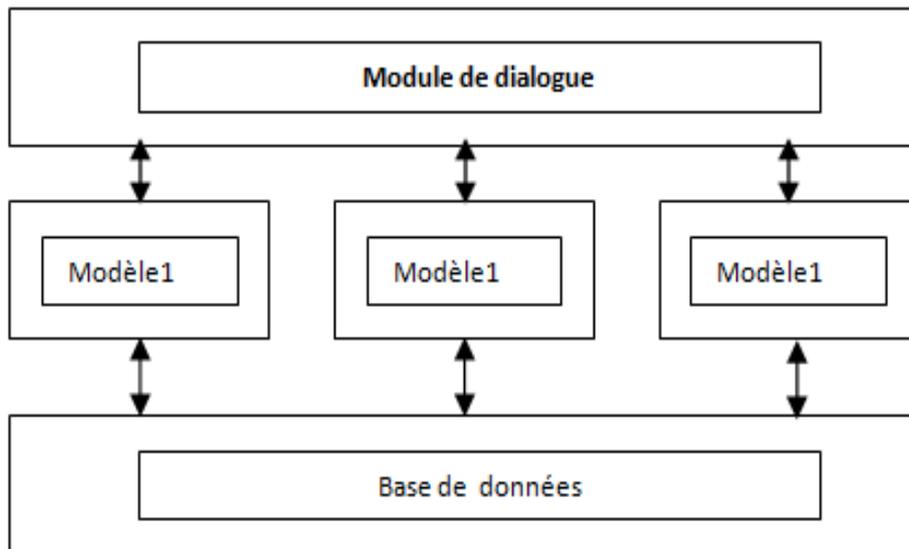


FIG. 1.5 : Architecture centralisée d'un S.I.A.D
[12]

- Architecture hiérarchisée :

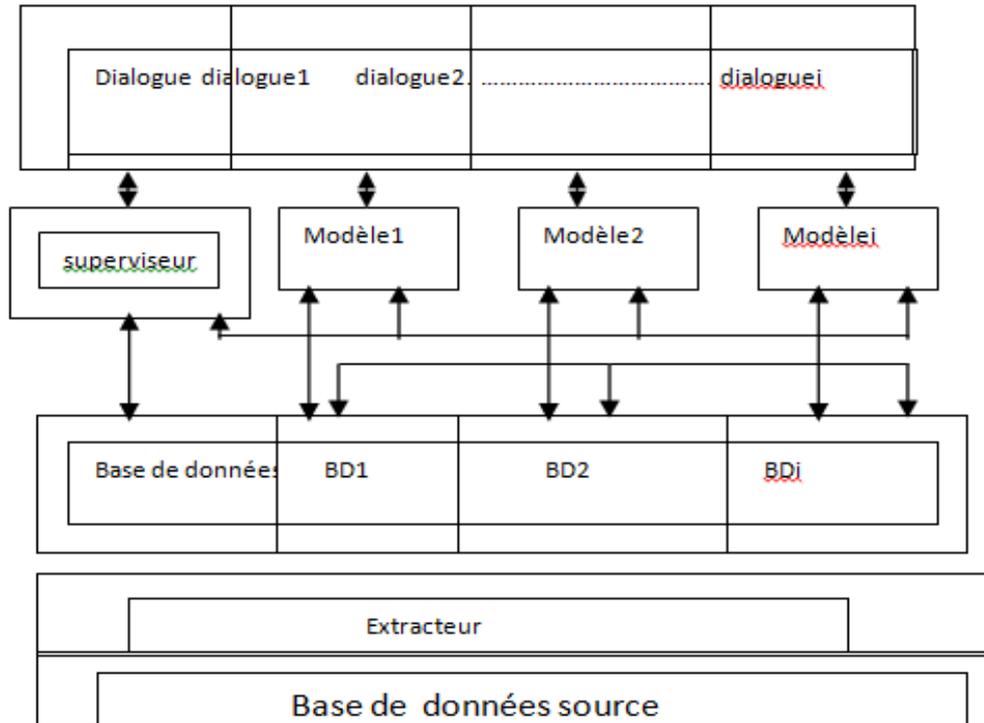


FIG. 1.6 : Architecture hiérarchisée d'un S.I.A.D
[12]

3. Classification des SIAD :

Les outils d'aide à la décision ont fait l'objet de plusieurs classifications qui ont été proposées par plusieurs chercheurs, où chaque chercheur a ses propres définitions et appellations.

Parmi ces classifications nous pouvons citer la classification proposée :[12]

- Selon les outils d'aides à la décision

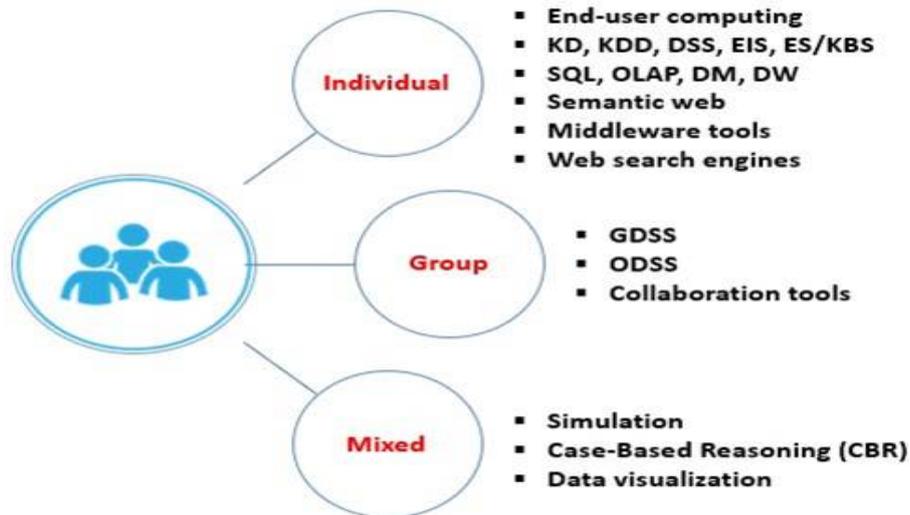


FIG. 1.7 : Classification Selon les outils d'aides à la décision [12]

nous on va s'intéresser avec la classification selon les outils d'aide à décision de groupe

3.1. les outils d'aides à la décision de groupe

Il s'agit d'outils facilitant les activités et améliorant l'efficacité d'un groupe de décideurs. Cette catégorie regroupe : les outils collaboratifs, les SIAD de groupe (GDSS : Group decision support systems), les SIAD organisationnels (ODSS : Organizational Decision Support System).

le principe c'est Pour la prise de décision de groupe ou d'organisation.[13]

- **selon le composant principal** [14]
 - a. DSS orienté-communication
 - b. DSS orienté-données
 - c. DSS orienté-document
 - d. DSS orienté-connaissance
 - e. DSS orienté-modèle

Dans notre thème on va s'intéresse sur :

3.2. SIAD orienté-communication

pour la prise de décision de groupe, il regroupe les technologies d'aide à la décision, de partage d'information, de communication, et de collaboration.

4. Conclusion

la décision est le processus de choisir un plan d'action parmi différentes alternatives pour atteindre un objectif donné. Les étapes de ce processus comprennent l'intelligence (collecte d'informations), la modélisation (génération d'alternatives), et le choix (sélection de la meilleure alternative).

L'aide à la décision vise à aider les décideurs à prendre des décisions informées en utilisant des modèles et des informations pertinentes.

Les systèmes interactifs d'aide à la décision (SIAD) sont des outils informatiques qui facilitent ce processus. Ils peuvent être classés en fonction de leurs composants principaux, tels que l'orientation vers la communication, les données, les documents, la connaissance ou les modèles. Dans le contexte de la prise de décision de groupe, les GDSS sont particulièrement importants pour faciliter la prise de décision collective.

Chapitre 2

Aide à la décision des groupes

Aide à la décision des groupe

I. Introduction

Pour aider les décideurs, les organisations utilisent une variété de systèmes d'information d'aide à la décision. L'expression "système d'information d'aide à la décision" fait référence à un large éventail de systèmes et de technologies et d'outils.

L'expression englobe les concepts suivants : systèmes interactifs d'aide à la décision (SIAD), entrepôts de données, systèmes d'information exécutifs (EIS) et tableaux de bord (TB) systèmes experts, systèmes d'aide à la décision de groupe (GDSS) et s, les systèmes basés sur la connaissance et les systèmes d'information collaboratifs systèmes d'information coopératifs, par exemple.

II. Définition

Selon HAMDADOU [7] « un GDSS est un système interactif et informatisé qui facilite la résolution des problèmes non structurés par un ensemble de décideurs fonctionnant ensemble en tant que groupe. Il aide des groupes, particulièrement groupes des directeurs, en analysant des situations de problème et en accomplissant des tâches de prise de décision de groupe »

D'un point de vue technologique le GDSS se situe aux frontières de l'informatique et des télécommunications. En effet des technologies issues de l'informatique ainsi que de la télécommunication sont utilisées[8].

D'un point de vue système d'information, le GDSS se situe aux frontières de la bureautique et de l'informatique transactionnelle. En effet, d'un point de vue utilisateur les outils de GDSS font partie de la gamme des outils de bureautique et utilisent des infocentres [8].

Le système d'aide à la décision de groupe est « « une combinaison d'ordinateurs, de communications et de technologies de décision travaillant en tandem pour fournir une aide à l'identification de problème, à la formulation et à la génération de solutions pendant les réunions de groupe »[9]

III. Caractéristiques des GDSS :

Quelque soit le type de GDSS considéré on distingue deux dimensions de bases qui caractérisent un GDSS .Ces deux caractéristiques sont [6] :

1. **La Proximité**
2. **La synchronisation**

IV. Architecture des GDSS

a -Les architectures centralisées :

L'architecture est une hiérarchie est imposée. Tous les composants(participants)transmettent leurs informations à une entité supérieure(le coordinateur centrale).

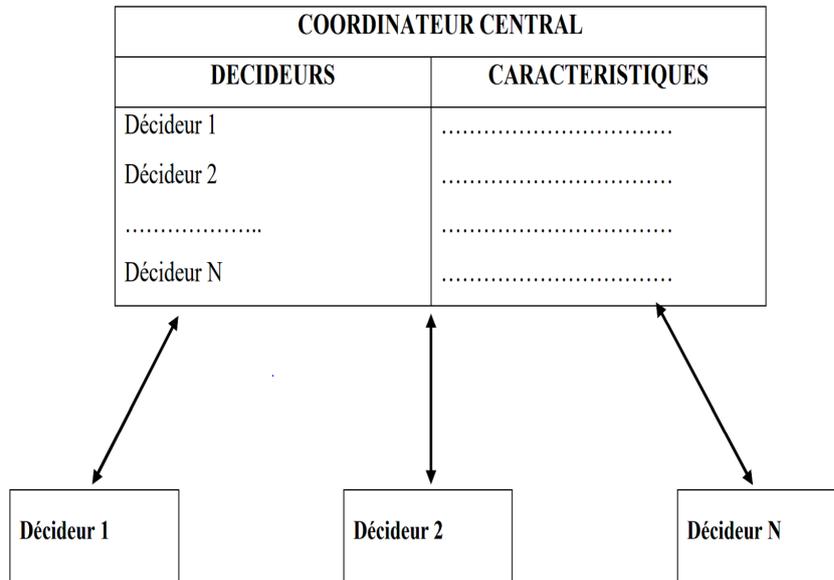


FIG. 2.1 : Architecture centralisée[1]

b -Les architectures décentralisées

Dans ce type d'architecture chaque composant est autonome. Il n'y a aucune hiérarchisation(figure).

Les GDSS distribués décentralisés sont en opposition avec les GDSS à architecture centralisées.

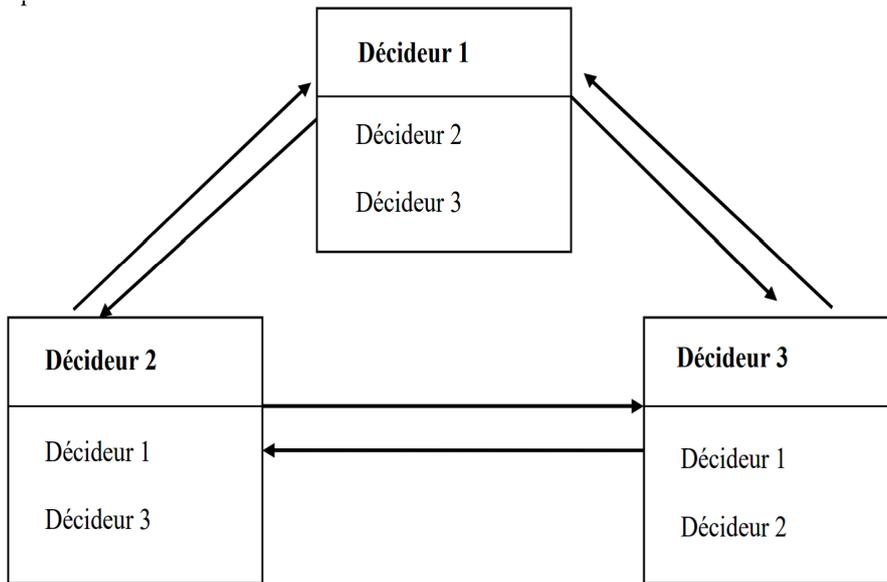


FIG. 2.2 : Architecture décentralisée [1]

c -Les architectures hybride

Comme son nom l'indique, l'architecture hybride est un mélange des deux architectures.

On y retrouve une entité supérieure et hiérarchique qui collecte les données des autres entités qui fonctionnent indépendamment de l'entité supérieure.

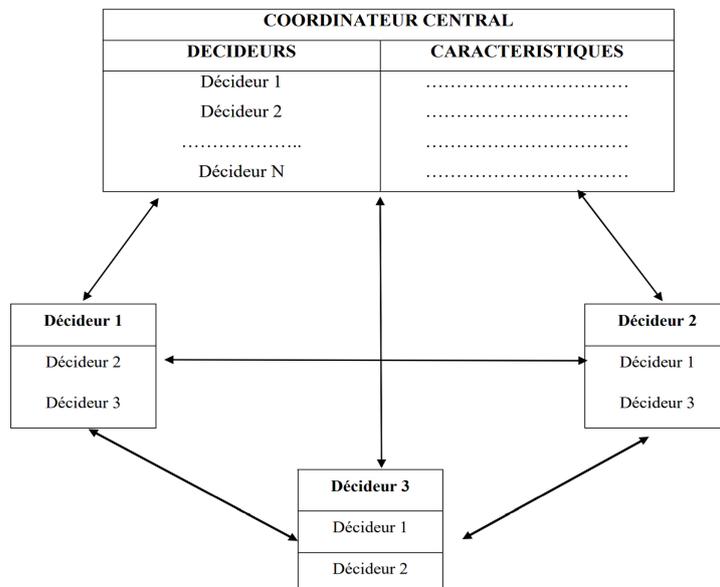


FIG. 2.3 : Architecture hybride [1]

V. Les composantes du GDSS

plutôt qu'un simple individu. Il existe trois types fondamentaux de composants qui composent les GDSS :[11]

1. Le logiciel : La partie logicielle peut être composée des éléments suivants :

- bases de données et capacités de gestion des bases de données.
- interface utilisateur/système avec accès multi-utilisateurs.
- applications spécifiques pour faciliter les activités des décideurs de groupe.
- capacités de modélisation.

2. Le matériel : La partie matérielle peut être constituée des éléments suivants :

- Périphériques d'entrée/sortie,
- PC ou stations de travail,
- moniteurs individuels pour chaque participant ou un écran public pour le groupe,
- un réseau pour relier les participants entre eux.

3. Les personnes :

- Les personnes peuvent comprendre les participants décideurs et/ou l'animateur.
- A facilitateur est une personne qui dirige le groupe tout au long du processus de planification.

VI. Les avantages des GDSS

Il est essentiel que la direction soutienne son utilisation. Si la direction ne croit pas que le GDSS, et le GDSS axé sur les communications bénéficieront à l'organisation, il sera difficile de convaincre les gens d'utiliser le système.

En revanche, si la direction soutient la mise en œuvre et l'utilisation des nouveaux outils, plusieurs effets positifs peuvent positifs.

Tout d'abord, lorsque le support de groupe est introduit dans une entreprise, il devrait augmenter la productivité de ses utilisateurs.

Cela se produit parce qu'une quantité accrue de travail peut être accomplie en moins de temps. de travail peut être accomplie en moins de temps et parce que la communication entre les communication améliorée entre les employés. Deuxièmement, le logiciel de support de groupe facilite le travail en équipe grâce à une communication ouverte. Enfin, certains logiciels de groupe permettent de documenter les informations professionnelles importantes dans un endroit pratique.

Enfin, les logiciels de communication peuvent améliorer la communication entre la direction et le reste des employés d'une entreprise.

Selon de nombreux partisans du soutien informatisé, le principal avantage d'un GDSS est qu'il permet de gagner du temps et de l'argent.

Comment y parvient-il ?

Voici quelques-unes de ces méthodes :

- La saisie simultanée permet d'optimiser le temps de l'équipe et de créer des idées de meilleure qualité.
- Le système informatique enregistre les idées en vue de leur distribution et d'un travail ultérieur.
- Le système informatique enregistre les idées en vue de leur diffusion et de leur travail futur.
- Dans certains cas, un GDSS donne accès à des informations qui permettent à un groupe d'utiliser des données extérieures tout en travaillant dans le système.
- Les réunions peuvent avoir lieu dans la même salle ou dans le monde entier.
- Les frais de déplacement peuvent être réduits.
- Une vidéo-conférence permet à un membre de l'équipe de discuter d'alternatives avec des membres distants. [12]

VII. Facteurs qui affectent le GDSS

La recherche indique qu'il y a généralement plusieurs facteurs qui affectent les GDSS :[13]

- **Anonymat :** Le degré d'anonymat que les utilisateurs de GDSS peuvent conserver est appelé anonymat. Comme les utilisateurs restent anonymes, ils peuvent être plus enclins à communiquer librement leurs pensées, leurs idées et leurs inquiétudes sans craindre d'être punis ou soumis à la pression de leurs pairs. Cependant, l'anonymat peut également entraîner un manque de responsabilité, ce qui peut avoir un impact négatif sur les résultats

de la prise de décision.

- **Conception de la facilité** : Le processus de prise de décision peut être influencé par l'aménagement physique de l'établissement où le GDSS est utilisé. La façon dont les participants interagissent avec la technologie et entre eux peut être influencée par des facteurs tels que la taille de la salle, la disposition des sièges, l'éclairage et le niveau sonore.
- **Écrans publics multiples** : Les écrans publics multiples peuvent afficher des informations et des données que tous les participants peuvent voir en même temps, ce qui permet de garder tout le monde sur la même longueur d'onde. Bien que cela puisse parfois entraîner une surcharge d'informations et une distraction, cela peut contribuer à améliorer la communication et la collaboration entre les membres de l'équipe.
- **Bases de connaissances et bases de données** : En ayant accès à ces ressources, les utilisateurs peuvent avoir accès à des faits pertinents qui peuvent les aider à prendre des décisions. L'exactitude et l'efficacité du GDSS peuvent toutefois être affectées par la pertinence et la qualité des données.
- **Vitesse du réseau de communication** : L'efficacité et l'efficacité du GDSS peuvent être affectées par la vitesse et la fiabilité du réseau de communication. Le processus de prise de décision peut être retardé par des réseaux lents ou instables.
- **Méthodologie fixe ou personnalisée** : L'utilisation de procédures décisionnelles fixes ou personnalisées peut avoir un impact sur la façon dont les utilisateurs interagissent avec le GDSS et l'utilisent. Les procédures fixes offrent un cadre clair et un ensemble de règles pour la prise de décision, mais elles peuvent être rigides et incapables de prendre en compte les exigences et les préférences particulières du groupe.
- **Conception du logiciel** : L'architecture et les fonctionnalités du logiciel du GDSS peuvent avoir un impact sur la façon dont les utilisateurs interagissent avec le système et prennent des décisions. L'implication et la collaboration des membres de l'équipe peuvent

être facilitées par un logiciel convivial doté d'interfaces claires.

- **Taille et composition du groupe** : La dynamique et les résultats du processus décisionnel peuvent être influencés par la taille et la composition du groupe. Les petits groupes peuvent manquer de diversité de points de vue et d'idées, tandis que les grands groupes peuvent avoir du mal à atteindre un consensus.
- **Satisfaction** : La satisfaction des participants à l'égard du GDSS peut avoir un impact sur leur engagement, leur motivation et leur expérience globale. Une satisfaction élevée peut conduire à de meilleurs résultats, tandis qu'une faible satisfaction peut conduire à un désengagement et à des résultats négatifs.

VIII. Exemples de GDSS

1. Microsoft Teams :

Microsoft Teams est une plateforme de collaboration et de communication développée par Microsoft qui fournit une gamme d'outils et de fonctionnalités pour aider les équipes à travailler ensemble et à prendre des décisions plus efficacement.[14]

On peut aussi voir sur la figure 2.5 ce qui est affiché à l'interface du logiciel

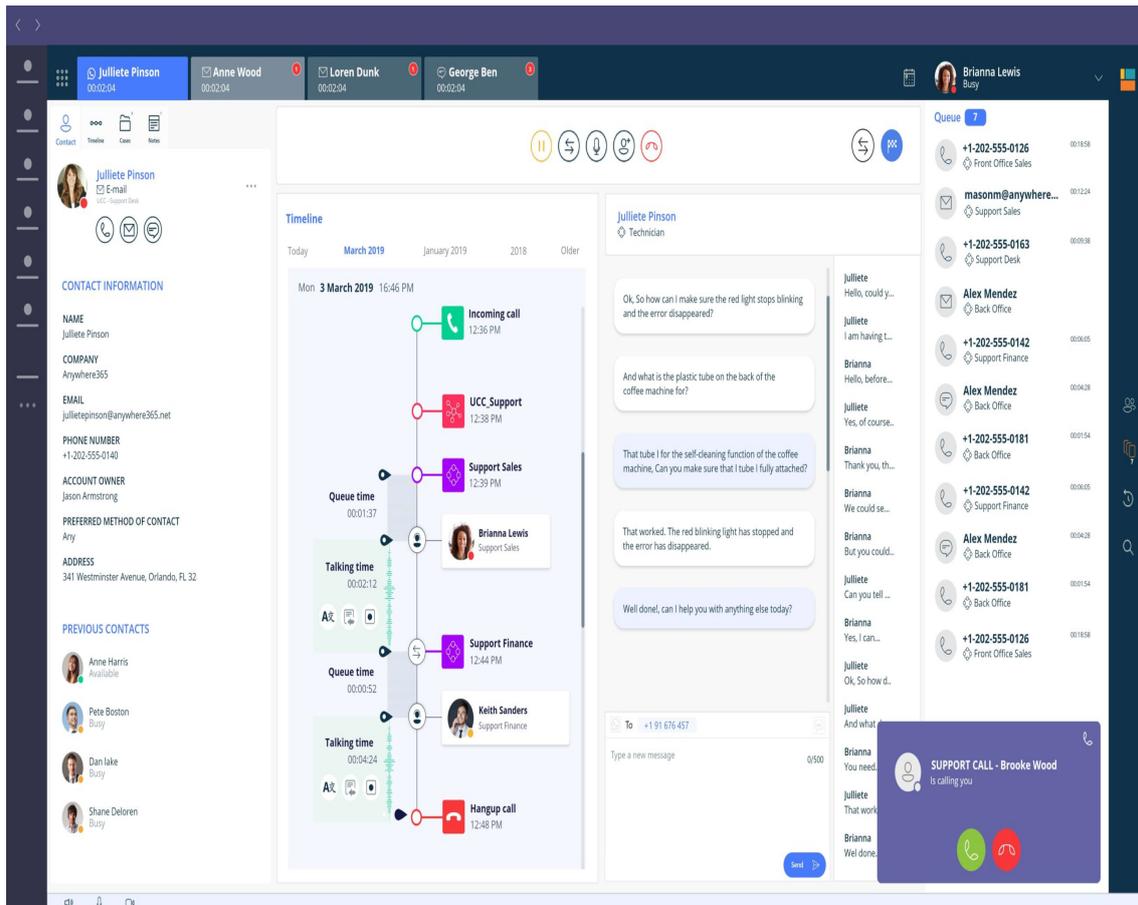


FIG. 2.4 : l'interface de Microsoft Teams [14]

Parmi les principaux outils et fonctionnalités offerts par Microsoft Teams :

- Communication en temps réel :
Les équipes peuvent utiliser le chat, les appels et la vidéoconférence pour communiquer entre elles en temps réel, partager des informations et échanger des idées. Cela peut aider les équipes à prendre des décisions plus rapidement et plus efficacement.
- Partage de fichiers :
Les équipes peuvent utiliser l'outil Fichiers de Microsoft Teams pour stocker, partager et collaborer sur des documents, des feuilles de calcul et des présentations. Cela peut aider les équipes à accéder aux informations dont elles ont besoin.
- Gestion des tâches :
Les équipes peuvent utiliser l'outil Tâches de Microsoft Teams pour assigner des tâches, suivre leur progression et fixer des échéances. Cela peut aider les équipes à hiérarchiser leur charge de travail et à s'assurer que tout le monde est sur la même longueur d'onde.
- Modèles de prise de décision :

Les équipes peuvent utiliser des modèles dans Microsoft Teams, tels que des matrices de décision et des sondages de vote, pour les aider à structurer leur processus décisionnel.

- Tableau blanc :

Les équipes peuvent utiliser la fonction de tableau blanc de Microsoft Teams pour faire du brainstorming et visualiser des idées ensemble en temps réel.

On peut aussi voir sur la figure 2.5 ce qui est affiché à l'interface du logiciel

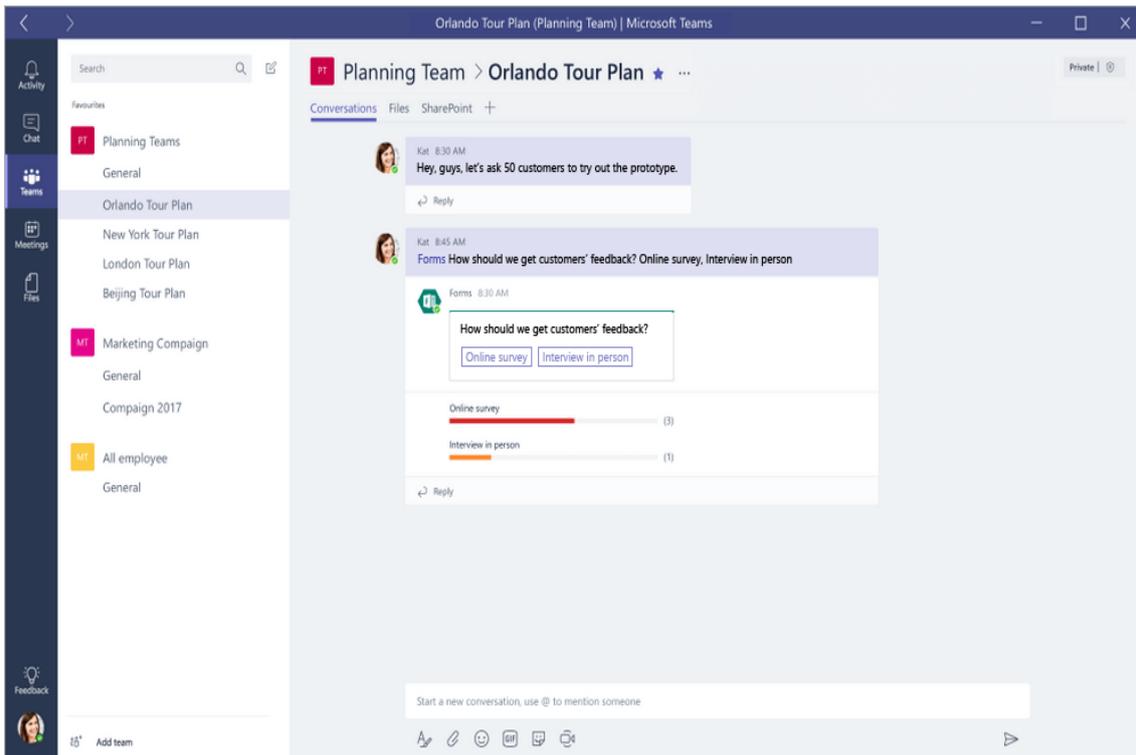


FIG. 2.5 : l'interface de Microsoft Teams [14]

2. ThinkTank :

est une plateforme logicielle qui applique l'engagement numérique et la productivité de la main-d'œuvre à distance pour transformer la façon dont les dirigeants engagent les parties prenantes sur des projets essentiels à la mission qui nécessitent un engagement et un alignement des parties prenantes. Basé sur trente ans de recherche cognitivo-comportementale sur la dynamique du consensus.[15]

On peut aussi voir sur la figure 2.6 ce qui est affiché à l'interface du logiciel

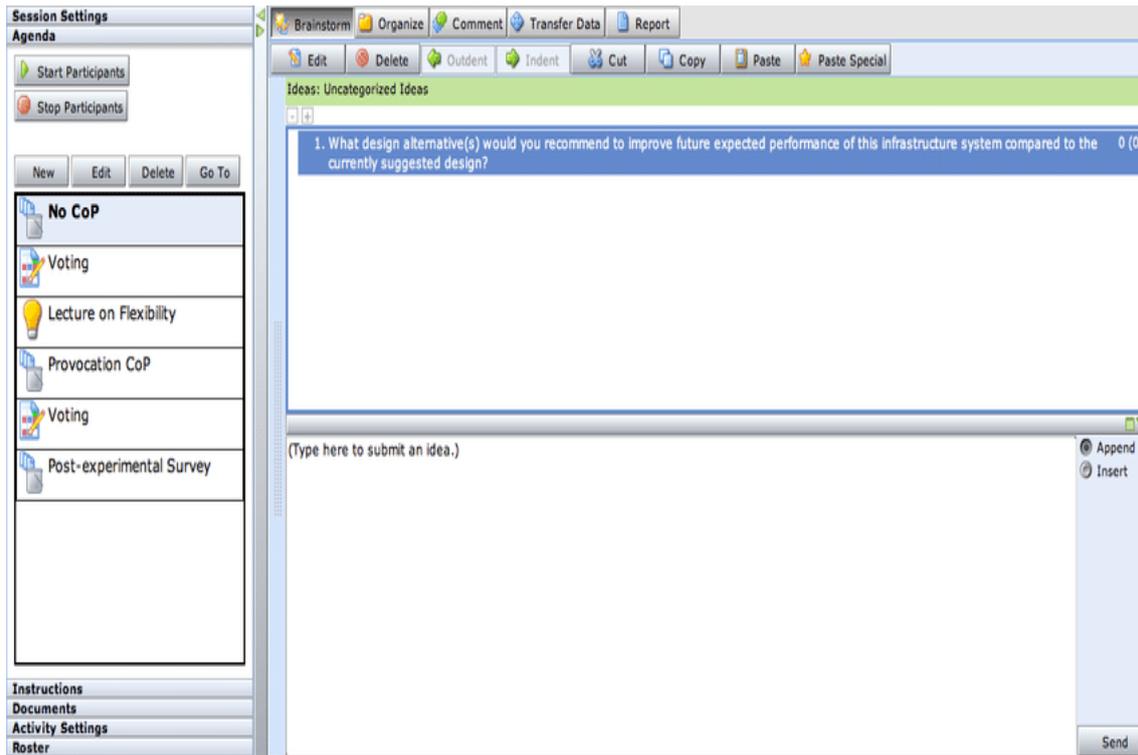


FIG. 2.6 : l'interface de ThinkTank [15]

- permet aux responsables de guider des équipes distribuées dans le cadre de programmes complexes de planification et de transformation.
- La plate-forme combine un ensemble d'outils de productivité et de facilitation de la main-d'œuvre à distance qui simplifient le processus d'idéation, de catégorisation, de hiérarchisation et d'alignement nécessaire pour parvenir à un consensus de groupe.
- Aspects essentiels de la planification stratégique, de la gestion des risques et des programmes de transformation.
- La plateforme comprend des outils en temps réel et asynchrones pour la présentation interactive, le crowdsourcing, le brainstorming et la collecte rapide d'informations ou d'exigences.
- Les équipes peuvent évaluer, voter, s'aligner et parvenir à un consensus grâce à des rapports détaillés, des données exportables et des analyses.

3. Lucid meetings :

est le logiciel de gestion des réunions le plus performant du marché.

Il permet aux équipes d'exploiter les meilleures pratiques à grande échelle, avec des résultats

tangibles et mesurables.

fournit la formation, les services et la technologie permettant d'améliorer les réunions d'affaires quotidiennes[16]

On peut aussi voir sur la figure 2.7 ce qui est affiché à l'interface du logiciel

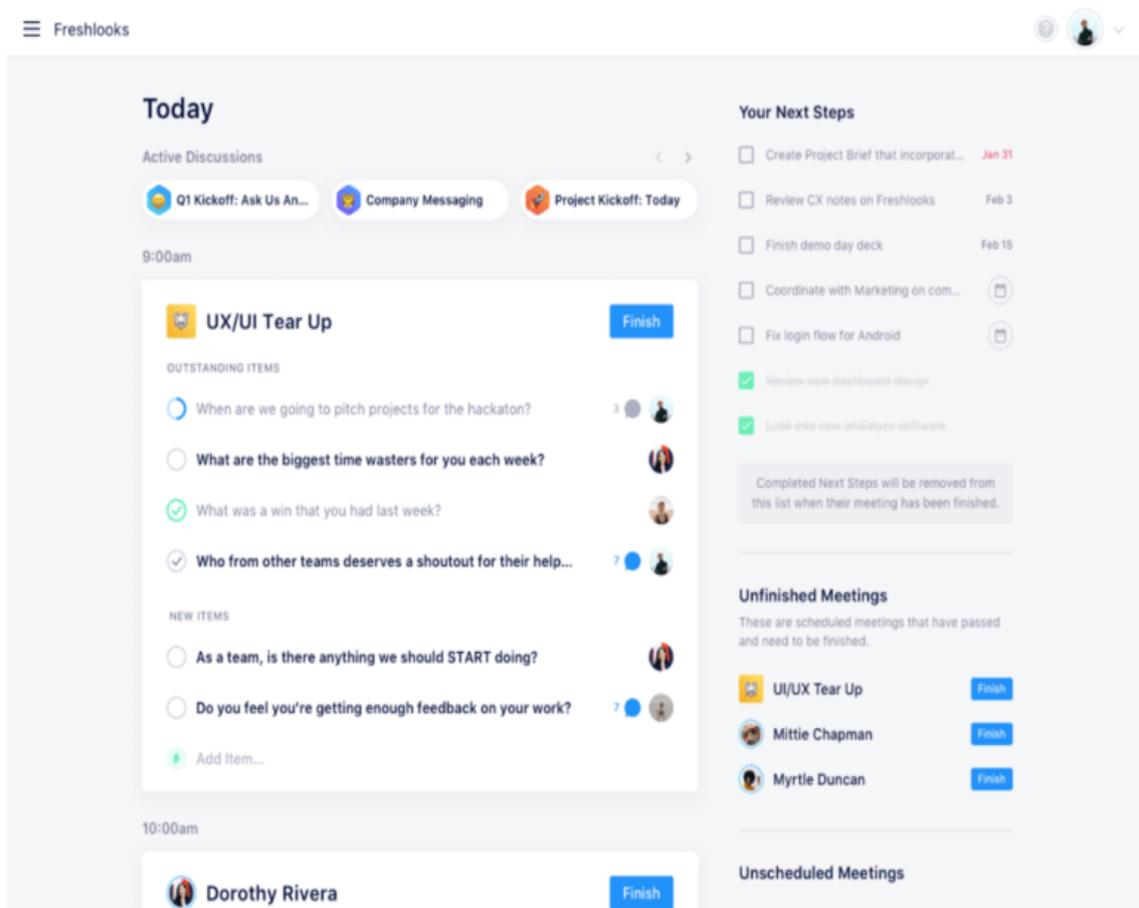


FIG. 2.7 : l'interface de lucid meetings [16]

3.1. Fonctionnalité :

1. Avant la reunion :

- Programmation de la réunion.
- Séries de réunions récurrentes.
- Ordres du jour et notes de reunion.
- Modèles d'ordre du jour de reunion.
- Invitations à des reunions.
- Rappels de reunion.

1. Durant la reunion :

- Réunion interactive(en ligne).
- Assistance aux participants à distance.
- File d'attente des orateurs.
- Ordre du jour automatisé.
- Gestion du temps de l'ordre du jour.
- Suivi des presences.
- Stationnement des sujets.
- Motions et votesPrésentation des documents.
- Audioconférence.
- Intégration d'applications externs.

2. Après la reunion :

- Enquête de satisfaction sur la réunion.
- Rapport sur l'efficacité de la réunion.
- Dossiers de réunion professionnels.
- Distribution automatique des comptes rendus.
- Rapport sur les présences.
- Rapport sur les points d'action.
- Recherche d'enregistrements en texte intégral.
- Alertes et rappels.
- Automatisation du flux de travail.

3.2. Autre fonctionalite :

- Exporter vos données.
- Formation personnalisée.
- Base de données et URL privées.
- Cloud privé virtuel (Amazon AWS).
- Autorisation Microsoft Azure AD.
- Intégration LDAP personnalisée.
- Ressources gratuites pour organiser de bonnes réunions.

IX. conclusion

les GDSS sont des outils essentiels à la prise de décision. Les GDSS peuvent aider les décideurs à prendre des décisions plus éclairées, opportunes et fructueuses en leur fournissant des informations factuelles et fondées sur des données. Néanmoins, les GDSS doivent être correctement contrôlés pour garantir la qualité et la sécurité des données et des informations utilisées.

Chapitre 3

Sécurité de GDSS

Sécurité de GDSS

I. Introduction

Au fil du temps, les technologies de l'information et de la communication ont connu de nombreux développements afin de faciliter, d'améliorer et de sécuriser l'échange et le partage d'informations, de données et de fonds de diverses manières. Avec l'émergence de l'internet, les communications numériques sont apparues, permettant toutes les formes d'échange de données par le biais de transactions en ligne. L'évolution de l'internet a donné lieu à d'importants problèmes et défis en matière de sécurité, ainsi qu'aux stratégies correspondantes pour y faire face. Ces questions ont un impact croissant sur la confiance, qui est la clé de voûte de notre société, car toute interaction humaine se fait par le biais de la confiance. La société de l'information a également besoin de confiance pour continuer à fonctionner. Nous montrerons comment cette technologie peut être utilisée pour partager et contrôler en toute sécurité des informations entre des parties qui ne se font pas nécessairement confiance, et comment elle peut améliorer la façon dont nous traitons les transactions. Le chapitre couvre les aspects suivants : illustration du concept, caractéristiques, applications, etc.

La blockchain est en fait quelque chose de plus profond : Une solution novatrice au problème humain séculaire de la confiance, qui change fondamentalement la façon dont les transactions sur Internet peuvent être effectuées en établissant la confiance entre des parties inconnues. Elle utilise la cryptographie pour protéger l'identité des utilisateurs, garantir que les transactions sont effectuées en toute sécurité, sécuriser les informations et le stockage des valeurs [20]

II. Généralités sur la Blockchain

la technologie blockchain a été proposée et déployée pour la première fois par une personne ou un groupe anonyme sous le nom de Satoshi Nakamoto, en 2008. Nakamoto a développé un système décentralisé de monnaie virtuelle basé sur un réseau pair-à-pair qui s'appuyait sur une nouvelle technologie, appelée plus tard "blockchain", pour créer le bitcoin, la célèbre et controversée crypto-monnaie.

Le système proposé permettrait aux paiements en ligne d'être envoyés directement d'une partie à une autre sans passer par un tiers de confiance. Le bitcoin permet la création d'un environ-

nement décentralisé où les transactions et les données validées par cryptographie ne sont pas sous le contrôle d'une autorité centrale ou d'intermédiaires. [21]

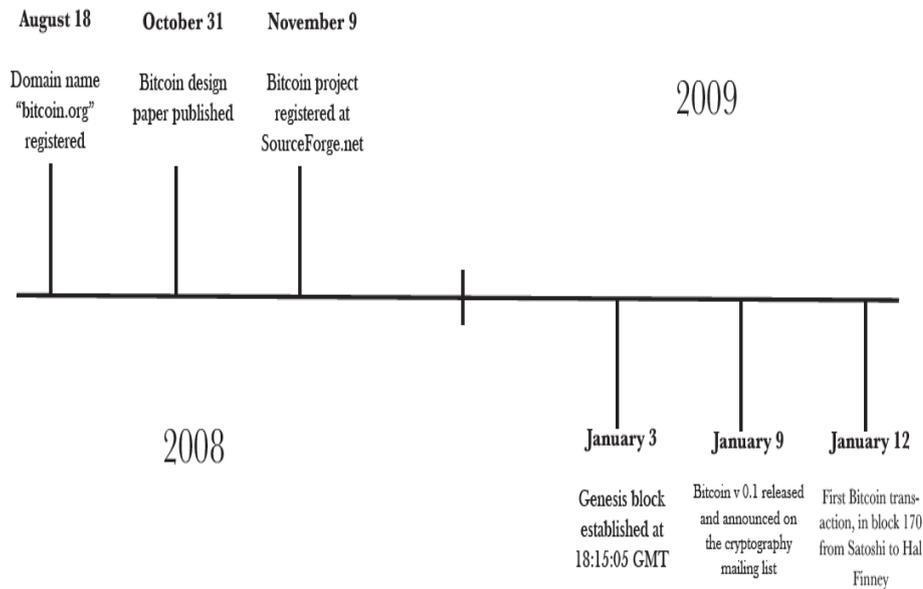


FIG. 3.1 : Histoire de la Blockchain[22]

1. Définition

La blockchain peut être considérée comme un grand livre numérique inviolable et mis en oeuvre de manière distribuée (c'est-à-dire sans dépôt central) et généralement sans autorité centrale (c'est-à-dire une banque, une entreprise ou un gouvernement).

À leur niveau de base, elles permettent à une communauté d'utilisateurs d'enregistrer des transactions dans un grand livre partagé au sein de cette communauté, de telle sorte que dans le cadre du fonctionnement normal du réseau Blockchain, aucune transaction ne peut être modifiée une fois publiée [23].

Blockchain est une technologie de registre distribué qui permet des transactions sécurisées et transparentes d'actifs numériques. blockchain fonctionne sur un réseau décentralisé, ce qui permet d'enregistrer et de vérifier les données sans avoir recours à des intermédiaires. Cette technologie offre une sécurité, une confidentialité et une efficacité inégalées dans les transactions

et la gestion des données. [24]

Sur la base des définitions ci-dessus, la blockchain peut être caractérisée comme un grand livre public, décentralisé et distribué, composé de nombreux pairs, appelés nœuds. tous les nœuds possèdent une copie du même livre, stockés dans des blocs constitués de groupes de transactions.

La blockchain est sécurisée et inaltérable, et sa transparence découle de l'enregistrement historique de toutes les transactions qu'elle contient.

2. Caractéristiques

La blockchain a de nombreuses caractéristiques : [25]

Décentralisation :

La gestion traditionnelle des transactions repose sur une validation centrale par un organisme de confiance, tel qu'une banque ou un gouvernement. Cette approche centralisée entraîne des coûts supplémentaires, des restrictions de performance et un risque de défaillance en un point unique chez les fournisseurs de services centralisés. En revanche, la blockchain permet la validation des transactions de pair à pair sans qu'il soit nécessaire de recourir à une authentification, une intervention ou une juridiction centrale, ce qui réduit les coûts, améliore les performances et diminue le risque de défaillance d'un point unique.

Immutabilité :

Une blockchain est une chaîne de blocs liés où chaque bloc est lié au précédent par un hachage. une fois qu'une transaction est ajoutée à une blockchain, elle ne peut être supprimée ou mise à jour. Toute modification d'un bloc précédent rend tous les blocs suivants invalides, ce qui permet de détecter facilement toute falsification.

Le consensus :

Aucun bloc ne peut être ajouté sans l'approbation de certains nœuds du réseau, conformément à un mécanisme de consensus bien connu qui est au cœur de la blockchain. Par conséquent, les nœuds peuvent ne pas se faire confiance entre eux, mais ils peuvent faire confiance à l'ensemble du système. Il existe de nombreux algorithmes de consensus différents selon le type ou le cas d'utilisation de la blockchain.

Transparency :

Pour la plupart des systèmes de blockchain publics, chaque utilisateur peut accéder et interagir avec le réseau de la blockchain avec un droit égal. En plus, chaque nouvelle transaction

est validée et sauvegardée dans la blockchain, et est donc disponible pour chaque utilisateur. Par conséquent, les données de la blockchain sont essentiellement transparentes pour chaque utilisateur qui peut accéder et vérifier les transactions engagées dans la blockchain.

L'anonymat :

Malgré la transparence des données de la blockchain, les systèmes de blockchain peuvent préserver un certain niveau de confidentialité en rendant les adresses de la blockchain anonymes.

Traceability :

Chaque transaction enregistrée dans la blockchain est assortie à un horodatage . Par conséquent, les utilisateurs peuvent facilement vérifier et retracer l'origine des éléments de données historiques après avoir analysé les données de la blockchain avec les horodatages correspondants.

3. Types :

Il existent différents modèles de conception de la Blockchain. Les termes "public" et "sans permission" sont utilisés de manière interchangeable, tout comme les termes "privé" et "avec permissions". En fonction du cas d'utilisation, il faut choisir une architecture appropriée parmi celles définies dans le tableau 1[26]

	Avec Permission de lecture	Sans Permission de lecture
permission d'écriture	Blockchain privée	Blockchain gouvernementale
Sans permission d'écriture	Surveillance/assurance	Blockchain publique

TAB. 3.1 : Caractéristiques de différents Blockchains

Il existe différentes configurations de systèmes basés sur la blockchain en fonction de plusieurs paramètres tels que la performance, la rentabilité et la flexibilité. Différentes dimensions d'un système de blockchain, telles que la configuration de la blockchain, le stockage, le calcul et le degré de décentralisation, sont prises en compte pour établir la classification.

3.1. Blockchain publique (permission-less Blockchain)

Une blockchain publique est un système distribué décentralisé dans lequel un nombre indéterminé de participants peuvent partager et vérifier mutuellement les informations relatives

aux transactions se produisant dans le système. Il n’y a pas d’entité de gestion distincte. Tout le monde peut participer de manière anonyme, et il n’y a aucune restriction sur l’autorité. Les blockchains publiques peuvent être utilisées efficacement dans le secteur financier par le biais de transactions telles que les crypto-monnaies, mais aussi dans d’autres domaines tels que le crowdfunding (un moyen de lever des fonds pour financer des projets et des entreprises) et le transport. En effet, une blockchain publique permet d’effectuer le processus d’authentification sans tiers de confiance. En outre, la blockchain publique est une blockchain ouverte qui permet à quiconque de créer des transactions et de participer en tant que nœud. Elle offre également une fiabilité et une intégrité élevées grâce à la vérification du travail des participants. Malgré ces avantages, il existe toutefois un inconvénient : les vitesses d’enregistrement et de traitement peuvent diminuer car les enregistrements des transactions de tous les participants sont stockés et partagés.[34]

3.2. Blockchain privée (permissioned Blockchain)

Les blockchains de permission sont généralement construites par des organisations pour leurs besoins commerciaux spécifiques. Les blockchains sont susceptibles d’avoir des interfaces avec les applications existantes de l’organisation. Les organisations peuvent opter pour des blockchains de consortium où des membres de confiance limités doivent obligatoirement signer une transaction. Dans les blockchains entièrement privées, l’autorisation d’utiliser la blockchain est accordée à une organisation centrale. [26]

3.3. Blockchain de consortium

Il s’agit d’un autre type qui n’est pas beaucoup mentionné dans la littérature, Ce type de Blockchain peut être considéré comme une Blockchain partiellement privée et semi-décentralisée, dans laquelle aucune organisation unique ne gère le processus de consensus et la validation des blocs, mais plutôt par un ensemble de nœuds présélectionnés (comme le montre la figure 3.2). Ces nœuds décident qui peut participer au réseau et qui peut prendre part au mécanisme de consensus. Il s’agit donc d’un système partiellement centralisé en raison du contrôle exercé par certains nœuds de validation sélectionnés . Parmi les exemples de blockchains de consortium, citons Ripple, R3, etc.

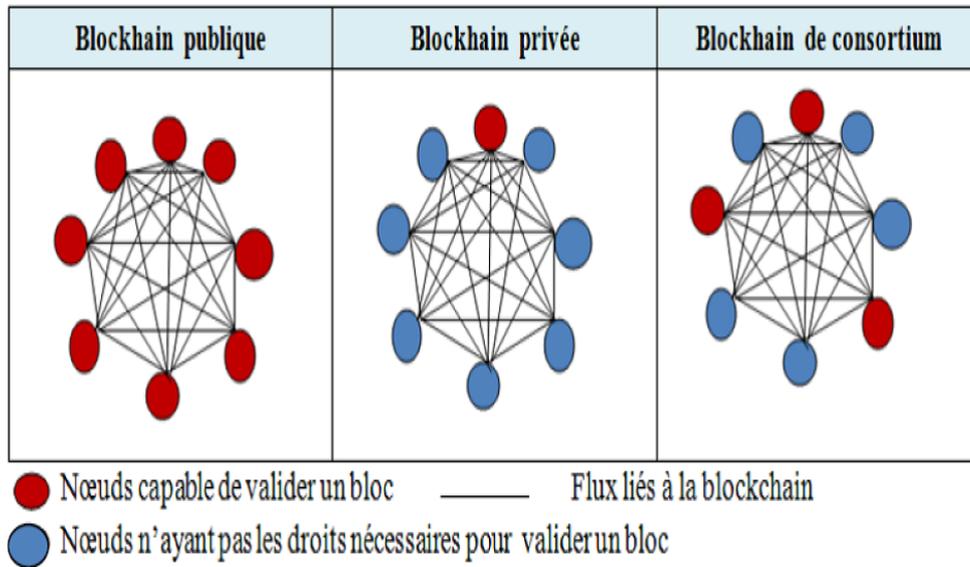


FIG. 3.2 : les types de la Blockchains[27]

Propriété	public	privé	consortium
décentralisation	Décentralisé	Centralisé	Partiel
Immutabilité	Immuable	Partiellement modifiable	Immuable
Non-répudiation	Non-refusable	Refusable	Partiellement refusable
Transparence	Transparent	Opaque	Partiellement transparent
Traçabilité	Traçable	Traçable	Partiellement traçable
Scalabilité	Faible	Supérieure	Bien
Flexibilité	Faible	Supérieure	Bien
Permission	Sans permission	Avec permission	Avec permission
Consensus	PoW, PoS	Ripple	PBFT, PoA, PoET
Exemples	Bitcoin, Ethereum	GemOS , Multi-chain	Hyperledger, Ethereum

TAB. 3.2 : un tableau comparatif des types de la Blockchain [28]

4. Protocoles de consensus

Comment atteindre un consensus dans une blockchain est un défi car le réseau de la blockchain est distribué. Dans la blockchain, il n'y a pas de nœud central qui garantit que les registres sur les nœuds distribués sont tous identiques. Les nœuds ne doivent pas faire confiance aux autres nœuds. Ainsi, certains protocoles sont nécessaires pour s'assurer que les grands livres

dans les différents nœuds sont cohérents. Nous présentons ensuite plusieurs approches communes pour atteindre le consensus dans la blockchain.

4.1. Pow (proof of work)

La preuve de travail (PoW) est un algorithme de consensus basé sur la preuve. Le concept de base de cette technique de consensus est d'identifier et de déterminer le nœud qui obtiendra le droit d'ajouter un nouveau bloc à la chaîne existante en fournissant une preuve suffisante de son effort. Le mécanisme PoW utilise la résolution de puzzle pour prouver la crédibilité des données. Le puzzle est généralement un problème mathématique complexe requérant une forte puissance de calcul pour y parvenir, difficile à calculer, mais facilement vérifiable. Lorsqu'un nœud crée un bloc, il doit résoudre un puzzle PoW. Une fois le puzzle résolu, il est diffusée aux autres nœuds pour les vérifier, afin d'atteindre l'objectif du consensus. Comme le PoW devient plus difficile avec le temps, Les mineurs sont certains nœuds du réseau consacrent des ressources à la vérification des transactions et au maintien de la sécurité de la Blockchain. Les mineurs sont payés par des récompenses de bloc. Pour chaque nouveau bloc, une récompense de bloc est attribuée à un seul mineur ou à un petit groupe de mineurs .les mineurs unissent leurs efforts pour obtenir plus de puissance de calcul en formant des groupes. Ces groupes sont connus sous le nom de pools miniers. Cette technique permet aux personnes qui font équipe d'augmenter leurs chances de miner de nouveaux blocs et donc de percevoir les récompenses. Cependant, ces techniques peuvent être dangereuses pour la sécurité de la blockchain. Si une entité (ou une minorité) contrôle une grande partie de la blockchain , elle sera en mesure de centraliser le processus de minage. C'est ce qu'on appelle une attaque 51 % et elle a d'abord été discutée comme un point faible de l'algorithme PoW : si un seul mineur ou un groupe de mineurs peut obtenir 51 de la puissance de hachage, il peut effectivement contrôler la blockchain.[29]

4.2. PoS (Proof of Stake)

Même si le bitcoin montre clairement qu'une monnaie numérique basée sur la preuve de travail est viable, des faiblesses existent toujours. C'est pourquoi de nombreux autres mécanismes de consensus ont été développés afin de fournir un algorithme alternatif à la PoW. Par rapport à la méthode PoW, la méthode PoS (proof-of-stake) peut constituer une alternative économe en énergie. Dans cette méthode de consensus, le mineur n'a pas besoin de gaspiller une énorme

quantité de ressources informatiques pour résoudre l'énigme mathématique. Au lieu de cela, il doit avoir un intérêt suffisant dans le système pour participer au processus de création de blocs .

La chance d'avoir la possibilité de valider un bloc dépend entièrement de l'enjeu ou de la richesse du nœud participant. On pense qu'une participation suffisante dissuadera la possibilité d'une attaque malveillante sur le réseau. [29]

4.3. DPOS (Delegated proof of stake)

Le mechanism de Delegated Proof of Stake (DPoS) est une variante du Proof of Stake (PoS). La principale différence entre PoS et DPOS est que PoS est une démocratie directe tandis que DPOS est une démocratie représentative. Les parties prenantes élisent leurs délégués pour générer et valider les blocs. Avec beaucoup moins de noeuds pour valider le bloc, celui-ci peut être confirmé rapidement, ce qui entraîne une confirmation rapide des transactions. Parallèlement, les paramètres du réseau, tels que la taille et l'intervalle des blocs, peuvent être réglés par les délégués. En outre, les utilisateurs n'ont pas à s'inquiéter des délégués malhonnêtes car ils peuvent être éliminés facilement [29].

La principale différence entre le PoS et le DPoS est que dans le DPoS, les parties prenantes élisent des délégués pour générer et valider un bloc. Avec beaucoup moins de nœuds pour valider le bloc, celui-ci peut être confirmé rapidement.

Propriété	PoW	PoS	DPoS
Gestion de l'identité du nœud	Ouvert	Ouvert	Ouvert
Consommation d'énergie	Haute	Faible	Très Faible
Tolérance aux adversaires	< 25%	<51%	< 51%
Scalability	Forte	Forte	Forte
Performance (transactions par seconde)	<20	<20	<500
Temps de confirmation du consensus	Élevé	Élevé	Moyen
Vitesse de création des blocs	Lente	Rapide	Dépend de la variante

TAB. 3.3 : Comparaison entre les différents algorithmes de consensus [30]

5. Domaines d'application de la Blockchain :

La technologie blockchain est largement reconnue pour son utilisation dans les crypto-monnaies. Cela est dû au fait que la première blockchain, introduite par Satoshi Nakamoto dans le Bitcoin[21], était également la première crypto-monnaie. L'importance de la blockchain réside dans sa capacité à permettre le transfert de valeur au lieu de simples copies de données. Cette caractéristique révolutionnaire a été rendue possible en empêchant la double dépense et en établissant la confiance entre des participants à des transactions auparavant anonymes, sans recourir à des intermédiaires. Le succès des crypto-monnaies a capté l'attention et stimulé l'imagination des développeurs et des innovateurs, les amenant à explorer le potentiel de la blockchain au-delà du secteur financier. En conséquence, la technologie a été adaptée pour être utilisée dans diverses industries. [30]

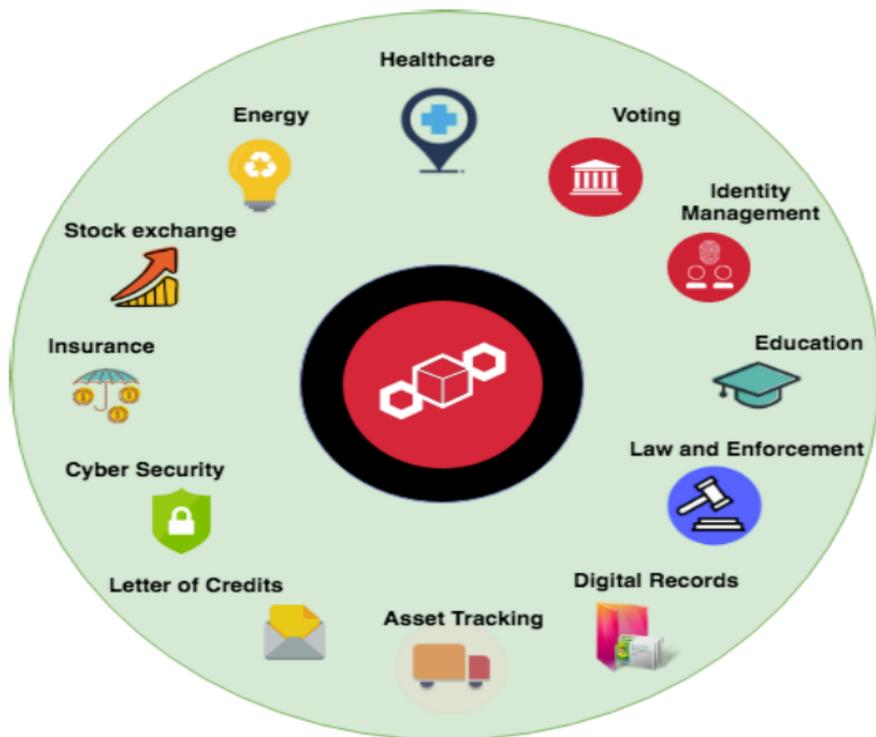


FIG. 3.3 : Domaines d'application de la technologie Blockchain. [30]

6. défis de la Blockchain :

Comme toute autre technologie révolutionnaire, Blockchain a ses avantages et ses inconvénients.

- Confidentialité : Comme Blockchain est basé sur un réseau de consensus distribué sans partie de confiance centralisée, toutes les transactions sont transparentes et annoncées au public.

Par conséquent, la vie privée dans Blockchain est maintenue par la rupture du flux d'informations.

La rupture du flux signifie que le public peut voir toutes les transactions, mais sans information reliant la transaction aux identités.

Pour ce problème de confidentialité, de nombreuses études ont proposé différents types de contre-mesures et de modèles de confidentialité pour augmenter l'anonymat dans Blockchain. Ces solutions proposées sont présentées sur la base d'une revue systématique de la littérature.[20]

- Les clés privées : chaque compte Blockchain a deux clés correspondantes :
 1. une clé publique (partagée) .
 2. une clé privée (secrète).

Les utilisateurs ont besoin de leur clé privée pour accéder à leurs fonds, ce qui signifie qu'ils agissent comme leur propre banque, Si un utilisateur perd sa clé privée, les données est alors concrètement perdu et il ne peut rien y faire.

- La consommation d'énergie :

LE POW nécessite une puissance de calcul élevée qui augmente également au fur et à mesure que le niveau de difficulté s'élève, Ce niveau de difficulté s'accroît au fur et à mesure que d'autres mineurs se joignent à la course, La consommation d'une grande quantité de puissance de calcul a un effet direct sur la consommation d'électricité, L'activité associée à Bitcoin consomme directement autant d'énergie qu'un grand pays comme l'Algérie.

Selon de nouvelles estimations publiées par des chercheurs de l'université de Cambridge, la consommation annuelle est d'environ 70TWh[32]

- L'espace de Stockage :

les registres de la Blockchain peuvent devenir très volumineux avec le temps.

La croissance de la taille de la Blockchain devient supérieure à celle des disques durs, le réseau risque de perdre des noeuds si le registre devient trop volumineux pour être téléchargé et stocké par les utilisateurs, si l'on prend l'exemple du bitcoin, il contient actuellement en 2023 plus de 490 giga-octets (Go) de données de transaction[33]

7. conclusion

Dans ce chapitre, nous avons présenté la technologie de la blockchain qui est une nouvelle technologie ,Elle ne permet pas d'insertion ou d'accès sans authentification ne donne jamais la possibilité de modification. Et reste la technologie blockchain jusqu'à présent sûre grâce à l'utilisation d'un mélange de techniques de cryptographie sûre.

Tout d'abord nous avons commencé par des généralités de cette technologie .Ensuite-nous avons défini les blockchains, et mentionné ces caractéristiques , types ces protocoles de consensus , quelques domaines d'applications, et nous avons terminé par ces défis.

Chapitre 4

conception et réalisation

conception et réalisation

1. Introduction

Ce chapitre présente spécifiquement les étapes fondamentales de la conception, modélisation et la réalisation d'un système de vote en ligne basé sur la technologie blockchain. Nous avons choisi Unified Process (PU) comme méthode de conception et Unified Modeling Language (UML) comme langage de modélisation.

2. Processus unifié(UP)

Le processus unifié est un processus de développement logiciel itératif et incrémental, construit sur UML, centré sur l'architecture, piloté par des cas d'utilisation, et semble être une solution idéale aux éternels problèmes des développeurs. [35]

Comme le montre figure 4.1, le processus UP est résumée comme les étapes suivantes :

- **Spécifications** : utilisées pour définir les différentes exigences du système
 - **Fonctionnalité** : Du point de vue de l'utilisateur.
 - **Non fonctionnel** : D'un point de vue technique.
 - **Analyse** : Permet de comprendre les besoins et les exigences des clients.
 - **Conception** : Permet d'acquérir une compréhension approfondie et de déterminer la méthode pour résoudre le problème posé
 - **Implémentation** : consiste à construire un programme en utilisant un langage de programmation donnée.
 - **Tests** : permet de vérifier que le système implémente bien les fonctionnalités attendues.
- [36]

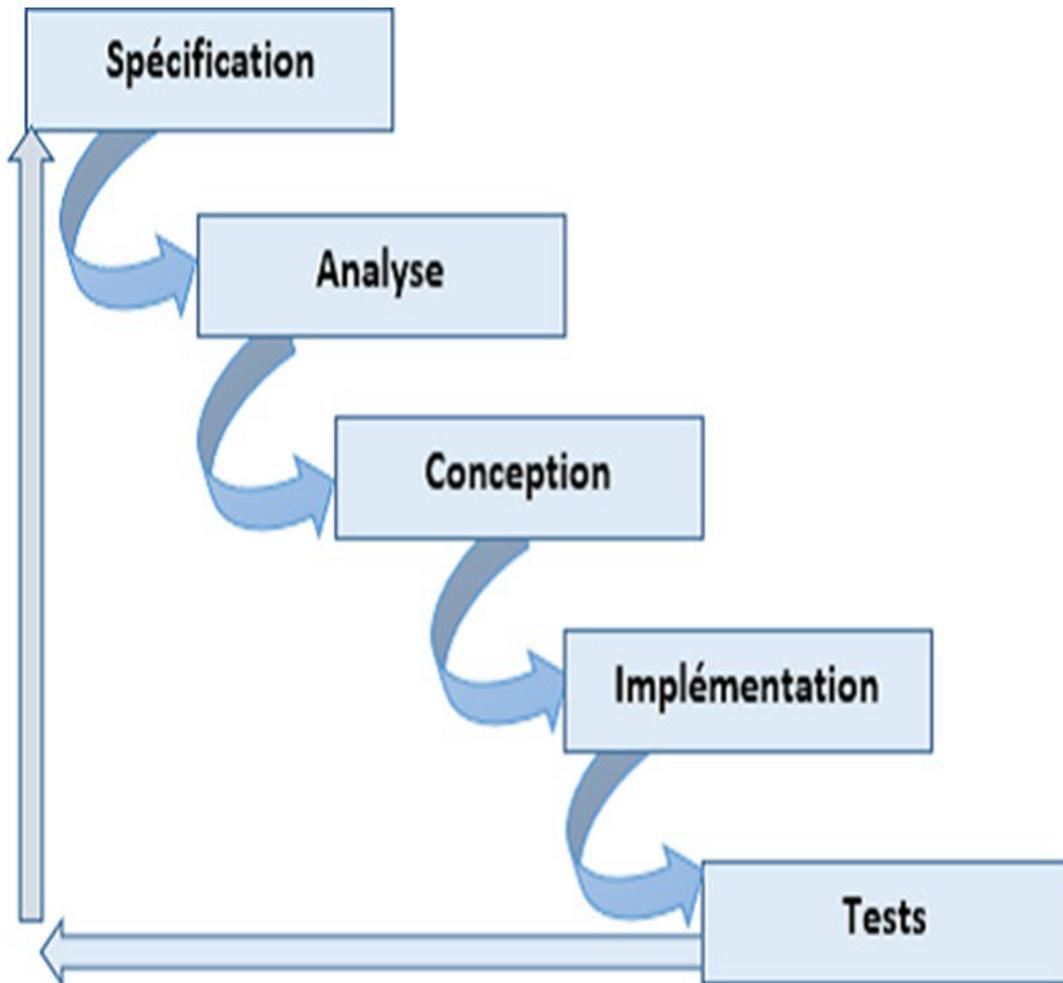


FIG. 4.1 : Le Processus UP [36]

3. Langage de modélisation unifié (UML)

UML est un langage de modélisation graphique et textuel utilisé pour comprendre et rédiger des exigences, spécifier et documenter des systèmes, concevoir des solutions et échanger des idées [37].

UML a treize diagrammes. Pour notre système, nous utilisons les trois diagrammes de base suivants :

- Le diagramme de cas d'utilisation permet d'exprimer le comportement du système sous forme d'actions et de réactions selon le point de vue de chaque utilisateur, il définit les limites du système et sa relation avec l'environnement [38].
- Diagrammes de séquence, ces diagrammes sont des représentations graphiques des interactions entre les participants et le système dans l'ordre chronologique selon la formule UML[39].

- Diagramme de classe, une représentation graphique de ce que sera l'implémentation du système. Il apporte une vue statique du système grâce à la représentation des classes et des relations entre ces dernières [40].

4. Identification des besoins

4.1. Besoins fonctionnels :

le système doit offrir les fonctionnalités suivantes :

- Lancement du vote
- Authentification des électeurs
- Ajout des candidats.
- Vote.
- Affichage des résultats.

4.2. Besoins non fonctionnels :

à part les besoins fondamentaux, notre système doit répondre aux critères suivants :

- Traçabilité** : : Les données sont enregistrées d'une manière sécurisée, dans le temps et sceller dans un registre décentralisé et infalsifiable. Les données sont ainsi certifiées et non répudiables.
- Sécurité** : : La blockchain assure un stockage des informations d'une manière non modifiable et toutes ces informations pourraient se retrouver de façon chronologique dans un registre sécurisé et aisément consultable.
- Performances** : Un logiciel doit être avant tout performant c'est à -dire à travers ces fonctionnalités, répond aux exigences des utilisateurs d'une manière optimale.
- Utilisabilité** : : Le système doit offrir à l'utilisateur une interface simple et facile à utiliser.
- Scalabilité** : : L'utilisateur doit pouvoir augmenter ses capacités de traitement, de stockage, de transmission et de réseaux selon ses besoins.

5. Diagrammes de séquence

5.1. Diagramme de séquence lancer le vote

Le diagramme de séquence "Lancer le vote" présente le séquençement des interactions entre Administrateur, Electeur et le system, l'opérateur « Alt » indique la structure conditionnelle if.

Cette condition va permettre d'afficher la page compte à rebours pour l'Administrateur et la page de vote pour l'électeur si et seulement si la différence entre les deux dates est supérieur à 0, sinon le système affiche un message fin de vote pour l'Administrateur et la page des résultats pour l'électeur.

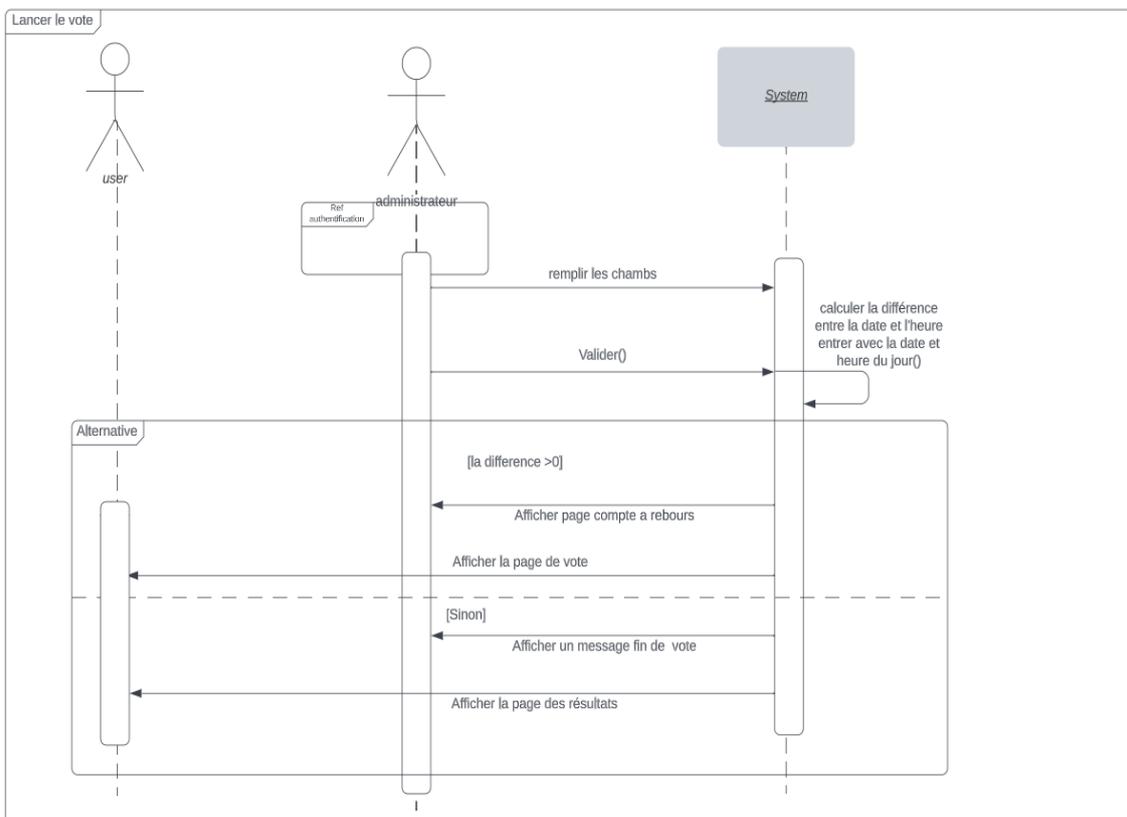


FIG. 4.2 : Diagramme de séquencer lancer le vote

5.2. Diagramme de séquence voter

Le diagramme de la séquence de vote montre la séquence d'interaction entre l'utilisateur et notre contrat intelligent. Dans ce diagramme, l'utilisateur pourra voir les candidats et voter pour l'un d'entre eux

- si l'utilisateur ne s'est pas enregistré auparavant, il n'aura pas accès à cette page.

- si l'utilisateur n'a pas encore voté, il devra choisir un candidat et voter pour lui.
- si l'utilisateur a déjà voté, l'option de vote sera annulée et seul le résultat de l'élection sera affiché.

Une fois que l'utilisateur aura appuyé sur le bouton de vote et confirmé la transaction, le système transmettra la transaction à notre contrat intelligent, enregistrera le vote et révoquera l'option de vote de l'utilisateur.

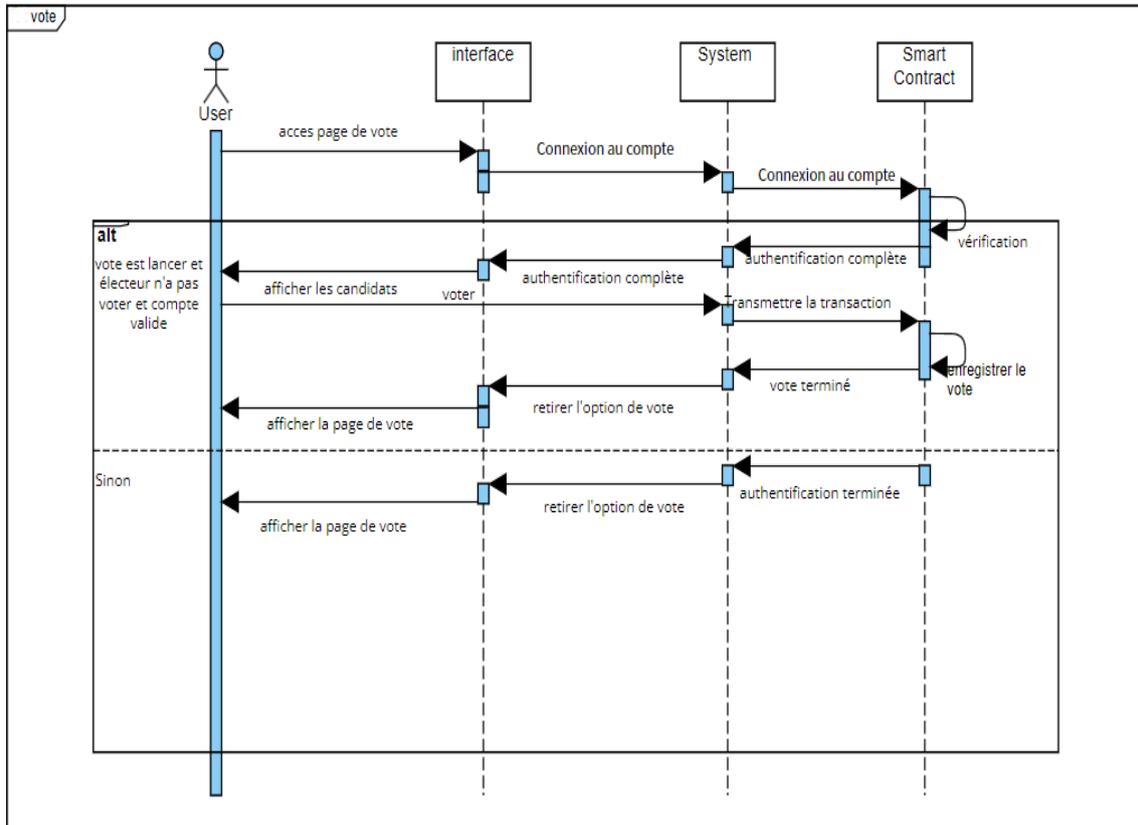


FIG. 4.3 : diagramme de séquence voter

6. Outils de développement et langages utilisés

- **Sublime texte 3** : est un éditeur de texte (beta) qui peut servir pour coder en quelques langages que ce soit du moment qu'on enregistre le fichier sous le bon format [41]
- **Ganache** : permet de créer une blockchain Ethereum pour que vous puissiez exécuter des tests, exécuter des commandes et inspecter l'état tout en contrôlant le fonctionnement de la chaîne. Il vous donne la possibilité d'effectuer toutes les actions que vous feriez sur la chaîne principale sans le coût. De nombreux développeurs l'utilisent pour tester leurs contrats intelligents pendant le développement. Il fournit des outils pratiques tels que des contrôles d'exploration avancés et un explorateur de blocs intégré[?].

Grace a ganache, nous pouvons avoir 10 comptes Ethereum avec une balance de 100 ether (du faux ether) pour chaque compte et même il nous permet d'examiner tout ce qui se passe dans cette blockchain c'est pour cela nous l'avons choisi. Pour installer ganache il faut avoir

- . Un processeur de 64 bits.
- . Système d'exploitation Windows 10.
- **Metamask** : est un portefeuille de crypto qui peut être utilisé sur les navigateurs Chrome, Firefox. C'est aussi une extension de navigateur. Il fonctionne comme un pont entre les navigateurs normaux et la blockchain Ethereum, il est accessible à tous, son but premier est de rendre le développement d'applications décentralisées plus simple [?]
- **Truffle** : est un Framework permettant aux développeurs de lancer un projet de contrat intelligent en un clic et vous fournit une structure de projet, des fichiers et des répertoires qui facilitent le déploiement et les tests [?]

Nous avons choisi truffle parce qu'il est puissant et il nous facilite l'interaction avec notre smart contract.

Il est nécessaire d'installer NodeJS sur la machine, puis Truffle par la commande suivante :
npm install -g truffle.

- **Node.js** : Un environnement d'exécution côté serveur open source basé sur le moteur JavaScript V8 de Chrome. Il peut être utilisé pour créer différents types d'applications telles que les applications Web, les applications de chat en temps réel...[42]

Pour développer des smart contracts, nous devons configurer notre environnement par l'installation de Node Package Manager(NPM), fourni avec Node.js.

- **Remix** : Un outil open source puissant qui vous aide à rédiger des contrats Solidity directement depuis le navigateur. Ecrit en JavaScript, Remix prend en charge à la fois l'utilisation dans le navigateur et localement [43]

Nous avons choisi Remix car [44] :

- Il est très pratique et très pertinent pour apprendre à coder sur Solidity
- On y accède juste par navigateur et il n'y a rien à installer
- On dispose automatiquement des dernières versions de Solidity
- Il permet de compiler et d'exécuter les smart contracts instantanément, dans toutes sortes de blockchains, c'est à dire qu'on peut déployer dans la vraie blockchain Ethereum un smart contract directement depuis Remix, mais il peut aussi se connecter à une blockchain locale comme Ganache. Il est donc très souple et flexible.

- **Bootstrap** : Bootstrap est un Framework front-end open source avec lequel vous pouvez créer des sites Web. Le Framework a été lancé en 2012 par un concepteur et développeur sur Twitter. Il contient des modèles de conception (typographie, formulaires, boutons, tableaux, etc.) basés sur CSS et HTML. Bootstrap est très souvent utilisé dans la conception de sites Web qui ont un design Web réactif afin de pouvoir afficher des pages Web sur l'ordinateur, la tablette et le smartphone [45]

- **JavaScript** : Un langage informatique utilisé sur les pages web. Ce langage est considéré comme un langage côté client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition à d'autres langages qui sont activé coté serveur comme les scripts PHP. L'exécution du code est effectuée par votre navigateur internet tel que Firefox ou Internet Explorer [46]

- **Web3.js** : Il s'agit d'une collection de bibliothèques qui vous permettent de développer des clients qui interagissent avec l'éthéréum blockchain et effectuer des actions comme envoyer Ether d'un compte à un autre, lire et écrire des données intelligents, créer des contrats intelligents, et bien plus encore [47]

Pour installer Web3.js taper la commande suivante : **npm install web3.**

- **Solidity** : Langage de programmation orienté objet, il a été développé par les principaux contributeurs de la plateforme Ethereum. Il est utilisé pour concevoir et mettre en oeuvre des contrats intelligents au sein de la plate-forme virtuelle Ethereum et de plusieurs autres plates-formes blockchain.

Solidity est de type statique, prend en charge l'héritage, les bibliothèques et les types complexes définis par l'utilisateur, entre autres fonctionnalités[48]

7. Configuration d'environnement

Nous allons d'abord créer un répertoire qui va contenir les fichiers de notre projet comme ceci :

- `mkdir election`
- `cd election`

Maintenant que nous sommes dans notre dossier, nous voulons être rapidement opérationnels avec un projet de truffles déjà existant. Donc, dans le dossier « election », exécutez la commande ci-dessous : **truffle unbox pet-shop**

Après que les dépendances sont installées, examinons la structure de répertoire de projet que nous venons de créer la figure 4.4

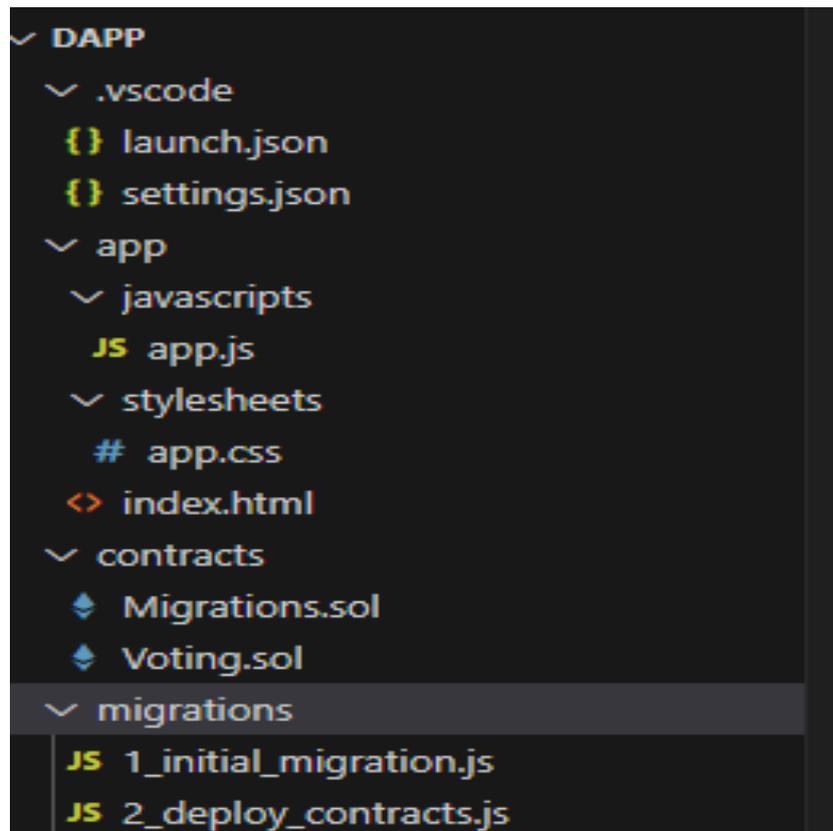


FIG. 4.4 : Structure de répertoire election.

1. **Répertoire des contrats** : c'est ici que nous conserverons tous nos contrats intelligents. Vous pouvez déjà voir que nous avons un contrat de migration à l'intérieur qui gère nos migrations vers la blockchain.
2. **Répertoire des migrations** : c'est là qu'il y a tous les fichiers de migration. Chaque fois que nous déployons des contrats intelligents sur la blockchain, nous mettons à jour l'état de la blockchain et nous avons donc besoin d'une migration.
3. **Répertoire application** : c'est ici que nous avons développé notre application.

8. Présentation des interfaces pour le vote

Dans ce qui suit nous avons choisi d'illustrer quelques interfaces de notre application.

8.1. Interface Connexion à la blockchain

L'électeur doit se connecter à la blockchain en utilisant l'extension *MetaMask* puis Importer le compte(figure 4.5) qui a été récupéré de site précédent.

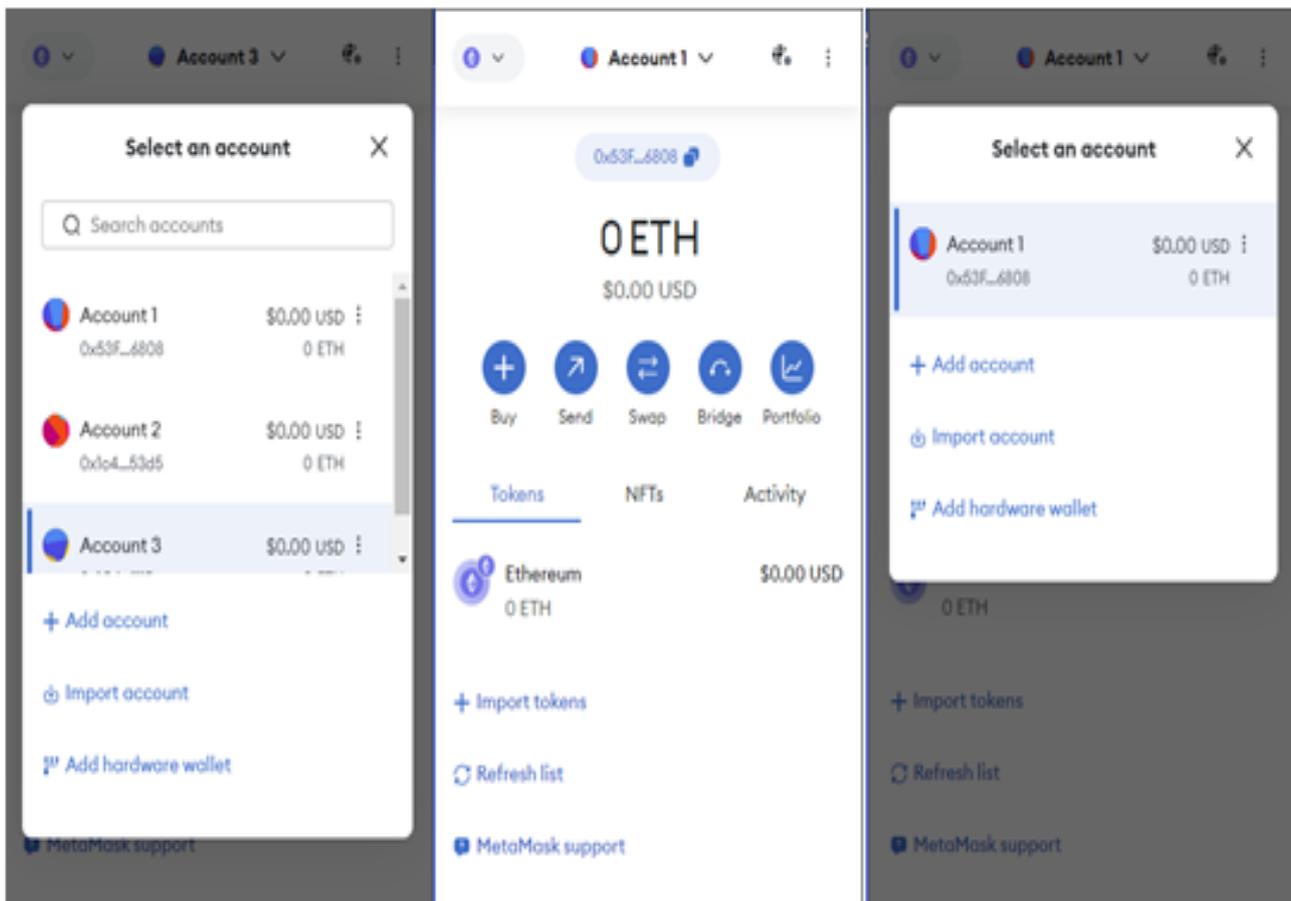


FIG. 4.5 : Connexion à la blockchain

8.2. Espace électeur

Lorsque l'électeur accède à son espace, le système va vérifier si le compte Metamask est autorisé pour voter.

Si le compte est autorisé, l'électeur va recevoir une liste des candidats et après avoir choisi le candidat en cliquant sur le bouton du vote, une transaction est initialisée vers la fonction vote de notre smart contract. Après que l'électeur a voté le bouton est caché et sa voix est affichée, il peut voir le total des voix pour chaque candidat. figure 4.6

vote page

Candidates

Candidate	Votes
user1	0
user2	0

Voter pour un candidat

Stats des jetons

Jetons à vendre	100
Jetons vendus	10
Prix par jeton	0.1
Solde dans le contrat	10

Achat de jetons

Recherche d'informations sur les électeurs

FIG. 4.6 : Espace électeur

8.3. Transactions (Ganache)

Chaque vote est sous forme de transaction, chaque transaction est écrite dans la blockchain de façon permanente et immuable, voici à quoi ressemble les transactions du déroulement précédent figure 4.7

ACCOUNTS		BLOCKS	TRANSACTIONS	LOGS	SEARCH FOR BLOCK NUMBERS OR TX HASHES	
CURRENT BLOCK 140	GAS PRICE 2000000000	GAS LIMIT 6721975	NETWORK ID 5777	RPS SERVER HTTP://127.0.0.1:8545	MINING STATUS AUTOMINING	
MNEMONIC pitch expand spin keen marine until wage pizza student repair breeze charge				HD PATH m/44'/60'/0'/0/account_index		
ADDRESS	BALANCE	TX COUNT	INDEX			
0x8010f5b2AacC7de2105d1854894084e4BB8D28E6	96.44 ETH	128	0			
0xB4321aCC50D980cde2D8c0EDe57008190129427c	99.97 ETH	12	1			
0xF7FD8d399EdC3Bfc15374aD2c52ab02498841dF4	100.00 ETH	0	2			
0xE96B2c947999E47D80886858C72B2217184c03B8	100.00 ETH	0	3			
0x6cE42584013075570A6eEf8FE484eFbd1DcbeaE4	100.00 ETH	0	4			
0x67013E23621C31525159f4fAAdeDaC9d7BDe4DAB	100.00 ETH	0	5			
0x4DB891618BA94aa717c7260E0EC6d276b4F21953	100.00 ETH	0	6			

FIG. 4.7 : Transactions (Ganache)

vous devez confirmer la transaction chaque fois qu'un utilisateur veut voter .figure 4.8

Account 1
→
0x452E...3117

http://remix.ethereum.org

TRANSFER

1

DETAILS
DATA

0.015

GAS FEE No Conversion Rate Available

Gas Price (GWEI) Gas Limit

AMOUNT + GAS FEE

1.015

TOTAL No Conversion Rate Available

Reject

Confirm

FIG. 4.8 : confirmer la transaction

9. Perspectives :

Nous ne prétendons nullement avoir répondu à tout ce qui se rapporte à cette application, celle-ci reste améliorable dans le future pour cela nous proposons :

- L'amélioration de l'interface graphique par la création d'une autre interface réservée à l'administrateur et l'électeur.
- Le perfectionnement de l'interactivité de l'interface graphique à travers le changement de couleur avant et après le vote.
- L'utilisation d'un algorithme permettant de classer les candidats selon les résultats du vote.
- Le renforcement du niveau de sécurité de l'application en faisant intervenir des experts en cyber-sécurité ...etc.

10. Conclusion :

Dans ce chapitre, nous avons montré le principe de fonctionnement du système, ainsi on a présenté le côté implémentation de notre projet en spécifiant les outils, les langages et l'environnement de développement ainsi que les interfaces les plus significatives de notre application du vote avec la technologie de la blockchain, à travers un ensemble de captures d'écran.

Conclusion Générale

La blockchain a largement dépassé sa fonction traditionnelle de monnaie électronique sans autorité centrale. Cette technologie a apporté de nouvelles idées qui garantissent l'immutabilité et la sécurité. La technologie de blockchain peut être utilisée dans de nombreux domaines, comme les systèmes de vote en raison de ces caractéristiques.

Dans ce mémoire, nous avons exploré la blockchain et proposé une solution basée sur cette technologie. Notre proposition concerne une application pour le vote électronique. Pour réaliser notre application du vote en ligne basée sur la blockchain. Nous avons élaboré une conception et une modélisation basée sur l'UP (Unified Process) et l'UML (Unified Modeling Language). Nous avons commencé par une étude préliminaire pour identifier les différents acteurs qui interagissent avec le système et nous avons procédé à l'analyse des besoins en spécifiant les besoins fonctionnels et non fonctionnels. Après, nous avons décrit le système à travers les diagrammes de séquence. L'implémentation nécessite la manipulation de l'outil spécifique à savoir la plateforme Ethereum basée sur les smart contract. L'application développée permet de garantir les besoins essentiels d'un vote démocratique.

Ce projet nous a été très bénéfique, car il nous a permis d'enrichir nos connaissances concernant la blockchain sur les deux plans : théorique et pratique. Il nous a aussi permis de découvrir et d'acquérir de nouvelles connaissances en matière de programmation et de développement dans le domaine des applications décentralisées. La technologie blockchain est encore très complexe à appréhender et le développement d'un système décentralisé nécessite énormément de temps, de ressources, de recherches et aussi de grands efforts de programmation. A cause de ces contraintes ainsi que des circonstances exceptionnelles, nous n'avons pas pu développer certains points dans la partie réalisation de l'application du vote.

Bibliographie

Documents Web et Articles

- [1] Adla, "Facilitation pour une prise de decision collective", Thèse de doctorat ,Université de Toulouse, France,2010
- [2] Roy, B. & D. Bouyssou : "Aide multicritère à la décision : méthodes et cas". Economica, Paris (France),1993.
- [3] Holtzman, S. : Intelligent decision systems, Addison Wesley,1989.
- [4] Herbert Alexander Simon. The New Science of Management Decision. Prentice Hall PTR, Upper Saddle River, NJ, USA, 1977.
- [5] MADOURI Souad, « Vers un système d'aide multicritère à la décision de groupe en aménagement du territoire : application à la localisation spatiale », Magister, Université Oran 1, 2010-2011
- [6] Hamdadou" Un modèle d'aide à la décision en aménagement du territoire, une approche multicritere et une approche de négociation", Thèse de doctorat, Université Oran1, Algerie 2008
- [7] HAMDADOU Djamila & BOUAMRANE Karim, NAOUI Oum El Kheir, « Méthodologie Multicritères d'aide à la décision cours et exercices », Université Oran 1, 2016
- [8] P. Zaraté. . Des systèmes interactifs d'aide à la décision aux systèmes coopératifs d'aide à la décision :Contributions conceptuelles et fonctionnelles. thèse de Doctorat, INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE (INPT), Toulouse.2005
- [9] DeSanctis.G "A foundation,for the study of group decision support system",Journal ,1987

- [10] Mahamadou, S. . Utilisation de l'approche FAHP/FPROMETEE pour l'élection d'un Facilitateur (coordinateur) au sein d'un GDSS. thèse de Master, Université de Mostaganem, Mostaganem,2021.
- [11] H. Bidgoli, Intelligent management support systems, Quorum books, Westport, Connecticut, 1998.
- [12] Power, D.J. : "Decision support systems : concepts and resources for managers", Westport, Conn., Quorum Books,2002.
- [13] Qian Chen , TEAMDEC : A GROUP DECISION SUPPORT SYSTEM Blacksburg, Virginia.1998
- [14] <https://www.microsoft.com/en-us/microsoft-teams/>
- [15] <https://www.groupsystems.com/>
- [16] <https://www.lucidmeetings.com/>
- [17] Tali Mohammed El Amine, Chalal Rachid, « Une grille de lecture des outils d'aide à la décision », Proceedings of the JST'10 de Sonatrach, Oran Octobre 2015.
- [18] Nasser Al-Housni. An Exploratory Study in Blockchain Technology. PhD thesis, The University of Manchester (United Kingdom), 2019.
- [19] Satoshi Nakamoto, Bitcoin : A peer to peer electronic cash system, 2008 (white paper)
- [20] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology : Beyond bitcoin. Applied Innovation, 2016.
- [21] Dylan Yag4 Peter Mell, Nik Roby and Karen Scarfone. NISTIR 8202 Blockchain Technology Overview. October 2018
- [22] Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda. Beginning Blockchain : A Beginner's guide to building Blockchain solutions. Springer, 2018.
- [23] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. Blockchain for internet of things : A survey. IEEE Internet of Things Journal, 6(5) :8076–8094, 2019.
- [24] Farah, Nadir Abdelrahman Ahmed. "Blockchain technology : Classification, opportunities, and challenges." International Research Journal of Engineering and Technology 5.5 (2018) : 3423-3426.
-

- [25] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. Applications of blockchains in the internet of things : A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2) :1676–1717, 2018.
- [26] AHong-Ning Dai, Zibin Zheng, and Yan Zhang. Blockchain for internet of things : A survey. *IEEE Internet of Things Journal*, 6(5) :8076–8094, 2019.
- [27] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology : Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017
- [28] Monrat, Ahmed Afif, Olov Schelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." *IEEE Access* 7 (2019) : 117134-117151
- [29] Cambridge Bitcoin Electricity Consumption Index (CBECI), <https://www.cbeci.org>, Michel Rauchs, Apolline Blandin, and Anton Dek at the Cambridge Centre for Alternative Finance, University of Cambridge, Judge Business School.
- [30] <https://bitinfocharts.com/>
- [31] Kim, J. W. "Blockchain technology and its applications : case studies." *Journal of System and Management Sciences* 10.1 (2020) : 83-93.
- [32] Jacobson, g. Booch, j. Rumbaugh. "The unified software development process". eyrolles, 2000.
- [33] <https://www.dappuniversity.com/articles/web3-js-intro>
- [34] Pascal Roques, "uml2 modeliser une application web ", 4^eedition 2007
- [35] Jacques Lonchamp, " genie logiciel sixieme partie la modelisation objet uml ", cours, cnam cra nancy. 2003.
- [36] Josef Gabay, David Gabay, " uml 2 analyse et conception ", Dunod, paris : 2008
- [37] <https://www.supinfo.com/>
- [38] <https://www.supinfo.com/articles/single/1114-sublime-text-3>
- [39] <https://www.trufflesuite.com/docs/ganache/overview>.
-

- [40] [https : //fr.bitdegree.org/tutos/metamask/](https://fr.bitdegree.org/tutos/metamask/)
 - [41] [https ://golden.com/wiki/truffle framework](https://golden.com/wiki/truffle%20framework)
 - [42] [https : //www.tutorialsteacher.com/nodejs/what-is-nodejs](https://www.tutorialsteacher.com/nodejs/what-is-nodejs)
 - [43] [https : //remix-ide.readthedocs.io/en/latest/](https://remix-ide.readthedocs.io/en/latest/)
 - [44] [http ://www.une-blockchain.fr/tutorial-developpement-solidity-remix/](http://www.une-blockchain.fr/tutorial-developpement-solidity-remix/)
 - [45] [https ://agency-inside.com/2016/06/definition-webmarketing-bootstrap/](https://agency-inside.com/2016/06/definition-webmarketing-bootstrap/)
 - [46] [http ://glossaire.infowebmaster.fr/javascript/](http://glossaire.infowebmaster.fr/javascript/)
 - [47] [https ://solidity.readthedocs.io/en/v0.6.11/](https://solidity.readthedocs.io/en/v0.6.11/)
 - [48] [https ://www.php.net/manual/fr/intro-what-is.php](https://www.php.net/manual/fr/intro-what-is.php)
-

