

# LA BLOCKCHAIN POUR LA CONFIANCE DES BAILLEURS DES FONDS

ThruthDonation

Ce Projet a été réalisé par DIALLO Abdourahamane développeur Blockchain et BARRY Mamadou Dian Chef de projet Blockchain,dans le cadre de la validation de notre formation sur la Blockchain à ALYRA sous la supervision de Bastien et de Yosra

*First release, September 2020*



# Contents

<b>0.1</b>	<b>INTRODUCTION</b>	<b>6</b>
<b>1</b>	<b>CONTEXTE</b>	<b>7</b>
1.1	Contexte	7
<b>2</b>	<b>DÉFINITION DES CONCEPTS CLÉS</b>	<b>11</b>
2.1	<b>Concepts Clés</b>	<b>11</b>
2.1.1	La Blockchain .....	11
2.1.2	Les cryptoactifs .....	12
2.1.3	Les ICO .....	12
2.1.4	Smart Contracts .....	13
2.1.5	Le «Wallet» .....	13
2.1.6	La transaction .....	14
2.1.7	Le minage .....	14
2.1.8	Le Porteur de Projet .....	14
2.1.9	Bailleurs de Fonds .....	15
2.1.10	Donateurs .....	15
<b>3</b>	<b>PRÉSENTATION DE TruthDonation</b>	<b>17</b>
3.1	<b>Les Acteurs et leurs Rôles</b>	<b>17</b>
3.2	<b>Élection des Propositions</b>	<b>18</b>
3.2.1	Le vote .....	18
3.2.2	La levé des fonds .....	18

<b>3.3</b>	<b>Politique d'adhésion</b>	<b>19</b>
<b>3.4</b>	<b>Suivi des Fonds</b>	<b>21</b>
<b>3.5</b>	<b>Business modèle</b>	<b>22</b>
<b>3.6</b>	<b>Les différent Scénario concernant les Porteurs de Projets</b>	<b>22</b>
<b>3.7</b>	<b>Les différents scénarios pour le Bailleu</b>	<b>23</b>
3.7.1	Scénario 1 .....	23
3.7.2	Scénario 2 .....	23
<b>3.8</b>	<b>LE ROADMAP</b>	<b>26</b>
<b>3.9</b>	<b>Déploiement et Contraintes Techniques</b>	<b>27</b>
<b>3.10</b>	<b>Défis techniques</b>	<b>28</b>
3.10.1	Gestion du compte "TheCryptos" .....	28
3.10.2	Remix .....	28
3.10.3	Ganache .....	28
3.10.4	MetaMask .....	28
3.10.5	Gestion des transactions .....	28
3.10.6	Gestion des taxes .....	28
3.10.7	Gestion de la sécurité .....	28
3.10.8	Exemple de période de vote .....	28
<b>4</b>	<b>ANALYSE DU MARCHÉ</b>	<b>31</b>
<b>4.1</b>	<b>Introduction</b>	<b>31</b>
<b>4.2</b>	<b>DISBERSE:</b>	<b>31</b>
<b>4.3</b>	<b>TruBudget :</b>	<b>32</b>
<b>4.4</b>	<b>AID : Tech</b>	<b>32</b>
<b>4.5</b>	<b>EN QUOI LE PROJET DIFFÈRE-T-IL</b>	<b>33</b>
<b>4.6</b>	<b>Description de TheCriptos</b>	<b>34</b>
<b>4.7</b>	<b>Gouvernance</b>	<b>34</b>
4.7.1	Vitesse de transaction .....	34
4.7.2	Taille du bloc .....	35
4.7.3	Le Coût .....	35
<b>5</b>	<b>LES INTERFACES DE ThruthDonation</b>	<b>37</b>
<b>5.1</b>	<b>Inscription:</b>	<b>37</b>
<b>5.2</b>	<b>Connexion:</b>	<b>37</b>
<b>5.3</b>	<b>Acceptation :</b>	<b>38</b>
<b>5.4</b>	<b>Création de proposition :</b>	<b>38</b>
<b>5.5</b>	<b>Liste des propositions:</b>	<b>38</b>
<b>5.6</b>	<b>La proposition Gagnante:</b>	<b>39</b>

<b>5.7</b>	<b>Donation :</b>	<b>39</b>
<b>5.8</b>	<b>Règlement:</b>	<b>40</b>

## 0.1 INTRODUCTION

On compte dans le monde plusieurs dizaines de milliers de projets de développement financés par des bailleurs de fonds. Chacun d'entre eux répond à une multiplicité d'impératifs, de principes et de règles de procédures destinés à en assurer la bonne marche et à faire en sorte que l'aide fournie serve effectivement aux pauvres. L'expérience montre qu'il est possible d'améliorer et de renforcer rapidement les capacités en place dans les pays en développement, à partir du moment où les bailleurs de fonds réussissent à coordonner leurs actions et à harmoniser leurs procédures. Mais le constat est qu'il existe aujourd'hui un énorme aléa de confiance entre les différentes entités à savoir bailleurs de fonds, ONG et responsables étatiques des ces différents pays pauvres. Cela se matérialise par des détournements massifs des fonds destinés aux pauvres populations soit de manières directes pour la réalisation des projets communautaires, ou étatiques destinés à améliorer leurs conditions de vie (eau potable, santé, éducation ...). À l'heure de la crise de confiance et du mécontentement vis-à-vis des tiers et médiateurs traditionnels, institutions, banques et États, la technologie blockchain qui porte la promesse d'une désintermédiation et de la transparence, séduit tout le monde.

Le terme «blockchain» est apparu en 2008 et depuis nous assistons à une croissance des projets basés sur cette technologie. Elle est souvent présentée comme une innovation de rupture, aussi importante que la naissance de l'imprimerie ou d'Internet. Ses impacts potentiels pourraient révolutionner nos systèmes économiques et nos manières d'échanger: la blockchain est porteuse de transformations profondes dans de nombreux domaines d'application. Cette technologie porte surtout la promesse d'une nouvelle gouvernance, à l'échelle locale comme mondiale, basée sur des principes novateurs qui lui sont associées: **collaboration, désintermédiation, traçabilité, transparence, consensus distribué, ineffaçable, structure distribuée, résilience, sécurité et confiance.** Toutes ces caractéristiques constituent le potentiel innovateur de la blockchain.

La technologie blockchain est également source de nouvelles opportunités de financement, plus démocratiques elles aussi, notamment grâce à la désintermédiation à travers lequel les institutions qui régissent et dominent traditionnellement le système financier, comme les États et les banques, perdent leur pouvoir, au profit de modes de financements plus horizontaux.

Ban Ki-moon, Secrétaire général des Nations Unies, a déclaré «L'année dernière», que «la corruption a empêché 30% de toute l'aide au développement d'atteindre sa destination finale. Cela se traduit par des ponts, des hôpitaux et des écoles qui n'ont jamais été construits, et des personnes vivant sans bénéficier de ces services. Il s'agit d'un échec de responsabilité et de transparence. Nous ne pouvons pas le laisser persister. » Distribuer et suivre les fonds pour garantir leur impact maximal reste un défi pour le secteur du développement international.

L'investissement via la blockchain permet également de régler le problème de la confiance dans l'allocation réelle des fonds, en raison de sa transparence. Elle rend les différentes étapes de financement plus transparentes, accessibles et traçables, ce qui permet d'augmenter l'efficacité et la confiance dans la gestion des investissements publics et des fonds dédiés au développement des pays pauvres.



## 1. CONTEXTE

### 1.1 Contexte

Les ONG sont de plus en plus confrontées au problème du contrôle de la destination de leurs dons. Le risque de détournement des fonds par les représentants locaux des organisations non gouvernementales et des organisations internationales ne cesse de s'accroître. Ces malversations ne touchent pas directement le personnel humanitaire de l'organisation, mais elles portent préjudice à la nature neutre et désintéressée de l'action conduite et décrédibilisent l'organisation en charge d'un projet de développement ou d'une intervention d'urgence. Ces pratiques frauduleuses nuisent directement à la légitimité de l'action humanitaire.

Les détournements aux fins d'enrichissement personnel sont de plus en plus fréquents, notamment dans les pays où intervient l'ONU, la Banque Mondiale et bien d'autres organisations internationales où l'on voit éclore de nombreuses associations pour la défense des droits de l'homme. La plupart d'entre elles prétendent à des subventions des organisations internationales ou cherchent à bâtir des partenariats avec des ONG afin de financer leur développement. La finalité humanitaire de ces associations n'est souvent qu'un prétexte. Beaucoup ne sont composées que d'une seule personne, qu'elles font vivre. Elles ne sont soumises à aucun contrôle de gestion, ce qui favorise le détournement de fonds originellement destinés à promouvoir les droits de l'homme ou à construire des écoles. Beaucoup d'autres sont fictives et ne servent qu'à des opérations d'instrumentalisation des fonds internationaux et d'intelligence économique au profit d'intérêts commerciaux.

Une publication des experts de la Banque Mondiale a déclenché un scandale mondiale. La publication remet directement en cause l'efficacité de l'action de la Banque mondiale. En résumé : les versements d'aide au développement de l'institution financière internationale nourrissent en partie la corruption dans plusieurs pays pauvres. « Ces versements d'aide vers les pays les plus dépendants coïncident avec une augmentation importante de transferts vers des centres financiers offshore connus pour leur opacité fiscale », comme la Suisse, le Luxembourg, les îles Caïmans et Singapour, expliquent les auteurs de l'étude. Rien de nouveau sous le soleil, sauf que « jusqu'ici, il

existait peu de preuves systématiques du détournement de l'aide », expliquent ces auteurs pour la plupart issus du monde académique.

Pour parvenir à de telles conclusions, ils se sont concentrés sur 22 des pays les plus pauvres principalement en Afrique. Ils ont procédé à la comparaison les chiffres de la Banque mondiale avec ceux des versements à l'étranger compilés par la Banque des règlements internationaux (BRI), une organisation internationale qui agit au service de banques centrales et d'autres autorités financières. C'est la banque centrale des banques centrales en somme et elle est basée à Bâle, en Suisse.

Pour en revenir aux résultats, le « taux de fuite » moyen est estimé à environ 7,5 % de l'aide, estiment ces experts. Une part qui grimpe à 15 % pour les 7 pays les plus aidés quand l'aide de la Banque mondiale représente au moins 3 % du produit intérieur brut parmi eux : l'Ouganda, l'Érythrée, la Sierra Leone, le Mozambique et d'autres. Les bénéficiaires de ces détournements sont bien les places financières occidentales et, donc, les pays plus riches. Saviez-vous que plus précisément, « dans un trimestre où un pays reçoit une aide équivalant à 1% du PIB, ses dépôts dans les paradis augmentent de 3,4% par rapport à un pays sans aide » ? Ce qui signifie que « plus un pays est dépendant de l'aide au développement de la Banque mondiale, plus les versements effectués vers des centres financiers offshore sont importants. »» ces taux représentent une estimation a minima, car l'étude ne prend en compte que les transferts vers des comptes offshore, sans intégrer les possibles dépenses en immobilier ou en biens de luxe », remarquent les auteurs du document.

Pour autant, les économistes n'ont pas voulu que leur constat soit interprété comme une preuve de cause à effet. Selon eux, l'hypothèse d'un détournement de l'aide internationale par les « élites » de ces pays est l'explication la plus plausible. « L'aide détournée par les politiques au pouvoir, les bureaucrates et leurs acolytes est cohérente avec la totalité des schémas observés », se contente-t-elle de souligner, ajoutant que les effets « sont plus importants pour les pays les plus corrompus ». Il n'y aura pas non plus de divulgation de nom. Selon les experts, il est impossible de dire qui transfère les fonds hors du pays, les statistiques BRI ne comptant que les flux totaux par trimestre entre les pays.

Autre cas très parlant, celui de la gestion d'Ebola en Afrique de l'Ouest entre 2014 et fin 2016. Un an après la fin de l'épidémie d'Ebola en Afrique de l'ouest, la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (FICR), basée en Suisse, s'est dite « outragée par la découverte de fraudes », à partir des fonds versés pour lutter contre la maladie en Guinée, en Sierra Léone et au Liberia. La FICR dénonce une malversation financière estimée à 5 millions d'euros. Celle-ci se décompose en trois séries d'actions malhonnêtes. Une fraude bancaire « entre les anciens employés de FICR et des employés d'une banque de Sierra Léone, a conduit à une perte financière possible de 2,13 millions de francs suisses » (1,83 million d'euros). La Croix-Rouge a aussi découvert un trafic de fausses factures d'un service de dédouanement (détournements liés aux primes) en Guinée qui aurait entraîné une perte estimée à 1,17 million de francs suisses (1 million d'euros). Au Liberia d'autres enquêtes ont révéléées le détournement d'un montant total estimé à 2,7 millions de francs suisses (2,3 millions d'euros), selon la même source.

Interroger sur cette question des détournement sur la Radio France internationale, le docteur **Jemilah Mahmood, sous-secrétaire général en charge des partenariats**, explique : « Ce qu'on a fait, c'est suivre les recommandations d'organisations comme Transparency international et de partager les résultats de nos enquêtes. On espère que ça va inspirer d'autres organisations. En tout

cas, on avait besoin d'apprendre de nos erreurs. ». « Personne ne veut qu'il y ait des fraudes, nous sommes tous furieux et en colère que ce soit arrivé. On a l'impression qu'on ne nous a pas seulement volé de l'argent, mais qu'on nous a enlevé la possibilité d'assister les gens qui avaient sérieusement besoin de notre aide, et c'est vraiment inacceptable », poursuit-il.

Comment cela est-il possible dans une institution qui se veut un fer de lance de la lutte contre la corruption ? La question mérite d'être posée. Un début de réponse réside dans le fait que des managers ont eu le temps et la possibilité de placer leurs personnel à des postes stratégiques, ce qui leur a permis de verrouiller le système et de prévenir toute enquête sérieuse contre eux. Détenant des leviers-clés dans la chaîne des enquêtes sur les violations des règles d'éthique et d'intégrité, ils peuvent ainsi mettre le système sous tutelle, le dévoyer et, en un mot, le corrompre. C'est là une première explication.

Une autre réside dans le fait que la bureaucratie de ces institutions conduit à bâtir un système résistant au changement et se protégeant contre les interventions extérieures, quitte à s'installer dans une certaine fuite en avant, à violer leurs propres règles d'éthique et d'intégrité et à détruire, au lieu de les soutenir, les lanceurs d'alerte sur des faits de corruption. De quoi priver les gouvernements de leur pays d'origine de leur capacité à contribuer au développement de leur pays sans compter le préjudice causé à leurs familles respectives.

Malheureusement, les exemples abondent, qu'il s'agisse de détournements de fonds ou de dons en nature. En France, quelques scandales plus ou moins retentissants ont marqué les esprits : les malversations de la Fondation Raoul-Follereau (spécialisée dans la lutte contre la lèpre) en 2002, la gestion désastreuse de SOS-Racisme de 1997 à 2001, les abus de Jacques Crozemarie, président de l'ARC (Association pour la recherche contre le cancer) en 1994, les associations fictives du secrétaire d'État aux handicapés Michel Gillibert entre 1989 et 1992, l'utilisation des subventions de l'association Carrefour du développement au profit du Parti socialiste via le ministre de la Coopération Christian Nucci en 1986, etc. En 2003, encore, un rapport du Service central de prévention de la corruption montrait que les structures associatives constituaient une aubaine pour les fraudeurs : la souplesse et le caractère obsolète de leur cadre juridique favorisaient notamment l'évasion fiscale.

En avril 2006, un militant congolais a été suspendu de ses fonctions de président de l'association Rencontre pour la paix et les droits de l'homme (RPDH) pour avoir détourné 3 millions de francs CFA (4 600 ) de financements accordés par l'ONG britannique Global Witness. La Banque mondiale, grâce à son département d'enquêtes a traité plus de 2 000 cas supposés de vols, trucages d'offres, corruptions, complicité et coercition depuis 2001. Ces enquêtes ont entraîné des sanctions publiques contre 330 entreprises ou individus qui se sont vus interdire tout contrat futur financé par la Banque.

L'ONG Transparency International a édité en 2014 un rapport destiné à la lutte contre la corruption dans le cadre d'actions humanitaires, estimant que ce type de détournements « prive les pauvres, les plus vulnérables, les victimes de désastres naturels et de conflits civils, de ressources capables de sauver des vies ».

Face à ces dérives, nombreuses institutions et ONG ont pris des mesures visant à éviter les fraudes, ou à les réparer. Progressivement, ONG et organisations internationales commencent à se doter de normes internes de qualité et d'outils d'évaluation de leurs programmes, selon plusieurs modalités :

C'est par exemple :

- Déployer des experts au niveau local pour contrôler la gestion des opérations
- Élaborer collectivement des normes « qualité »
- Se regrouper pour proposer des démarches « qualité » (guide Synergie qualité)
- Mettre en place des codes de conduite, à l'image du Comité International de la Croix Rouge (CICR).
- Engager des agences spécialisées dans l'évaluation des risques,
- Mettre en place des formations pour les employés locaux et internationaux,
- Limiter aussi la durée des missions de chaque agent pour éviter la création de réseaux de détournement bien installés.
- Enfin, la Convention des Nations Unies contre la corruption qui est entrée en vigueur depuis 14 décembre 2005. Elle est juridiquement contraignant pour les États et prévoit, par exemple, en cas de détournement, des mécanismes de recouvrement des fonds.

Ces démarches sont indispensables car les bailleurs de fonds sont de plus en plus exigeants quant à la transparence financière et sur la qualité et l'efficacité des programmes.

Toutefois les principales questions qui se posent aujourd'hui encore est de savoir,  
**si les mesures prises parviennent à rompre ce système de détournement installer et nourri depuis des années par ces différents dirigeants ?**

**N'est-t-il pas nécessaire de nos jours de penser des systèmes informatisés et plus décentralisés permettant mettre fin à ces malversations ?**

Dans ce cadre intervient notre projet de fin de formation à Alyra l'école de la Blockchain. Ce projet nommé **TruthDonation** vise à mettre en place une application décentralisée basée sur le concept de la Blockchain dans le but de remédier aux différentes failles de sécurité et aléas de confiance dans le processus de financement des projets socio-humanitaire en Afrique.

En règle générale, les donateurs internationaux réagissent aux risques en contournant les systèmes des institutions partenaires dans les pays en développement respectifs. Cependant, outre les coûts de transaction élevés, cela signifie que les pays partenaires ne maîtrisent pas la planification et la mise en œuvre de manière indépendante. Avec application **TruthDonation**, nous créons de la transparence dans la coopération et contribuons ainsi à la résolution de ces problèmes.

## 2. DÉFINITION DES CONCEPTS CLÉS

### 2.1 Concepts Clés

#### 2.1.1 La Blockchain

La Blockchain est un type de registre distribué décentralisé, permettant de valider et retracer des transactions. Cette base de données « distribuée » n'est pas détenue par un intermédiaire dans un lieu centralisé mais est disponible à tout moment via les ordinateurs participant à cette blockchain, qui sont les « nœuds » de celle-ci. Les transactions sont regroupées par blocs. Chaque bloc est validé par des utilisateurs (« mineurs ») selon des techniques propres variant selon le type de blockchain. La décentralisation, la sécurité et la transparence de la blockchain est susceptible de venir soutenir de nombreuses applications :

- le transfert d'actifs (monétaires, mais également pour des titres, votes, actions, etc.) ;
- le suivi et la traçabilité de produits ;
- l'exécution automatiquement de conditions contractuelles (smart contracts) sans intervention humaine.

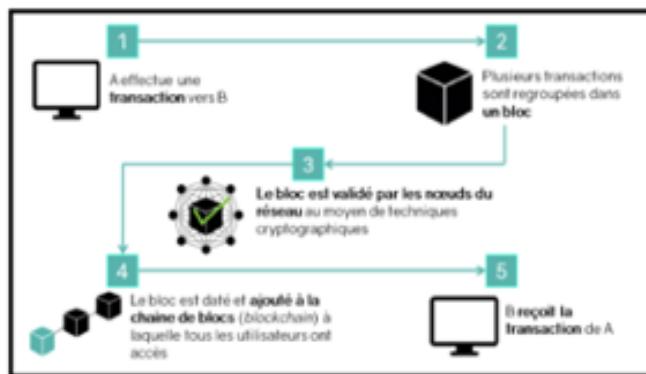


Figure 2.1: Example of a superpixel algorithm

### 2.1.2 Les cryptoactifs

Les crypto-actifs sont des actifs numériques échangés sur une blockchain. Plusieurs catégories de cryptoactifs peuvent être distinguées, selon les « droits » qu'ils revêtent :

- les crypto-monnaies (telles que le Bitcoin), qui sont des représentations de valeur et des moyens d'échange transmis sur une blockchain ;
- les jetons (ou tokens) qui comportent des droits, par exemple une part du capital de l'entreprise ou un paiement à l'avance du service qu'elle développe. Les émissions de ces jetons sont connues sous les noms de STO (Security Token Offering) lorsque le jeton a les caractéristiques d'un titre financier et d'ICO (Initial Coin Offering) lorsque le jeton ne revêt pas ces mêmes caractéristiques.



Figure 2.2:

### 2.1.3 Les ICO

Une ICO (Initial Coin Offering – émission de jetons en français) est une méthode de levée de fonds fonctionnant grâce l'émission de jetons (« tokens ») échangeables contre des actifs numériques ou des monnaies ayant cours légal dans la phase de démarrage d'un projet. Ces jetons peuvent ensuite être revendus sur un marché secondaire. Les ICO se distinguent des levées de fonds classiques car elles permettent d'acquérir des jetons, et non pas des titres financiers de l'entreprise (sinon, la levée de fonds sur blockchain est qualifiée de Security Token Offering – ou STO). Ces jetons peuvent offrir un droit d'usage du service développé par l'entreprise appelé à être développé. Les ICOs permettent aux start-ups d'avoir accès à un financement très rapidement tout en s'adressant à un large public international d'investisseurs potentiels.



Figure 2.3:

### 2.1.4 Smart Contracts

Les smart contracts, ou contrats intelligents, sont des programmes informatiques irrévocables, le plus souvent déployés sur une blockchain, qui exécutent un ensemble d'instructions pré-définies. L'idée maîtresse derrière ce concept de smart contracts est de garantir la force obligatoire des contrats non plus par le droit, mais directement par le code informatique : “code is law”, pour reprendre la célèbre formule de Lawrence Lessig.



Figure 2.4:

### 2.1.5 Le «Wallet»

Le porte-monnaie virtuel, le «Wallet»: il est installé sur ordinateur ou sur mobile. Permet de consulter votre solde, effectuer des transactions, ou recevoir des bitcoins.



Figure 2.5:

### 2.1.6 La transaction

Comme indiqué plus haut, pour effectuer une transaction, il vous faut un porte monnaie virtuel. Ensuite, celui-ci va créer pour vous une adresse qu'il faudra communiquer à la personne avec laquelle vous souhaitez faire une transaction. On peut grossièrement comparer cette adresse à un IBAN.



Figure 2.6:

### 2.1.7 Le minage

Le minage est un système permettant de confirmer les transactions en attente et donc de les inclure dans la chaîne de blocs. Le minage sert notamment à :

- Imposer un ordre chronologique dans la chaîne de blocs ;
- Protéger la neutralité du réseau ;
- Permettre aux ordinateurs du réseau d'être en accord sur l'état du système



Figure 2.7:

### 2.1.8 Le Porteur de Projet

Personne physique ou morale pour le compte de qui l'objet du projet est réalisé, responsable de la définition des objectifs du projet et de la décision d'investir dans le projet.



Figure 2.8:

### 2.1.9 Bailleurs de Fonds

Les bailleurs ici sont les différentes institutions financières, personne physique ou moral disposant des moyens financiers souvent obtenu par des donations et prêt à investir sur des projets socio-humanitaires.



Figure 2.9:

### 2.1.10 Donateurs

Le donneur est une personne physique ou morale qui fait des dons qu'il soit numéraire ou matériel pour soutenir une cause, un projet, une association.



Figure 2.10:



### 3. PRÉSENTATION DE TruthDonation

#### 3.1 Les Acteurs et leurs Rôles

Notre Projet est principalement composé de trois acteurs. La figure suivante présente ces acteurs et leurs rôles:

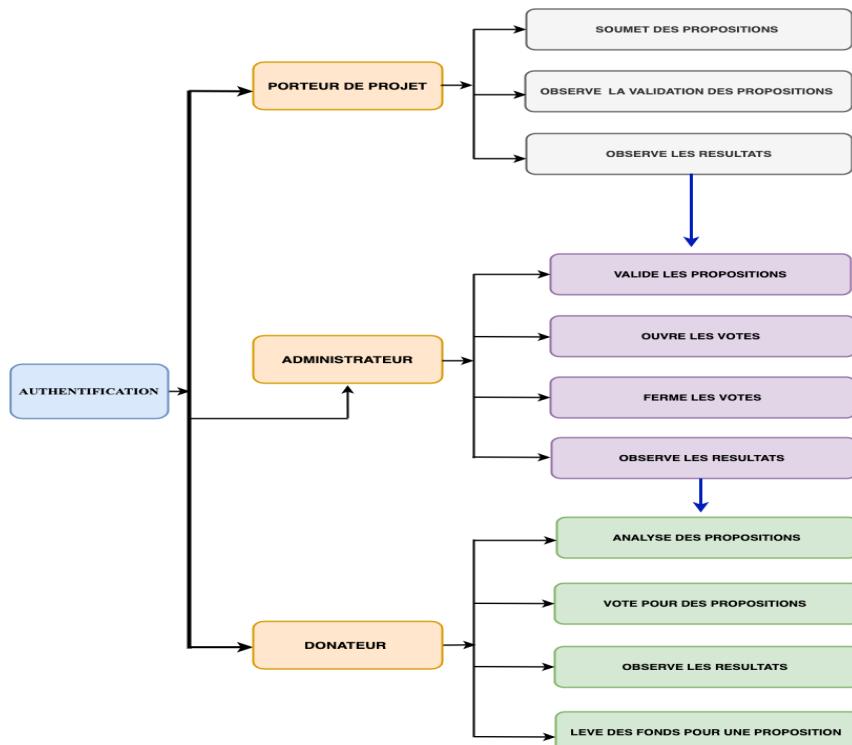


Figure 3.1:

### 3.2 Élection des Propositions

#### 3.2.1 Le vote

##### (Les Phases du vote)

- La phase d'enregistrement
- La phase de vote
- La phase de validation et publication des résultats

##### (Les Caractéristiques du Vote)

- Le vote a une heure de début et une heure de fin
- Le vote a un votant
- Le vote abouti à un résultat
- Le résultat du vote élu un projet au financement
- Le vote est anonyme

#### 3.2.2 La levé des fonds

- Les fonds sont levés suite à l'élection d'un projet
- Les fonds sont destinés à financer un projet
- Les fonds sont levés par un bailleur ou un investisseur
- Une date limite est définie pour lever des fonds

### 3.3 Politique d'adhésion

TruthDonation est une plateforme de gestion de fonds qui vise à rendre l'acheminement de l'aide au développement et humanitaire plus transparent, efficace et efficient. En utilisant une blockchain autorisée, ils aident les donateurs, les gouvernements et les ONG à transférer et à retracer leurs fonds à travers toute la chaîne de valeur, garantissant que les ressources vitales atteignent réellement les personnes qu'elles sont censées servir et obtiennent le plus grand impact possible.

L'aide publique au développement (APD) est largement décaissée par le biais de systèmes bancaires hérités qui sont opaques, lents et coûteux, les frais bancaires, les taux de change et les fluctuations monétaires grugeant les fonds essentiels. Les figures suivantes montrent la différence entre les systèmes classiques et l'utilisation de la Blockchain.

#### a- Système actuel sans Blockchain

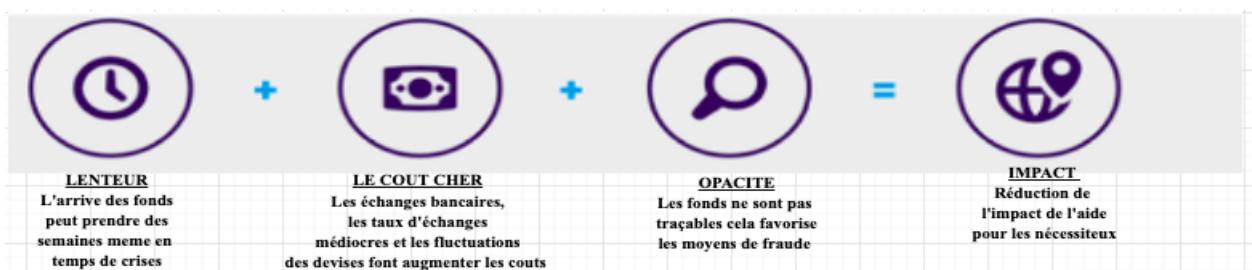


Figure 3.2:

#### b- Système utilisant la Blockchain

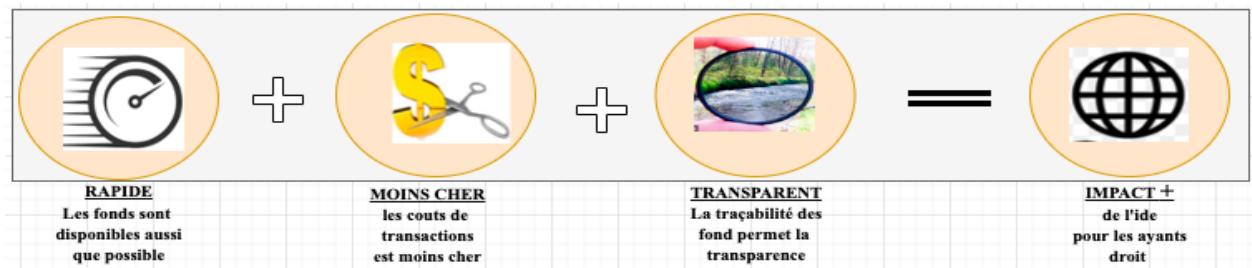


Figure 3.3:

En outre, une fois que les fonds des donateurs arrivent dans un pays, ils sont généralement dispersés vers un certain nombre d'ONG et d'autres partenaires locaux de mise en œuvre, créant un environnement facile pour que les dons soient perdus ou détournés. Plus fondamentalement, l'une des raisons du manque de responsabilité dans la distribution de l'aide est que les organisations de développement n'ont aucun moyen de retracer les fonds lorsqu'ils se déplacent entre le donneur et le bénéficiaire final, ce qui rend impossible de mesurer pleinement l'efficience et l'efficacité de l'aide. Les fonds des donateurs peuvent être acheminés par le biais d'organisations multilatérales ou regroupés avec d'autres fonds apportés par d'autres pays ou organisations, ce qui limite le contrôle direct qu'ils ont sur leurs dépenses.

L’application TruthDonation bénéficiera aux pays partenaires et aux donateurs de plusieurs manières:

- Réduction des frais de transactions des deux côtés ;
- Accroître la transparence et l’efficacité des projets financés par les donateurs ; et ainsi
- Faciliter l’obtention des financements à partir de plusieurs sources pour les porteurs de projets.

Et ces bénéfices ont le potentiel d’augmenter l’impact structurel de la coopération au développement en renforçant les structures de gouvernance nationales et ainsi les systèmes d’aide internationales. Notre vision est que TruthDonation soit entièrement détenu, utilisé et adapté par les pays partenaires et les institutions bailleurs des fonds. Il peut servir de plate-forme pour des initiatives financées par des donateurs, ce qui faciliterait dans une large mesure l’harmonisation des donateurs. Enfin, les pays seraient également libres d’adapter et d’utiliser le logiciel pour la mise en œuvre de programmes et de projets nationaux, bénéficiant à nouveau de l’efficacité et de la transparence accrues comme élément central de TruthDonation.

L’adoption de cette application serait d’une importance capitale pour les institutions de financement du développement et les pays donateurs. Car il existe un risque élevé perçu dans la mise en œuvre de la coopération au développement et la fourniture de fonds budgétaires aux pays partenaires. Ce risque réside dans l’utilisation abusive des fonds à des fins autres que celles prévues. La gestion des finances publiques dans les pays partenaires est souvent perçue comme manquant du niveau de transparence et d’efficacité requis des donateurs. C’est d’ailleurs dans ce contexte que chaque institution donatrice a mis en place ses propres règles et procédures qui doivent être respectées par les pays partenaires s’ils veulent recevoir un financement, ce qui conduit à plusieurs résultats négatifs, tels que des coûts de transaction élevée, la tâche difficile de manque de coordination et absence d’impact structurel qui pourrait autrement être atteint.

Cette situation a conduit les donateurs et les pays en développement en 2005 à approuver la Déclaration de Paris sur l’efficacité de l’aide et, plus tard en 2012, le partenariat de Busan pour une coopération efficace au service du développement. Le Partenariat de Busan, tout en exigeant des pays en développement qu’ils améliorent leurs systèmes de gestion des fonds publics, appelle à l’utilisation des systèmes nationaux comme option par défaut pour les pays donateurs. Cependant, bien que des progrès en matière de gestion des fonds publics aient été réalisés au fil du temps, les pays donateurs hésitent encore à utiliser les systèmes nationaux dans une plus large mesure. La raison en est une perception du risque inchangée de la part des donateurs. Nous supposons qu’une augmentation de la transparence et de la confiance pourrait surmonter cet obstacle, permettant ainsi de se produire dans l’utilisation des systèmes nationaux et un effet plus durable du développement. TruthDonation est un outil basé sur une blockchain qui permet une implémentation efficace et transparente de projets collaboratifs. TruthDonation sert de plate-forme à toutes les parties prenantes impliquées dans un projet (par exemple, ministère des finances, donneur, collectivités locales, bénéficiaires...). Chaque partie prenante, ou utilisateur de logiciel, reçoit des droits spécifiques en fonction de son rôle dans le projet.

### 3.4 Suivi des Fonds

Le suivi des fonds est l'une des étapes les plus importantes de notre projet. C'est pourquoi, notre projet ne se limite pas seulement à l'organisation du vote et de la donation, mais elle accompagne également la réalisation du projet et le suivi des fonds. TruthDonation permet de partager des informations en temps réel entre les utilisateurs. Ainsi, des étapes d'approbation cruciales, telles que la non-objection d'un donneur à un processus de passation de marchés ou à un contrat, ou le déblocage de paiements sur la base des factures de l'entrepreneur, peuvent être donnés immédiatement et sans délai. Toutes les activités sont documentées dans le système et sont traçables à toutes les étapes.

En effet, les fonds existants dans le compte du porteur du projet ne sont pas décaissables librement. Comme cela sera indiqué dans le plan budgétaire de son projet, le décaissement se fera étape par étape. Après l'exécution de chaque phase, des factures et des reçus sont présentées authentifiées et validées avant le prochain décaissement. Les processus de travail pertinents pour la mise en œuvre du projet tel que, l'allocation de fonds, les procédures d'appel d'offres, de passation de marchés et les processus de paiement, par lesquels les paiements continueront d'être effectués traditionnellement via des comptes mais sont enregistrés sur la plate forme à partir d'un API extérieur(exemple: Orangemoney, QRCode) comme le montre la figure suivante.

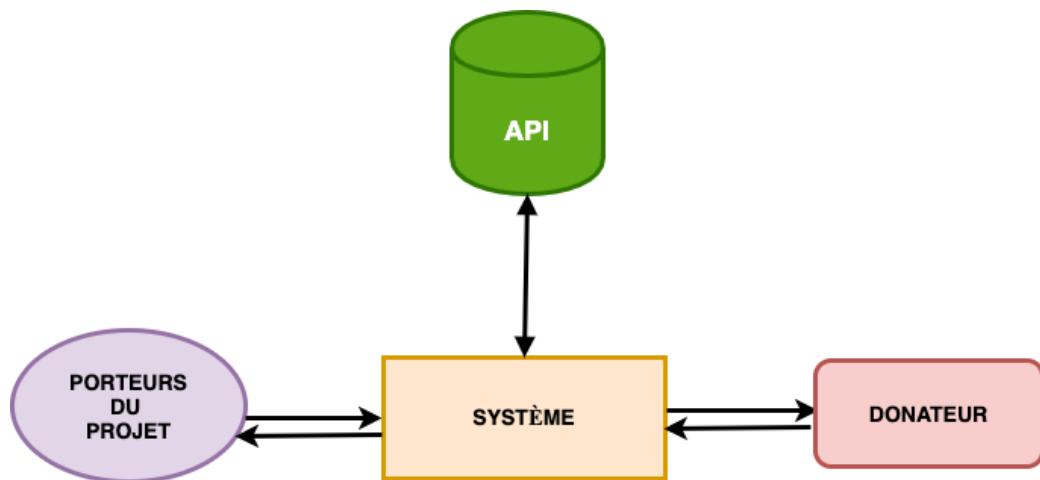


Figure 3.4:

### 3.5 Business modèle

Notre système a principalement 2 cas d'utilisation à savoir :

- aider aux porteurs de projets (personne physique ou morale) à bénéficier de financement pour leurs projets.
- mettre un système afin de rassurer les bailleurs de fonds sur l'utilisation efficace et efficient de leurs fonds.

1. **Cas d'utilisation N1** :Un système pour la résolution des aléas de confiance entre donateurs et porteurs de projets.

L'ONU estime qu'à peu près 30% [...] de l'aide publique au développement est perdue à cause de la fraude et de la corruption. Cette situation a créé un manque de confiance entre les institutions donatrices et les demandeurs d'aides. Cela a conduit à la signature de plusieurs traités et conventions, qui malheureusement n'ont pas vraiment changés grands choses aux pratiques classiques de détournement des fonds. La gouvernance de l'aide basée sur la Blockchain pourrait permettre aux États de prendre des engagements plus crédibles, améliorant ainsi l'efficacité de l'aide. Ainsi, l'utilisation de notre application contribuerait à ramener cette confiance dores et déjà perdue.

2. **Cas d'utilisation N2** :Un système pour faciliter l'obtention des dons pour les porteurs de projets (personne physique ou morale).

Des ONG, des gouvernements, des particuliers sont porteurs de projets plus souvent à caractère socio-humanitaires. Sans l'aide extérieure, ces projets ne seront jamais réalisés au bénéfice des populations locales. La majeure partie de ces entités ont du mal à trouver des moyens pour rentrer en contact avec les bailleurs de fonds crédibles. Notre application leur permet à cet effet, de rentrer en contact avec ces bailleurs, mais de gérer également les fonds reçus de façon crédible et transparente.

### 3.6 Les différents Scénarios concernant les Porteurs de Projets

Dans la réalisation de notre projet TruthDonation, de la soumission des propositions par les porteurs jusqu'au financement des projets retenus en passant par le vote des bailleurs, il existe plusieurs scénarios possibles. Dans cette section, nous décrivons quelques-uns de ces scénarios, leurs avantages et leurs inconvénients avant de présenter celui choisi à mettre en place dans notre projet. Pour ce qui est des porteurs de projets, toutes les propositions doivent être déposées sur la plateforme par le proposant.

**1er cas :** Une fois que le proposant est inscrit sur la plate-forme, il a la possibilité de déposer ses propositions de projets. Le système valide toutes les propositions et elles sont directement visibles par les votants.

**2eme cas :** Chaque porteur peut déposer ses propositions sur la plate-forme du moment où il est déjà inscrit, mais une proposition ne peut être visible par les bailleurs/investisseurs que lorsqu'elle est validée par l'administrateur de la plate-forme. Dans notre approche, nous avons choisi d'implémenter le deuxième cas, cela nous permettra d'éviter que n'importe quelle type de proposition soit visible par les donateurs. C'est pourquoi après le dépôt des propositions, une analyse de leur contenu est effectuée afin de vérifier leur cohérence avant d'être validé et visible par les votants.

### 3.7 Les différents scénarios pour le Bailleu

#### 3.7.1 Scénario 1

**Description du scénario :** Chaque projet proposé est associé à un compte proposant et a une clé publique. Les personnes qui investissent pour le projet envoient directement leur crypto-monnaie à l'adresse publique du compte proposant.

**Les étapes :**

1. Le bailleur clique sur le bouton investir d'un projet.
2. Le système affiche la clé publique du projet.
3. Le bailleur va sur son wallet pour faire la transaction en utilisant la clé publique fournie.
4. Le système met à jour le total de l'investissement du projet en question

**Avantages du scénario :**

- Les donateurs peuvent utiliser les wallets qu'ils possèdent déjà pour faire la transaction.
- Permet aux personnes qui proposent des projets de définir quel type de crypto-monnaie elles veulent récupérer
- Les donateur/bailleurs peuvent voter pour plusieurs projets.

**Inconvénients du scénario :**

- Le site a seulement l'utilité de proposer les projets mais ne fait rien de plus.
- Les donateur/bailleurs voient les projets sur le site, mais lorsqu'ils veulent investir sur un projet, ils doivent aller sur un autre site / une autre application pour faire la transaction.
- La personne proposant le projet, peut partir avec l'argent directement, car c'est son compte qui contient les investissements et cela même si son sa proposition n'atteint pas son objectif.
- A notre niveau, nous ne pouvons pas gérer le blocage des investissements jusqu'à la fin du vote car le site ne gère pas les comptes des proposants et ne peut pas les forcer à rendre l'argent lorsque leur projet ne gagne pas.

#### 3.7.2 Scénario 2

**Description du scénario :** Chaque bailleur possède un compte sur le site. Lors de son inscription, les clés privés et publics lui sont fournies pour qu'il puisse remplir son compte avec certaines crypto-monnaies. Un ensemble de projets lui est proposé sur la plate-forme, il peut analyser les différentes propositions et peut voter pour au deux propositions au maximum. Lorsqu'il souhaite voter pour une proposition, il choisit combien de sa monnaie il veut y investir et la monnaie est transférée sur le compte de gestion du site internet. Lorsqu'une proposition pour laquelle il a voté atteint son objectif, la proposition est considérée comme gagnante, ainsi le montant reste dans le compte du gestionnaire et le proposant peut faire le retrait progressivement tout au long de la réalisation du projet.

**Les étapes :**

1. Le bailleur choisi la monnaie et rentre la valeur qu'il souhaite investir dans le projet et ensuite clique sur le bouton investir.
2. Le système transfert la monnaie vers le compte de gestion et prend en compte la somme pour le projet.
3. Après le vote, lorsqu'un projet atteint l'objectif, le compte de gestion bloque la monnaie correspondante a l'investissement du projet, moins les taxes.

4. Lorsqu'un projet n'atteint pas l'objectif, le compte de gestion renvoie la monnaie correspondante au bailleur, moins les taxes.

**Avantages du scénario :**

- Le bailleur peut voter / investir pour plusieurs projets.
- Le site gère la monnaie entre les votes, donc la monnaie n'est transférée au vainqueur que lorsque sa proposition a gagné et cela de manière échelonnée.
- 

**Inconvénients du scénario :**

- Plusieurs éléments sont à prendre en compte lors du développement.
- Le montant est géré par le gestionnaire

**Scénario 3 ( scénario Choisi)**

**Description du scénario :** Dans ce scenario, nous savons que chaque projet proposé est associé à un porteur. Chaque donateur dispose d'un compte lui permettant de participer aux votes et aux donations. Il possède nos tokens qu'il a acheté avec une certaine crypto-monnaie. Une fois que le vote est lancé par l'administrateur, chaque donateur peut voter pour deux projets au maximum. La proposition gagnante sera celle soumise à la donation. Chaque donation s'effectue sur une période d'un mois. Tout au long de cette période, le porteur ne peut pas retirer l'investissement en cours. Une fois que la donation clôturée, si la proposition a atteint son objectif le montant correspondant sera débloqué pour permettre au porteur de retirer périodiquement la monnaie. Si la proposition n'a pas atteint son objectif, une période de donation supplémentaire d'un mois est accordée afin d'aboutir à l'objectif. A défaut les différents dons seront retournés aux donateurs sur leurs comptes moins les taxes. Puisqu'il faut atteindre un certain objectif pour recevoir l'investissement, une proposition n'ayant pas atteint l'objectif ne peut pas être le vainqueur. Donc il se peut que lors d'une période de vote, il n'y ait aucun vainqueur.

**Les étapes :**

1. Le bailleur s'inscrit/se connecte
2. Le bailleur analyse et vote pour une proposition
3. Le bailleur clique sur le bouton investir pour la proposition gagnante.
4. Le système affiche la clé publique du projet.
5. Le bailleur va sur son wallet pour faire la transaction en utilisant la clé publique fournie.

**Avantages du scénario :**

- Les bailleurs peuvent utiliser les wallet qu'ils possèdent déjà pour faire la transaction.
- Les bailleurs peuvent voter pour plusieurs projets.
- Seule la proposition gagnante est soumise à la donation
- Les donations ne sont débloquées que si la proposition gagnante atteint son objectif, donc pas de risque de perdre les dons car elles seront retournées aux donateurs respectifs.

**Inconvénients du scénario :**

- Le cours des monnaies change, donc il faut prendre en compte ce paramètre lors des achats et ventes de tokens.
- Les personnes peuvent voter uniquement pour un projet à la fois.
- Plusieurs éléments à prendre en compte lors du développement

### **Choix du scénario**

Le choix final du scénario à développer dans le site est le scénario 3. Pour arriver au choix de ce scénario, plusieurs problèmes ont été évoqués et pris en compte. D'abord, Il y a le problème qu'en faisant un investissement directement sur le compte du proposant, il peut récupérer l'argent directement et ne pas le rendre aux donateurs même si son projet n'atteint pas son objectif. C'est pourquoi, pour sécuriser ces fonds, le système empêche que les cryptos disponibles sur le compte du proposant puissent être retiré avant la fin de la donation et avant que le projet atteint son objectif de financement. Ensuite, nous avons dissocié le vote pour les propositions et les donations afin de rendre le système plus transparent et facile à utiliser. Nous avons également fait en sorte qu'à chaque lancement d'un vote, seul 4 propositions soient soumises aux donateurs pour élire une proposition qui à son tour sera soumise à la donation. Cela nous permettra d'éviter de plonger la période de donation car elle aura plus de chance d'atteindre son objectif.

### 3.8 LE ROADMAP

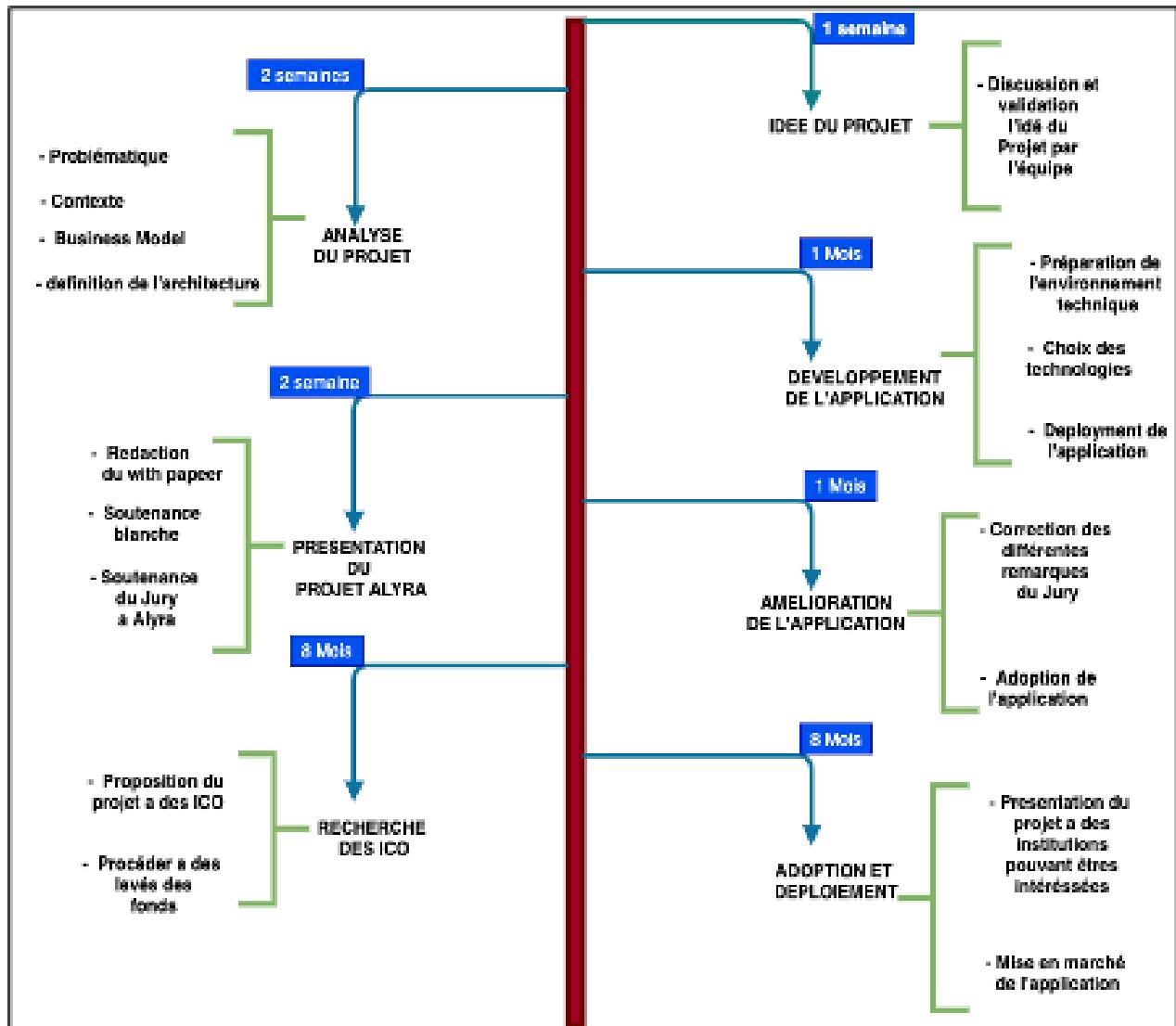


Figure 3.5:

### 3.9 Déploiement et Contraintes Techniques

TruthDonation est une application décentralisée qui sert d'interface entre des porteurs de projets et des bailleurs de fonds ou des donateurs. Il est défini pour cela des périodes au cours desquelles des propositions seront soumises sur la plate-forme par les porteurs des projets, validées puis soumis aux votes des donateurs. Pour chaque période, un ensemble de 4 projets déposés par les porteurs sont validés et visibles par les donateurs. Les donateurs qui le souhaitent peuvent parcourir, analyser et choisiront la/les propositions qui leurs ont le plus séduit. Toutefois, à la fin du vote, une seule proposition (la proposition gagnante) sera soumise à la phase de donation. L'implémentation globale de notre application se présente comme suit:

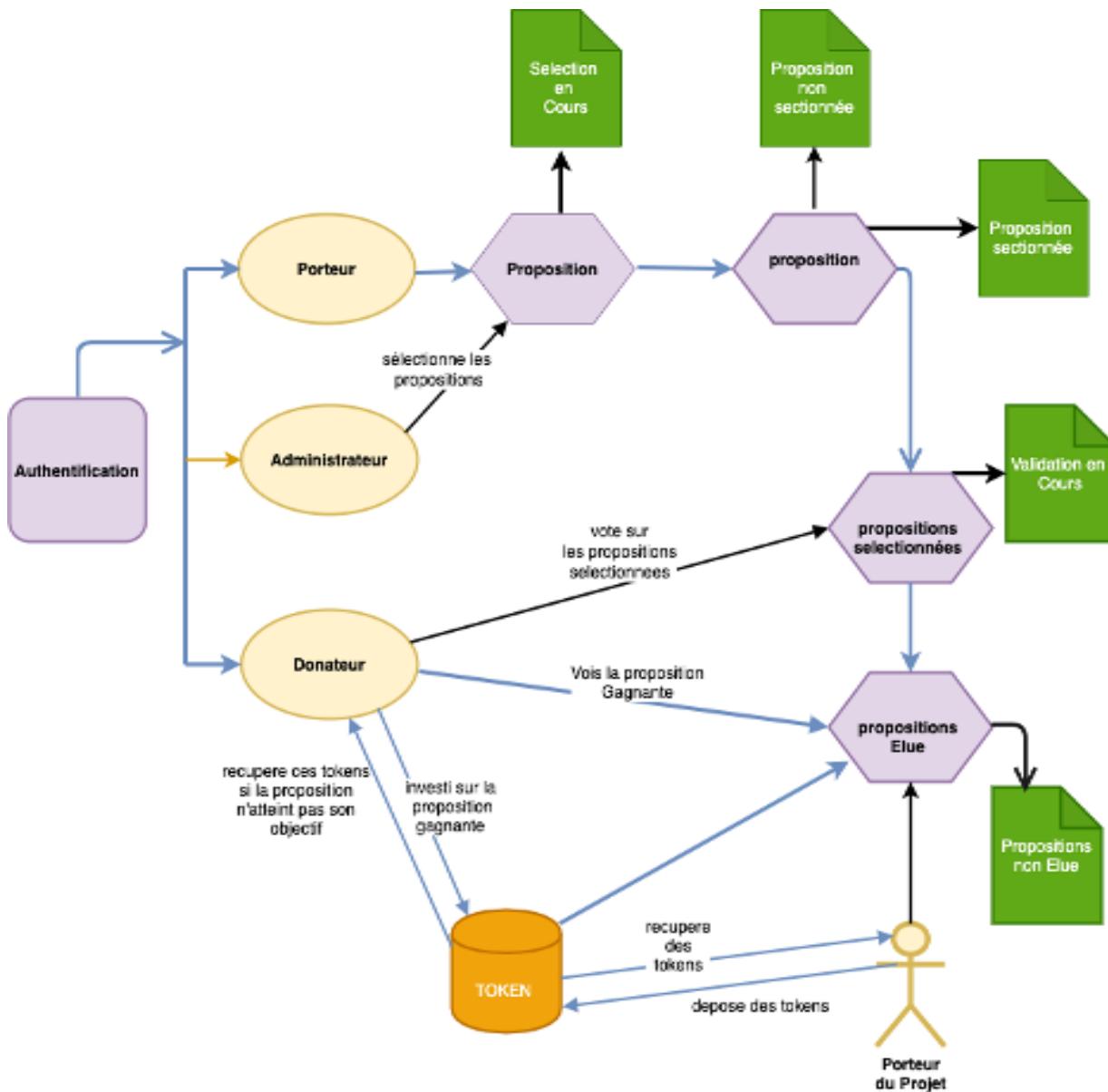


Figure 3.6:

### 3.10 Défis techniques

Le développement du scénario choisi plus haut va apporter des défis techniques. Ces derniers sont expliqués ci-dessous:

#### 3.10.1 Gestion du compte “TheCrytos”

Il faut nécessairement savoir gérer un compte directement dans le code. Le site devra être au courant de toutes les transactions faites vers son compte et devra savoir quoi en faire et à quel moment.

#### 3.10.2 Remix

Est un environnement de développement qui permet développer des applications de smart contrat. IL permet aussi de développer, compiler, déployer et tester des smart contrats

#### 3.10.3 Ganache

C'est une blockchain qui nous a permis de simuler localement notre contrat. Disposant des comptes locaux et des balances Ethereum il nous a permis de bénéficier des services relatifs à la Blockchain, le Web3 provider par exemple.

#### 3.10.4 MetaMask

MetaMask est un portefeuille de crypto-monnaies qui peut être utilisé sur les navigateurs Chrome, Firefox et Brave. Il permet de faire le lien entre un navigateur classique et la blockchain Ethereum. Il s'agit également d'une extension pour navigateur qui permet de parcourir la blockchain Ethereum. Le wallet MetaMask permet de stocker les clés des tokens Ethers et ERC-20. Il permet également, d'envoyer ou/et de signer des transactions.

#### 3.10.5 Gestion des transactions

Il y'a la gestion des transactions des donateurs, il faudra savoir c'est qu'une réussite de transaction, comment savoir qu'une transaction a été faite et pouvoir les incrémenter.

#### 3.10.6 Gestion des taxes

La gestion des taxes fera aussi partie d'une réflexion, il faudra savoir à combien s'élèvent les taxes de transaction, comment les payer et comment les calculer pour que la transaction soit valide.

#### 3.10.7 Gestion de la sécurité

Il ne faut pas que les clés privées soient enregistrées. L'utilisateur doit rentrer la clé privée uniquement pour se connecter et faire des transactions. La clé publique peut être enregistrée quant à elle.

#### 3.10.8 Exemple de période de vote

La crypto-monnaie utilisée pour faire les investissements est : TheCrytos qui est notre propre crypto-monnaie.

Exemple du déroulement d'une fin de période de vote et de donation avec l'objectif commun de 200 000.

NUMERO	PROPOSITION ID	PROJET	NBRE DE VOIE	Objectif
A.	Afs10	Aide à la scolarisation des jeunes filles	4	200 000€
B.	Fax05	Réalisation d'un forage	3	280 000€
C.	Bhc89	Réalisation d'un barrage hydroélectrique	0	1 000 000€
D.	Cee07	Projet de construction d'une école	2	300 000€

Figure 3.7:

A la sortie de ce vote, seule la proposition A qui a obtenu plus de vote sera soumis aux donateurs pour l'investissement. A partir de leur interface, les proposants peuvent suivre directement le vote et savoir si sa proposition est nominée ou pas. En plus, des notifications leurs sont automatiquement envoyées pour confirmer le résultat du vote.



## 4. ANALYSE DU MARCHÉ

### 4.1 Introduction

Bien qu'un ce soit un sujet ambitieux, dans un domaine passionnant, notre projet vient rejoindre un ensemble de projets dans le marché. La sécurisation des fonds d'aide international est devenue depuis quelques années un sujet réel au centre des discussion non seulement dans le milieu de la recherche mais aussi dans celui des innovations technologiques. Particulièrement depuis l'avènement de la technologie Blockchain en 2008. Durant ces dernières années, plusieurs beaucoup de projets ce sont créés autour de cette idée. Nous donnerons ici les projets les plus significatifs que nous avons trouvés dans la littérature.

### 4.2 DISBERSE:

Disberse est une plate-forme de gestion de fonds qui stimule le flux et la livraison transparents, efficents et efficaces de l'aide au développement et humanitaire, basée sur la technologie de la blockchain. La plate-forme permet aux donateurs, aux gouvernements et aux ONG de transférer et de retracer les fonds à travers toute la chaîne, du donneur au bénéficiaire via des intermédiaires. La plate-forme reçoit les fonds des donateurs en monnaie fiduciaire et les garde sous séquestre. Il tokenise ensuite les fonds et les verse en tant qu'argent à toutes les parties prenantes impliquées dans un projet donné via leur wallet.



Figure 4.1:

#### 4.3 TruBudget :

La Banque de développement KfW et le bureau numérique de KfW ont développé un logiciel qui peut servir de plate-forme pour suivre et coordonner la mise en œuvre des investissements financés par des dons. En promouvant la confiance des partenaires donateurs, TruBudget cherche à rendre l'utilisation des systèmes de donations viables. Implémenter déjà au Burkina Fasso, Georgia.

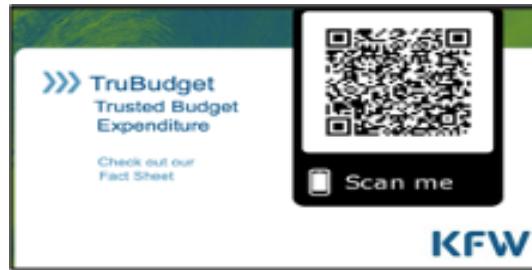


Figure 4.2:

#### 4.4 AID : Tech

AID:Tech a développé une plateforme basée sur la blockchain pour garantir « l'intégrité des contributions caritatives et des programmes de protection sociale ». En partenariat avec la Croix-Rouge irlandaise, la société a livré une aide à 500 réfugiés syriens au Liban en utilisant la technologie de la blockchain. Les réfugiés ont obtenu un identifiant unique enregistré sur la blockchain qu'ils peuvent utiliser pour acheter des produits dans les magasins partenaires locaux. Le système fonctionne même lorsque les réfugiés ne sont pas connectés à Internet car leurs cartes de paiement ont un code QR estampillé dessus.



Figure 4.3:

## 4.5 EN QUOI LE PROJET DIFFÈRE-T-IL

Même si aujourd’hui plusieurs applications existent dans ce domaine et sont majoritairement mises au marché. Notre application se démarque à plusieurs niveaux. Le tableau ci-contre en est la démonstration :

	ThruthDonation	AID : TECH	TRUBUDGET	DISBERSE
Secteur d'intervention	Solution Blockchain	Développement General	Développement General	Développement General
Type de Modèle	Infrastructure	Service	Service	Infrastructure
Modèle de traçabilité	End to End	Transfert Cash	End to End	End to End
Utilisation de la blockchain	Oui	Oui	Oui	Oui
Domaine d'expertise	Haut	Bas	Haut	Haut
Autres	Basé sur un système de vote	Non	Non	Non
	Tokenizer	Non	Non	Non
	Accessible aux porteurs de projets	Non	Non	Non

Figure 4.4:

## 4.6 Description de TheCriptos

Le token "TheCriptos" représente le Token qui sera utilisé sur notre plateforme afin d'effectuer des donations et autres transactions. Cette tokenization va nous permettre de fidéliser les différents partenaires de notre application. Ce token sera également utilisé pour:

- Les Paiements des noeuds et autres moyens de paiement
- Les Smart-contract
- Le référencement

## 4.7 Gouvernance

Les blockchains réussies doivent s'adapter et changer au fil du temps. Alors que les blockchains privées peuvent être modifiées à volonté, les blockchains publiques et de consortium sont chacune régies par un modèle de consensus avec des règles spécifiques intégrées dans la logique de la blockchain. La gouvernance définit les incitations économiques pour les participants et les règles de modification de la blockchain pour répondre à l'évolution des besoins ou des défis. Le nombre de modèles de gouvernance est presque aussi grand que le nombre d'écosystèmes blockchain, et de nouveaux naissent chaque jour. Bien qu'un traitement complet de ce sujet dépasse le cadre de ce rapport, on dit souvent que la gouvernance est le facteur le plus important pour déterminer la réussite d'un écosystème de Blockchain. Les incitations économiques sont-elles suffisantes pour encourager tous les participants nécessaires ? L'intégrité de la blockchain peut-elle être garantie ? La blockchain peut-elle évoluer et changer à l'avenir ?

Comme toute technologie relativement nouvelle, la blockchain présente de nombreux défis, et en particulier après l'introduction d'Ethereum en 2014. Les plus grands défis sont spécifiques aux chaînes de blocs publiques, ou sont au moins plus faciles à gérer ou à compenser dans les chaînes de blocs privées et de consortium. Les applications qui nécessitent une blockchain publique dépendent souvent des innovations futures pour surmonter les limitations actuelles, bien qu'elles puissent être prises en charge dans la blockchain d'aujourd'hui privée ou en consortium. Dans certains cas, les compromis peuvent être acceptables, dans d'autres non. Les défis les plus couramment cités pour la technologie de la Blockchain sont la vitesse de transaction ; la taille des blocs, le coût, la gouvernance, la questions réglementaires et internationales ; l'ensemble de talents et de compétences ; les risques techniques, les risques financiers et l'escroquerie blockchain.

### 4.7.1 Vitesse de transaction

Les blockchains publiques ne prennent actuellement pas en charge les délais de confirmation quasi instantanés attendus pour de nombreux types de transactions. Les blocs Ethereum sont actuellement écrits toutes les 15 à 20 secondes et les transactions peuvent être ajoutées au bloc suivant à moins que l'expéditeur n'offre une incitation financière suffisamment importante (c'est-à-dire un coût). Selon sa conception actuelle, Ethereum ne peut traiter qu'environ 15 transactions par seconde. En outre, la plupart des participants ne considéreront pas une transaction comme réellement confirmée tant que six blocs supplémentaires n'auront pas été ajoutés par la suite. La vitesse de transaction n'est généralement pas un problème dans les blockchains privées car les blocs ajoutés le font automatiquement pas besoin de frais de calcul.

#### 4.7.2 Taille du bloc

La plupart des écosystèmes de blockchain courants ont des limitations de taille qui ont un impact non seulement sur la vitesse des transactions, mais également sur la quantité de données qui peuvent être stockées sur la blockchain. Pour cette raison, il est recommandé de minimiser la quantité de données stockées sur la chaîne. Certains écosystèmes, comme Ethereum, ont des capacités de stockage « latérales » intégrées telles que Swarm et IPFS qui maintiennent de nombreuses fonctionnalités clés du stockage de données de la chaîne de blocs sans créer d'enregistrements sur la chaîne principale.

#### 4.7.3 Le Coût

L'approche actuelle de « preuve de travail » pour valider les nouveaux blocs, utilisée par les chaînes de blocs publiques communes, y compris Bitcoin et Ethereum (mais pas par les chaînes de blocs privées), est très coûteuse en terme de calcul et nécessite d'énormes quantités d'électricité. Plus d'électricité que ce qui a été utilisé par l'ensemble du pays de la Nouvelle-Zélande. Combiné avec des limitations sur la taille des blocs, cette rareté de disponibilité et les coûts de transaction élevée. Depuis plusieurs années, Bitcoin coûte rarement plus de 0,25\$ par transaction, mais au début de 2018, il a atteint un sommet de 54,90\$ par transaction. Les nouvelles approches de validation sont beaucoup moins exigeantes en termes de calcul et offrent la promesse de coûts beaucoup plus bas. Ce qui en fait une priorité majeure actuelle dans l'innovation de la blockchain publique. Le protocole Ethereum Casper envisagé actuellement dans les tests utilise une « preuve de participation » pour valider les transactions plutôt qu'une « preuve de travail ». La blockchain NEO utilise une approche appelée tolérance byzantine déléguée aux pannes



## 5. LES INTERFACES DE ThruthDonation

### 5.1 Inscription:

La page « inscription » permet aux personnes de créer un compte en entrant leur adresse email. Suite à ça, elles reçoivent leur clé publique et privée par email.

### 5.2 Connexion:

La page « connexion » permet à un utilisateur préalablement inscrit de se connecter au site. Pour se faire, il aura besoin de sa clé privée et de sa clé public.

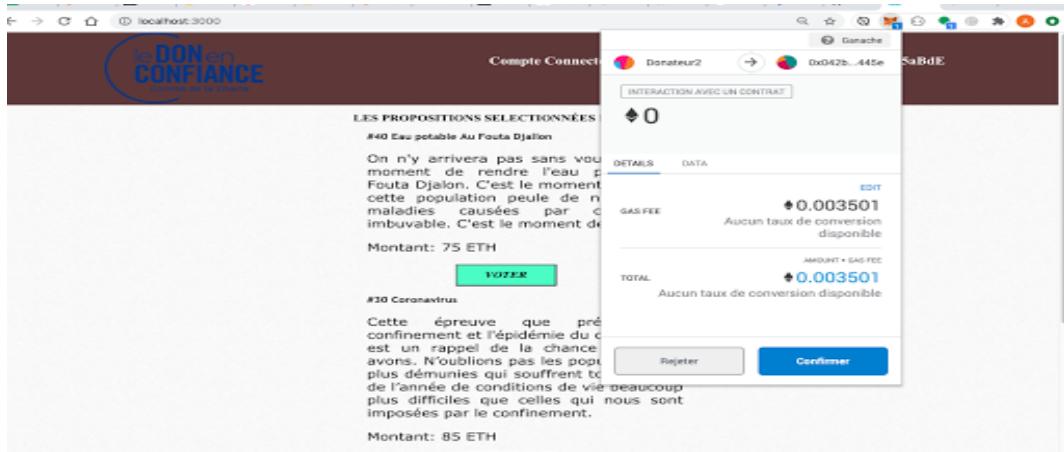


Figure 5.1:

### 5.3 Acceptation :

Cet interface s'affiche lors de la première connexion de l'utilisateur. Elle affiche le règlement /fonctionnement de TruthDonation. Et pour entrer dans le site, l'utilisateur doit obligatoirement accepter le règlement en cliquant sur le bouton « lu et accepter ».

### 5.4 Création de proposition :

Elle permet de créer une proposition, elle contient les champs de dates qui sont à remplir. De plus, il y a un éditeur de texte qui permet de mettre en forme et soigner la présentation de la description du projet, d'y ajouter des images, ou encore d'importer un fichier PDF.

### 5.5 Liste des propositions:

Elle affiche la « liste des propositions », en cours de vote, il y a la liste des propositions de projets pour la période en cours, avec pour chaque proposition, son nom, la date de début et de fin du vote ainsi que le lien pour aller voir la proposition en détail. De plus, il y a un onglet pour voir les propositions précédentes et leurs état (propositions en attentes d'être soumises au vote, propositions déjà nominées ayant atteint leur objectif ou non). Il y a également un bouton qui permet d'aller sur la page de création d'une proposition.



Figure 5.2:

## 5.6 La proposition Gagnante:

C'est la proposition qui aura recueilli le plus de vote et qui sera soumis à la donation des bailleurs. Elle a une échéance de donation d'un mois, renouvelable un mois si jamais l'objectif n'est pas atteint lors de la première échéance. Une fois l'objectif atteint, le système clôture automatiquement la donation.



Figure 5.3:

## 5.7 Donation :

Cette page contient l'historique des donations fait pour la proposition de projet correspondante. Chaque ligne, contient la clé publique du donateur, la date et l'heure de l'investissement, le nombre de token investis et le lien vers une représentation en JSON de la transaction complète. Elle contient également un bouton investir pour la proposition gagnante, qui permet de réinvestir ou d'investir à nouveau.

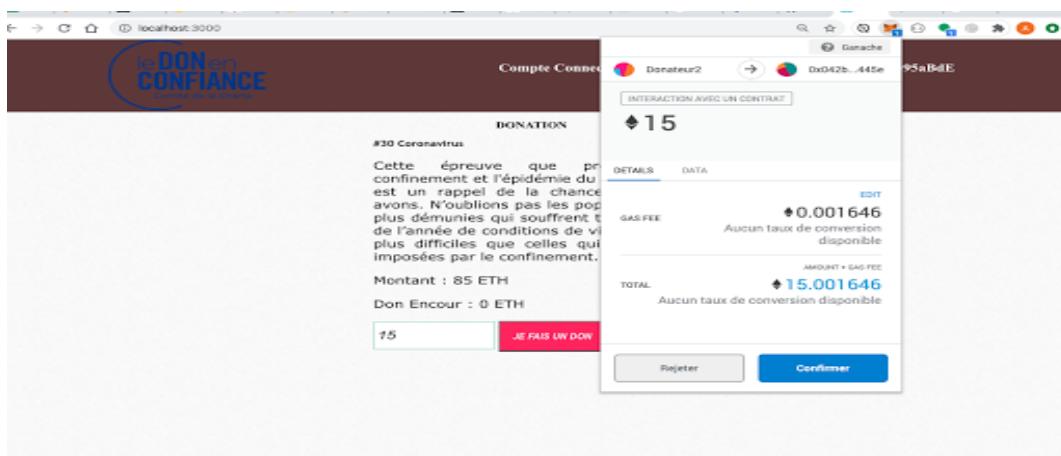


Figure 5.4:

**5.8 Règlement:**

Nous avons édité un ensemble de règles en accord avec la loi. Ces règles sont clairement décrites sur la page intitulée « règlement ». Les utilisateurs doivent les lire et accepter les conditions d'utilisation et de fonctionnement. Ce règlement doit être accepté lors de la première connexion. Dans le respect des lois sur la protection des données (RGPD ou d'autres lois), aucune donnée personnelle des utilisateurs n'est stockée dans ThruthDonation.

## NOTRE EQUIPE



### CHEF DE PROJET

#### **Mamadou Dian BARRY**

Jeune cadre dynamique, avec un esprit d'équipe, motivé, rigoureux et passionné des technologies. Il dispose de connaissances et de compétences en Blockchain, data science, Intelligence Artificielle, Machine Learning Deep Learning, réseaux et systèmes, avec une bonne maîtrise de l'anglais. Diplômé d'une licence en Réseaux et Télécommunications, puis d'un master en Intelligence Artificielle, il prépare actuellement un deuxième master spécialisé en traitement de signal et d'images médicales à l'Université de Clermont Ferrant. Il a une expérience en tant que consultant et chef de projet. Il a travaillé en tant que chef de Projet chez Labomobile\_Link Guinée pendant plus de 3 ans. Dans le cadre de son stage de master effectué au laboratoire de recherche de l'Université de La Rochelle, il a mis en place des algorithmes robustes pour le Service Hydrographique et Océanographique de la Marine pour la numérisation automatique des maregrammes. Ces travaux ont permis de mesurer l'évolution du niveau de la mer depuis le 350 dernières années et ainsi prédire également son évolution dans les 100 prochaines années. Il a participé à l'Institut Francophone International à Hanoi au développement d'un modèle Deep Learning pour la détection et la classification des images médicales (cas du cancer de la peau). Très passionné par la Blockchain, il travaille sur ce projet en tant que chef de projet. Il assure la modélisation, la conception de l'architecture générale du projet. Il Analyse et donne les objectifs du projet, définit les méthodologies de développement, il planifie les réunions avec l'équipe de développement, il fait l'estimation et la gestion des risques.



#### **DEVELOPPEUR BACK-END**

**DIALLO ABDOULRAHAMANE** est diplômé d'un master II en Génie Logiciel a de l'Université de Grenoble. Il a été consultant en tant que Concepteur Développeur Informatique, chez Crédit Agricole, Edf, Coriolis. Réalisant plusieurs projets qui sont soit des projets individuels, soit des projets en équipe avec différents langages (c#, java Scripts, Sql Linq to Entities, Html5, JQuery, typescript). Aujourd'hui passionné dans le monde de Blockchain, il s'est lancé dans ce domaine pour devenir un développeur web Blockchain, en suivant la formation de développeur Blockchain chez Alyra. Sur ce projet il travaille en tant que Développeur Blockchain en utilisant les technologies telles que (Solidity, React js, JavaScript, etc ...).