

## Table des matières

I-	PRESENTATION DU PROJET .....	2
1.	A PROPOS DE SOMBE .....	3
2.	GOUVERNANCE COMMUNAUTAIRE ET LE STAKING .....	3
3.	TRANSACTIONS PRIVEES ET INSTANTANEEES (protocole suspendu) .....	4
4.	APPROCHE PHILOSOPHIQUE DE LA CRYPTOMONNAIE SOMBE.....	4
II-	FONCTIONALITES .....	5
1-	Protocole Zerocoin (protocole suspendu).....	5
2-	Le protocole iBanX .....	6
3-	Code de Base : Pos 3.0 Bitcoin Core 0.10.x .....	6
4-	Mécanisme d'équilibre de récompense des blocs.....	6
5-	Masternodes .....	6
III-	Caractéristiques de la pièce.....	7
1-	Désignation .....	7
2-	Core spécification.....	7
3-	Taux d'émission de la pièce Coin.....	7
4-	Eligibilité.....	7
a.	Eligibilité des SBE en POS.....	7
b.	Eligibilité des transactions envoyées .....	7
c.	Eligibilité ibanX .....	7
5-	Différentes phases .....	8
a.	Phase de distribution des pièces pré-minées .....	8
b.	Phase Proof of Stake (PoS) .....	8
	CONCLUSION .....	8

## I- PRESENTATION DU PROJET

Le projet SOMBÊ est le projet d'une cryptomonnaie développée par un groupe de cryptopationnés et qui croient que la technologie de la blockchain est une révolution à laquelle il est important de participer. Le but du projet est de mettre à la disposition de la population et aux jeunes entrepreneurs africains un instrument moderne de paiement alternatif sécurisé et totalement décentralisé sur un réseau de personne à personne (peer to peer) basé sur la technologie de la blockchain et de la cryptographie.

L'enjeu avec cette technologie c'est que chaque citoyen devienne sa propre banque en installant un nœud du réseau SOMBE sur son ordinateur ou son téléphone mobile.

L'objectif est de faciliter la vie à des millions d'africains qui pour la plupart sont exclus du système financier classique contraignant et lourd en leur permettant de faire des :

- Transactions rapides
- Transactions moins chères en frais
- Transactions partout dans le monde entier
- Paiements sécurisés sur internet

SOMBÊ est une monnaie cryptée de type Proof-of-Stake (preuve d'enjeu) et centrée sur la protection de la vie privée. SOMBÊ s'efforce de construire un moyen de paiement numérique exploitable, facile à utiliser dans la vie quotidienne. À cette fin, l'objectif principal est de rendre possible des transactions rapides avec moins de frais tout en préservant la confidentialité et la sécurité.

Ce guide passera en revue la vision de la pièce, les caractéristiques techniques son réseau, le fonctionnement du staking et des masternodes.

## 1. A PROPOS DE SOMBE

SOMBÊ s'inspire des technologies blockchain DASH et PIVX et est adapté pour répondre à des besoins spécifiques. SOMBE est un système entièrement axé sur le Proof-of-Stake, utilisant un algorithme de hachage sûr et sécurisé : le Quart. La technologie de SOMBE intègre la protection de la vie privée et envisage d'être le cash numérique pour les micro-paiements peer to peer rapides et moins chers dans les magasins et sur internet en Afrique.

## 2. GOUVERNANCE COMMUNAUTAIRE ET LE STAKING

Le réseau SOMBE permet la production de 2 628 000 pièces SOMBE par an qui seront réparties comme suit :

- 45% aux Masternodes
- 45% aux Stakers
- 10% pour financer les propositions budgétaires votées par les Masternodes.

Un réseau de Masternodes est formé d'utilisateurs qui détiennent des pièces comme garantie. Ce réseau est utilisé pour vérifier et rendre anonymes les transactions, sécuriser la blockchain et voter pour les propositions de la communauté. En retour, ces masternodes reçoivent des dividendes en SOMBE sous forme de récompenses. Pour être masternode il faut disposer d'au moins 2 000 000 (deux millions) de SOMBE dans son portefeuille.

Les budgets de développement et les décisions communautaires majeures sont prises par un mécanisme de vote, décentralisant ainsi la gouvernance du projet et met le pouvoir de décision entre les mains des personnes engagées dans le succès de la technologie.

Les pièces en staking sont utilisées pour sécuriser le réseau et valider de nouveaux blocs. **N'importe quelle quantité de SOMBE peut être stockée dans le portefeuille.** Une récompense est libérée au hasard à chaque bloc (toutes les 60 secondes) en fonction du montant déposé. Plus vous détiendrez de SOMBE, plus vos chances seront grandes, mais chaque portefeuille en staking recevra des récompenses.

La blockchain utilise un mécanisme de bascule pour équilibrer les récompenses entre les Masternodes et le staking traditionnel, en équilibrant automatiquement la fréquence et la taille des récompenses à mesure que le nombre de nœuds augmente et que le réseau grandit.

### **3. TRANSACTIONS PRIVEES ET INSTANTANEEES (protocole suspendu)**

SOMBE utilise une version personnalisée du protocole Zerocoin pour rendre anonyme les transactions en masquant les adresses associées aux pièces. Ce mécanisme se base sur la technologie libzerocoin que de nombreuses crypto monnaies utilisent. Contrairement à certaines cryptomonnaies utilisant ce protocole, SOMBE pourrait être totalement anonyme, empêchant l'analyse de la chaîne de blocs de révéler les destinataires et les expéditeurs des pièces SOMBE.

Cette version interne de Zerocoin produit des transactions plus petites et plus rapides que la bibliothèque libzerocoin originale employée par d'autres monnaies, ce qui lui permet de protéger la vie privée tout en s'efforçant d'atteindre les objectifs de transactions super rapides à des frais négligeables car tous ces protocoles engendrent des frais de transactions supplémentaires.

La blockchaine SOMBE ajoute également un mécanisme pour la production automatique des pièces anonymes, ainsi il y aura toujours des pièces en circulation pour sécuriser le réseau et garder les données privées.

Pour pouvoir dépenser leur monnaie anonymement, les utilisateurs pourront choisir l'option anonyme pour convertir leurs pièces SOMBE standard en pièces 'nSBE' et les envoyer à n'importe quelle adresse SOMBE. A l'autre extrémité, un utilisateur recevra des pièces SOMBE comme n'importe quelle transaction normale, mais grâce au protocole Zerocoin, la transaction sera à la fois vérifiable sur la chaîne de blocs et anonyme quant à celui qui envoie et reçoit ces pièces. Cette manœuvre inclura des frais de transactions supplémentaires.

**Important! En raison d'une vulnérabilité découverte dans la bibliothèque libzerocoin l'implémentation de ce protocole a été suspendu en attendant un nouveau protocole.**

**En utilisant la technologie que nous appelons ibanX,** les transactions sont presque instantanées et la monnaie peut être dépensée en quelques secondes grâce à une fréquence d'émission de blocs de 60 secondes et un réseau de masternodes qui vérifient constamment les transactions.

### **4. APPROCHE PHILOSOPHIQUE DE LA CRYPTOMONNAIE SOMBE**

Le but du projet SOMBE est de créer une monnaie cryptée basée sur la technologie de la blockchaine et fonctionnant comme une véritable monnaie et de façon totalement décentralisée. La mission de la blockchaine SOMBE est de :

- Contrôler la production des pièces SOMBE
- Protéger les transactions
- Protéger les identités de ses utilisateurs

La blockchaine SOMBE produit et gère par le protocole de son algorithme de

consensus la pièce SOMBE. SOMBE n'a pas de limite maximale de pièces (total supply). La blockchain SOMBE récompense ses utilisateurs au lieu de dévaluer par l'inflation puisque chaque portefeuille peut staker et recevoir des SBE.

Pour qu'une devise soit une vraie devise et non un actif, elle a besoin de rapidité et de liquidité. Pour maintenir cette liquidité sur le marché, il faut absolument assurer la prime de minage ou de validation pour éviter la flambée des frais de minage. Le fait que SOMBE n'a pas de total supply en pièces, assure que ladite récompense sur les blocs sera permanente à 5 pièces de SOMBE par minute, soit 5% de taux d'inflation. Ce qui fait une production de:

- 300 pièces/heure
- 7200 pièces/jour
- 2 628 000 pièces/an

Ces 2 628 000 pièces produites par an seront distribuées à 90% aux masternodes et aux stakers et 10% pour la proposition de financement de projets communautaires qui seront approuvés par le réseau des masternodes. C'est comme cela que La blockchain SOMBE compte gérer l'inflation de sa monnaie.

**La blockchain SOMBE contrôle l'approvisionnement en pièces de SOMBE. Aucun développeur, concepteur, masternode et staker ou quiconque ne pourra créer de nouvelles pièces.**

Le fait qu'il n'y ait pas de total supply rend le fonctionnement de SOMBE semblable à celui d'une monnaie traditionnelle, car l'inflation introduite dans le système a pour but d'encourager l'utilisation quotidienne et éviter la rétention.

## **II- FONCTIONALITES**

### **1- Protocole Zerocoin (protocole suspendu)**

Zerocoin est un protocole qui est implémenté dans la monnaie. Il permet des transactions privées et anonymes de façon totale aux utilisateurs de la monnaie. L'implémentation du protocole Zerocoin convertit la monnaie qui est visible publiquement en une monnaie anonyme. Sous cette forme les montants apparaîtront dans le portefeuille du destinataire comme des pièces normales sans l'historique d'où elles proviendront.

**Important ! En raison d'une vulnérabilité découverte dans la bibliothèque libzerocoin l'implémentation de ce protocole a été suspendu en attendant un nouveau protocole.**

## **2- Le protocole iBanX**

Ce protocole permet d'effectuer des transactions instantanées :

Les transactions iBanX sont confirmées en quelques secondes par le réseau de masternodes, sans besoin d'attendre plusieurs confirmations pour être sûr de la validité de la transaction.

## **3- Code de Base : Pos 3.0 Bitcoin Core 0.10.x**

La monnaie est une pièce "Proof of Stake" une des rares basées sur la version 0.10 ou supérieure du Bitcoin core. C'est une forme de minage qui prend en compte la mise à disposition de la monnaie dans le portefeuille de l'utilisateur pour valider les transactions sur le réseau. Cela rend le réseau plus fort grâce à la disponibilité de plus de nœuds. Les utilisateurs qui souhaiteront participer à la validation des transactions sur le réseau et être rémunérés devront laisser leur portefeuille ouvert 24h/24 et 7jrs/7.

## **4- Mécanisme d'équilibre de récompense des blocs**

Les récompenses de blocks reçues par ceux qui gardent leurs portefeuilles ouverts et les masternodes tirés au sort par l'algorithme de consensus varient en fonction du montant détenu par les masternodes par rapport à celui détenu par les stakers. Le but est de contrôler une distribution équitable entre les services du réseau des masternodes et les stakers. Ce mécanisme ajuste la rémunération du réseau en fonction de sa taille.

## **5- Masternodes**

Les masternodes sont des nœuds implémentés en surcouche qui reçoivent une récompense basée sur leur disponibilité et leur capacité à offrir des services au réseau de manière décentralisée et de confiance mutuelle. Faire fonctionner un masternode nécessite de bloquer 2 000 000 SBE minimum comme garantie pendant toute la durée de fonctionnement du masternode. Cela donne le droit au propriétaire du masternode de :

- Voter sur les propositions de budget, de développement et de mise à jour.
- De valider les transactions.

Ces nœuds représentent l'épine dorsale des services qui sont offerts par le réseau de SOMBE. A ce titre, ils seront rémunérés un peu plus par rapport aux stakers. La régulation de leur rémunération se fait via le mécanisme de bascule.

### III- Caractéristiques de la pièce

#### 1- Désignation

- Nom : SOMBE
- Symbole : SBE
- Décimaux : 8

#### 2- Core spécification

- Algorithme Consensus : PoS
- Algorithme de Hachage : Quart
- Taille du block : 2MB
- Time du block : 60 Seconds
- Nombre de transactions per second : 173
- Forme de minage : POS
- Stake disponible : oui
- Masternode disponible: 2 000 000 SBE pour être masternode

#### 3- Taux d'émission de la pièce Coin

- Récompense de block: Maximum 5 SBE par block
- Distribution dynamique entre staker et masternode (45% masternode, 45% staker)
- Récompense pour les budgets : Maximum 0,5 SBE par block (payable mensuellement)
- Premine : 1 000 000 000 (1 milliard) de pièces sur le genesis block pour la distribution et la mise en place des 5 premiers masternodes

#### 4- Eligibilité

##### a. Eligibilité des SBE en POS

Maturité de Confirmations : 101 confirmations

Statut du portefeuille : Requiert le core wallet (installation du nœud total de la blockchain SOMBE) pour maintenir le portefeuille ouvert afin de staker.

##### b. Eligibilité des transactions envoyées

Confirmation minimale (SBE) : 6 confirmations

##### c. Eligibilité ibanX

Confirmations : une confirmation pour le verrouillage et 6 pour être dépensé.

Temps de maintien de la garantie : 15 minutes.

## **5- Différentes phases**

### **a. Phase de distribution des pièces pré-minées**

A la fin de la phase de prévente

### **b. Phase Proof of Stake (PoS)**

Cette phase sera annoncée après la phase de distribution

## **CONCLUSION**

SOMBE a pour objectif de faire des transactions, des transferts et réceptions instantanées de devise une réalité en Afrique.

En s'inspirant des protocoles existants dans la technologie de la blockchain, SOMBE ambitionne de faciliter la vie à des millions de personnes pour des transactions quotidiennes rapides moins chères et sécurisées.

Ceci est possible grâce à sa technologie qui permet d'avoir des frais de transactions extrêmement bas, qui pourront tourner autour de l'ordre des fractions de centime par transaction. Ce protocole très important sera essentiel pour des achats et des micro-paiements quotidiens et cela contribuera grandement à préparer le terrain pour que SOMBE puisse jouer un grand rôle dans l'évolution de la monnaie digitale et devenir une solution de paiement alternative en Afrique.