BULWARK

CRYPTOCURRENCY

Whitepaper de la Cryptomonnaie Bulwark

Core Team de Bulwark :

Eatbatterys (Coordinateur de Projet)

Jack (Directeur du Marketing)

SerfyWerfy (Développeur Blockchain)

Frogman (Responsable des Communications)

Patrick (Valorisation et Conception de la Marque)

Stu (Développeur Ecosystème)

La Core Team de Bulwark

Décembre 2017

Nous, la Core Team de Bulwark, confirmons que le travail présenté dans ce whitepaper est le nôtre. Là où l'information a été dérivée à partir d'autres sources, nous confirmons que cela a été indiqué dans les attributions.

Résumé

Bulwark (symbole : BWK) est une monnaie orientée vers la communauté et née de l'observation de pratiques injustes au sein de l'espace des monnaies de privacité. Notre stratégie de lancement réfléchie et juste donne l'opportunité aux participants de rejoindre un projet prometteur au commencement. Nous offrons une proposition de simple valeur sans promesse grandiose : nous délivrerons une coin de privacité qui fonctionne aujourd'hui et dans le futur en tirant profit des bonnes pratiques de DASH et PIVX. Pas de visions fantasques avec une perspective restreinte de livraison, mais une monnaie qui fonctionne sur une plateforme fonctionnelle avec un support vers le futur. Ce qui ne signifie pas que nous ne planifions pas d'innovation, mais qu'au contraire nous délivrerons des résultats plutôt que de la hype. Il y a trop de monnaies qui sont alimentées par la hype - mais complètement dépourvues de substance - et nous ne voulons pas rejoindre le cadre grandissant des coins portées par des promesses en l'air finissant par ne rien produire. Sans ICO, un démarrage en soft-launch pour les récompenses, une petite premine, et une allocation des récompenses de block favorisant les mineurs, les adopteurs de Bulwark auront un accès aux fondations d'une monnaie de privacité offrant un mélange de masternodes et de la meilleure technologie disponible pour les coins de privacité avec une roadmap de développement ayant du sens. Les masternodes seront disponibles, et fonctionnels, dès le lancement, et sont une partie fondamentale de la vision de cette monnaie, et stabiliseront la circulation, sécuriseront le réseau, et fourniront une fonctionnalité importante.

Mentions

Bulwark n'aurait pas été possible sans le travail préalable des équipes compétentes de Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash et PIVX. Les softwares open-source et leurs contributeurs sont constamment en train d'ouvrir la voie vers d’excitantes nouvelles innovations. Quand on peut construire librement sur les fondations existantes de l'information et de la connaissance, la société en son ensemble en profite. Nous sommes reconnaissants envers nos prédécesseurs pour cette opportunité de contribuer à cet écosystème grandissant.

Table des Matières

Chapitre 1

Brève Introduction aux Cryptomonnaies

1.1 Contexte

En 2009, Satoshi Nakamoto a publié un document titré *Bitcoin: A Peer-to-Peer Electronic Cash System* détaillant sa vision du commerce. La vision de Nakamoto détaillait une monnaie peer-to-peer soutenue par un proof-of-work *(preuve de travail)* basé sur le hash. Le réseau horodaterait les transactions en les hashant dans un registre persistant qui ne pourrait être changé sans refaire le proof-of-work. Les nodes choisiraient la chaîne la plus longue en tant que preuve des événements constatés par le pool avec plus grande puissance de hashing. Tant que 51% de la puissance de hashing du réseau est contrôlée par des nodes qui ne prévoient pas de faciliter une attaque, la chaîne qu'ils généreront restera la plus longue (Nakamoto 2009).

1.2 Le Block

Chaque block du réseau est précédé par un header de 80 byte contenant une copie doublement hashée en SHA256 de l'header du bloc précédent (une dérivation doublement hashée en SHA256 de tous les hashs qui ont eu lieu dans le bloc), la date et l'heure auquel le proof-of-work a commencé, la cible de difficulté à laquelle l'hash de cet header doit être inférieur ou égal, et le nonce auquel les mineurs ont atteint la cible de difficulté. Ainsi, toutes tentatives de modifier n'importe quelle transaction dans n'importe quel bloc aboutirait au refus du bloc par le réseau de mineurs (Bitcoin Core Team 2017).

1.3 La Blockchain

Les groupes de transactions sont formés en blocks et ces blocks sont placés chronologiquement dans une chaîne – formant la blockchain. La blockchain crée un historique

mouvant de toute l'activité dans le réseau et sert de modèle de consensus distribué où chaque transaction peut être vérifiée à tout moment. (Crosby et al. 2015).

1.4 Proof-Of-Work

Le proof-of-work *(preuve de travail)* est un système de vérification dans lequel les mineurs doivent dédier des ressources tangibles (électricité, coûts hardware) pour résoudre un *puzzle de mots* arbitraire et probabiliste. Pour qu'un mauvais joueur entache la blockchain avec une transaction frauduleuse, il doit compléter le proof-of-work jusqu'au point présent (Okupski 2016).

Chapitre 2

Introduction à Bulwark

2.1 Une fondation solide

Chaque maison a besoin de fondations solides, et Bulwark ne déroge pas à la règle. Bulwark est construit sur la base de *PIVX*, lui-même construit sur la base de la populaire cryptomonnaie *DASH*. Même si leurs origines peuvent être retracées au Satoshi Core originel, chaque projet a choisi une direction particulière avec des objectifs et des idéaux qui représentent la communauté qu'ils servent. Nous allons étendre, et mettre l'accent, sur les fonctionnalités de privacité des monnaies des plateformes de nos prédécesseurs en explorant de nouvelles technologies, tout en créant des tool sets et des opportunités pour l'intégration de Bulwark dans les plateformes technologiques actuelles.

2.2 Une équipe dédiée à la communauté

Pour certains projets, les communautés sont une réflexion après-coup. La priorité numéro un de Bulwark est la communauté. Avec des cadeaux, des concours, une plateforme de discussion vivante et une politique de tolérance zéro envers le harcèlement des nouveaux arrivants, Bulwark aspire à être la communauté pour toutes sortes d'utilisateurs finaux. Les membres de notre base d'utilisateurs contribuent déjà avec des scripts utiles et des guides pour améliorer l'expérience utilisateur

2.3 Equitable et équilibré

A l'heure où ce document est rédigé, il y a eu un afflux de cryptomonnaies utilisant des fondations similaires. Alors que la technologie sous-jacente est sérieuse, souvent un examen approfondi de leurs spécifications et des paramètres de la blockchain révèle des pratiques moins que justes.

2.4 Le problème des méthodes de pre-mine

2.4.1 Etude de cas : FooBarBazCoin

Une pratique grandissante dans l'espace des cryptomonnaies est de choisir une date arbitraire loin dans le futur et de baser un pourcentage de premine sur la masse monétaire à cette date. Jetons un coup d'œil à la fictive FBC (*FooBarBaz Coin*), un fork de *DASH*.

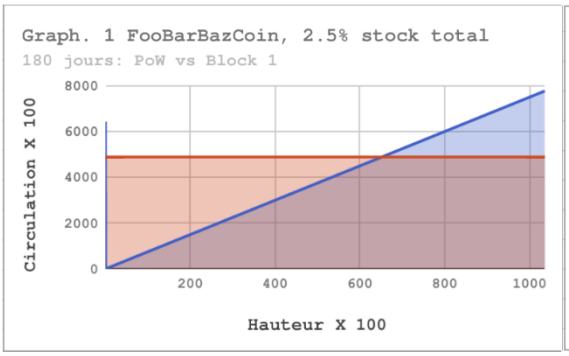
- Récompense par Block : 15
- Durée par Block : 2.5 minutes
- Partage POW/Masternode : 50/50%
- Algorithme de difficulté initial : KGW
- La subvention est réduite de 12% chaque année
- Masse Maximum de Coins : ~25 Millions
- Pre-mine de 2.5%

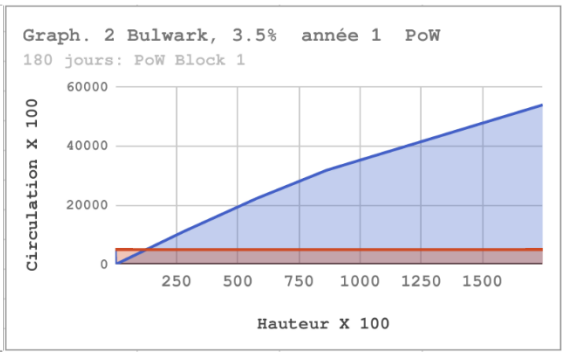
Dans cet exemple, une pre-mine annoncée de 2.5% équivalant à ~643,000 coins (sur ~25 Millions) semble raisonnable à l'observateur lambda. Cependant, pour que les récompenses de PoW et de Masternodes, toutes les deux, correspondent aux coins que les développeurs possèdent, cela prendrait approximativement 43,000 blocks. A un objectif de 2.5 minutes par block ; cela prendrait à peu près 150 jours aux mineurs (ou 75 jours globalement) pour générer le même nombre de coins. Après 75 jours, les développeurs auraient toujours le contrôle de la moitié des coins existantes.

2.5 Une alternative plus équitable

L'équipe de Bulwark en a eu conscience, et a décidé d'être franche. Notre pre-mine de 489,720 coins (3.5%) représente un peu moins de 12 jours de minage PoW ou à peine plus que 10 jours de production globale. Nous avons espoir que cela servira à instiller une tranquillité d'esprit dans la communauté, à un certain moment, le marché ne pourra pas être significativement dévalué à cause des coins possédées par la core team. Comme vous pouvez le voir dans les graphiques ci-dessous, représentant tous les deux un scénario de 180 jours, la différence est flagrante. Nous espérons qu'en approchant le sujet de manière franche, cela créera un précédent et bénéficiera à l'ensemble de la communauté.

2.5.1 Comparaison des deux approches





2.5.2 Les Instamines et Notre Approche

Dash (Darkcoin) présente une étude de cas intéressante sur le besoin de protection contre l'instamine. Presque 10-15% de l'ensemble de la masse monétaire de Dash fut créé dans les premiers jours de l'existence de la coin grâce à quelques utilisateurs entreprenants (Wiecko 2017). Notre approche au problème de l'instamine fut double. Nous avons utilisé une subvention lente dans laquelle les premiers 960 blocks (1 jour) ont atteint linéairement la récompense de block complète, de même 100% des récompenses de blocks sont allées aux mineurs ce jour-ci. Historiquement, ceci a été approché par une très faible récompense de block qui change soudainement à une certaine hauteur vers une récompense de block complète, cependant, cela a souvent abouti à des pools se faisant délibérément DDOS ou submergées par la nouvelle affluence de mineurs. Avec une récompense augmentant linéairement, il n'y aurait aucun intérêt d'essayer d'interférer avec les mineurs ou les opérateurs de pool pour des gains financiers.

2.5.3 ICO? Plutôt IC-NON!

Il faut admettre, qu'en ce moment même, nous sommes constamment confrontés aux ICOs. Alors qu'elles ont leur place légitime dans l'écosystèmes des cryptomonnaies, souvent elles ne servent qu'à concentrer des poches de richesse. Etant donné que Bulwark offre des récompenses de Masternode, et dans sa deuxième phase, des récompenses de proof-of-stake *(preuve d'enjeu)*, cette concentration de richesses peut causer d'importantes variations sur le marché et basculer le système de gouvernance fortement en faveur des premiers (et plus riches) utilisateurs. Alors qu'une concentration des richesses est inévitable en général, nous croyons que toute opportunité de garder le terrain de jeu équilibré est à prendre. Le lancement s'est fait avec une stratégie de récompense de block graduée, une mécanique de lancement juste pour encourager une large distribution de Bulwark parmi plusieurs utilisateurs, évitant idéalement une partie des concentrations de richesse vues dans d'autres projets.

2.6 Rapide et fonctionnel

Avec une durée de block de 90 secondes, le consensus des masternodes et le verrouillage des transactions, un programme d'émission raisonnable, et un staking écologique, bulwark aspire à être une cryptomonnaie réellement rapide et fonctionnelle.

Chapitre 3

Nos Paramètres de Blockchain

3.1 Les spécifications de Bulwark en un coup d'oeil

Tableau 3.1: Les specifications de Bulwark en un coup d'oeil

Spécification	Descripteur
Symbole	BWK
Algorithme	NIST5
Port RPC	52541
Port P2P	52543
Durée de Block	90 Secondes
Algorithme de Difficulté	Dark Gravity Wave v3.0
Taille de Block	1MB
Maturité Mined/Minted	67 Blocks (~100 Minutes)
Confirmation	6 Blocks (~9 Minutes)
Circulation (1 an)	14,505,720 BWK
Circulation (5 ans)	27,668,220 BWK
Période en PoW	*nHeight* ≤ 345,600
Période en PoS	*nHeight* ≥ 345,601
Support de Protocol	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw rewards

3.2 Démarrage Lent

Notre démarrage équitable est assuré par l'extrait de code suivant (crédit *ZCash*) :

```
int64_t nSlowSubsidy = 50 * COIN;
```

```
if (nHeight < 960 / 2) {      // If block height less than 480,
    nSlowSubsidy /= 960;            // Set nSubsidy to .05208333
    nSlowSubsidy *= nHeight;  // Multiply present height by .05208333
} else if (nHeight < 960 {    // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;            // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave est utilisé par Bulwark dès le démarrage comme méthode de re-ciblage pour la difficulté du PoW. Il utilise une simple moyenne mobile qui peut répondre à de grandes hausses de nethash ou des chutes en seulement quelques blocks. Cela diminue « l'effet de block coincé » souvent causé par les multipools et empêche une personne ajoutant une quantité considérable de puissance de calcul de résoudre instantanément plus que quelques blocks.

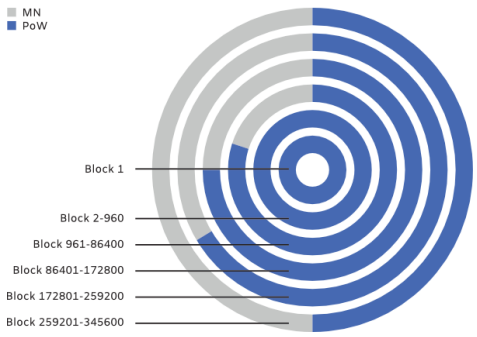
Chapitre 4

Récompenses de blocks

4.1 Récompenses de blocks PoW

Tableau: Spécifications des Récompenses de Blocks de la Phase de PoW

Subvention	Block	PoW	MN	Circulation
489720	1	100%	NA	489200
~25(moy.)	2-960	100%	NA	513150
50.000	961-28800	80%	20%	1953150
50.000	28801-57600	75%	25%	3393150
50.000	57601-86400	66%	33%	4833150
43.750	86401-172800	50%	50%	8613150
37.500	172801-2 59200	50%	50%	11853150
31.250	259201-345600	50%	50%	14553150



Graphique 4.1: Durée de Récompense de Block PoW

4.2 Récompenses de Block PoS

Tableau 4.2: Spécifications des Récompenses de Blocks de la Phase de PoS

Subvention	Block	Budget	PoS/Masternode	Note
25.000	345601-432000	10%	SeeSaw	Année 2
21.875	432001-518400	10%	SeeSaw	Année 2
18.750	518401-604800	10%	SeeSaw	Année 2
15.625	604801-691200	10%	SeeSaw	Année 2
10.250	691201-777600	10%	SeeSaw	Année 3
10.938	777601-864000	10%	SeeSaw	Année 3
9.3750	864001-950400	10%	SeeSaw	Année 3
7.8120	950401-1036800	10%	SeeSaw	Année 3
6.2500	1036801-1123200	10%	SeeSaw	Année 4
5.4690	1123201-1209600	10%	SeeSaw	Année 4
4.6880	1209601-1296000	10%	SeeSaw	Année 4
3.9060	1296000-1382400	10%	SeeSaw	Année 4
3.1250	1382401-1468800	10%	SeeSaw	Année 5
2.7340	1468801-1555200	10%	SeeSaw	Année 5
2.3440	1555201-1641600	10%	SeeSaw	Année 5
1.9530	1641601-1728000	10%	SeeSaw	Année 5
1.6250	1728000+	10%	SeeSaw	A perpétuité

Chapitre 5

Hashage NIST5

5.1 Pourquoi NIST5

Popularisé par Talkcoin en 2014, l'algorithme d'hashing NIST5 a eu un usage mainstream modeste. NIST5 peut être miné sur une vaste gamme d'hardwares grand public incluant les CPUs, ainsi que les GPUs d'AMD et NVidia. NIST5 n'est pas aussi résistant aux ASIC que d'autres algorithmes résistants à la mémoire, mais nous croyons que ce compromis est acceptable pour améliorer la stabilité du système et réduire la consommation d'énergie relative à ces algorithmes utilisant beaucoup de mémoire. Dans l'éventualité où des updates firmware ajouteraient le support des ASICs à NIST5 avant la fin de notre phase de PoW, nous sommes prêts à utiliser un autre algorithme en remplacement. Nous en appellerons au vote de la communauté sur le plan d'action (si tel est le cas) et l'implémenteront en conséquence. Nous sentons que notre courte phase de PoW et la volonté de changer d'algorithme dissuade les fabricants d'ASIC et ne prévoyons pas qu'un problème surgisse.

5.2 Les Cinq Finalistes (Compétition NIST SHA-3)

Les cinq algorithmes de hashage qui constituent NIST5 sont les finalistes de la compétition NIST (Chang et al. 2012). Ils sont (dans l'ordre dans lequel les blocks sont hashés) :

Blake (Aumasson 2013), **Grøstl** (Gauravaram1 et al. 2012), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), and **Skein** (Ferguson et al. 2010).

5.3 Le nouveau Standart SHA-3

Keccak a finalement réussi le round final pour être nommé en tant que nouvelle fonction SHA-3, tandis que les quatre autres algorithmes (malgré le fait d'être considérés cryptographiquement sécurisés) ont perdus plusieurs points de la part des juges pour quelques technicités mineures. Nous croyons que la combinaison du nouveau standard SHA-3 au côté des autres finalistes assure un algorithme de hashage rapide, sécurisé et établi.

5.4 Softwares de Minage Disponibles

Au moment d'écrire, il y a plusieurs options pour les mineurs :

Nom	Plateforme	Lien
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Chapitre 6

Fonctions intégrées

6.1 Masternodes

Les Masternodes sont, essentiellement, une toile décentralisée d'ordinateurs qui servent le réseau Bulwark. Ils servent l'écosystème Bulwark en stabilisant la masse monétaire, traitant les transactions, et en sécurisant le réseau. Les Masternodes requièrent 5000 BWK et des connaissances techniques modestes pour fonctionner. Tout wallet contrôlant 5000 BWK peut mettre en place un masternode.

6.2 Obfuscation / Mixage de Coins

Une des caractéristiques de Bulwark est l'Obfuscation, basée sur Coinjoin, mais avec plusieurs améliorations, et faite en mixant les coins de manière décentralisée, opération facilitée par le réseau de masternodes. Cela fournit une couche additionnelle de discrétion dans les transactions. Quoique pas parfaitement anonyme, l'Obfuscation via mixage par les nodes est de loin meilleure que la transaction Bitcoin standard. Par exemple, toutes les transactions Bitcoin sont transparentes. Pour Bulwark, un acteur néfaste aurait besoin de contrôler 50% des masternodes opérationnels pour avoir moins de 0.5% de chance de rendre non-anonyme une seule transaction qui aurait été mixée avec 8 rounds d'Obfuscation (Kiraly 2017b). Cette fonctionnalité importante fournit un haut niveau d'anonymat pour les utilisateurs de BWK qui choisissent d'obfusquer leurs transactions.

6.3 SwiftTX

SwiftTX fournit aux masternodes le verrouillage et l'autorité de consensus pour les transactions. Si ces masternodes atteignent un consensus sur la validité de la transaction, elle sera verrouillée pour une introduction ultérieure dans la blockchain (comme la durée de block de 10 minutes avec plusieurs confirmations pour Bitcoin). SwiftTX permet à plusieurs transactions d'avoir lieu avant qu'un block soit miné sur le réseau avec les mêmes données. Ce système est basé sur l'InstantSend de Dash (Kiraly 2017a).

6.4 Sporks

Le réseau Bulwark utilise le mécanisme de fork multi-phasé appelé "sporking". Cela permettra au réseau BWK d'implémenter de nouvelles fonctionnalités tout en réduisant les chances d'un fork du réseau involontaire lors du déploiement. Les changements Spork sont déployables via le réseau et peuvent être activés et désactivés si nécessaire sans exiger d'updates du software des nodes (strophy 2017). Cette fonctionnalité est extrêmement utile et permet au réseau de réagir rapidement aux failles de sécurité.

6.5 Masternodes TOR et IPV6

Bulwark permet à l'utilisateur de faire tourner son full node ou masternode depuis une adresse onion ou une adresse IPV6. Nous avons travaillé pour ajouter des nodes full TOR pour renforcer le réseau TOR lui-même, ainsi que l'expérience utilisateur en opérant en mode TOR seulement. Une fonctionnalité unique du support du masternode TOR est d'être capable d'opérer votre masternode en tant que service caché TOR. Les nodes TOR permettent aux utilisateurs avec une connexion internet stable d'opérer des masternodes depuis leur réseau domestique sans exposer de renseignements personnels pouvant révéler leur location, sans exposer leur réseau domestique à de potentielles attaques ou se compromettre.

6.6 De l'Importance de la Communauté et du système de Gouvernance

La communauté de bulwark est le facteur le plus important pour le succès du projet sur le long terme, et sa capacité à influencer de manière significative le futur de la coin est primordiale. Ainsi, à la fin de la phase de PoW nous prévoyons d'activer des superblocks de budget sur le réseau. Ces superblocks, payés mensuellement, permettront à la communauté d'exercer un contrôle significatif sur tous les aspects du développement, de la présence de la marque, et des affaires de la communauté de Bulwark. Délayer l'activation de ce système nous donnera le temps de développer le framework sous-jacent nécessaire pour une expérience utilisateur positive, et maximiser les récompenses de block disponibles pour les mineurs et les masternodes.

Nous utiliserons un processus en plusieurs phases pour créer et soumettre les propositions. Chaque étape devra être complétée entièrement. Un échec à compléter les étapes exposées résultera probablement en une proposition non activée. Voici une exposition de ces étapes ci-dessous :

- Commencez dans notre chat discord, et discutez avec nos utilisateurs chevronnés. Jaugez l'intérêt, et si la réponse est positive, passez à la phase suivante.
- Utilisez plusieurs plateformes de réseaux sociaux pour discuter et avoir du feedback. Rappelez-vous que Bulwark possède une base d'utilisateurs divers et plusieurs niveaux de participation de gouvernance, atteindre une portion de la base d'utilisateurs nécessitera plusieurs manœuvres. Prenez note de ces discussions et soyez capable de les citer dans une pré-proposition formelle. Le plus de citations, le mieux c'est.
- Soyez ouvert aux suggestions de la part de la communauté et des développeurs. Soyez flexible et disposé à incorporer des idées extérieures et des suggestions dans votre proposition.
- Créez une pré-proposition formelle sur la section Gouvernance->Pré-proposition de notre site. Fournissez des citations pour toutes les discussions qui ont eu lieu dans l'étape précédente. Traitez votre pré-proposition comme si elle allait être soumise à la blockchain pour un vote.
- Après avoir complété ces étapes, soumettez votre proposition à la blockchain. Soyez prêt à payer deux commissions, une au moment de la soumission et un frais de vote payé au développeur qui active votre proposition sur la blockchain. Les frais de soumission sont non-remboursables, et les frais de vote ne seront payés qu'au moment de l'autorisation et de l'activation de votre proposition.

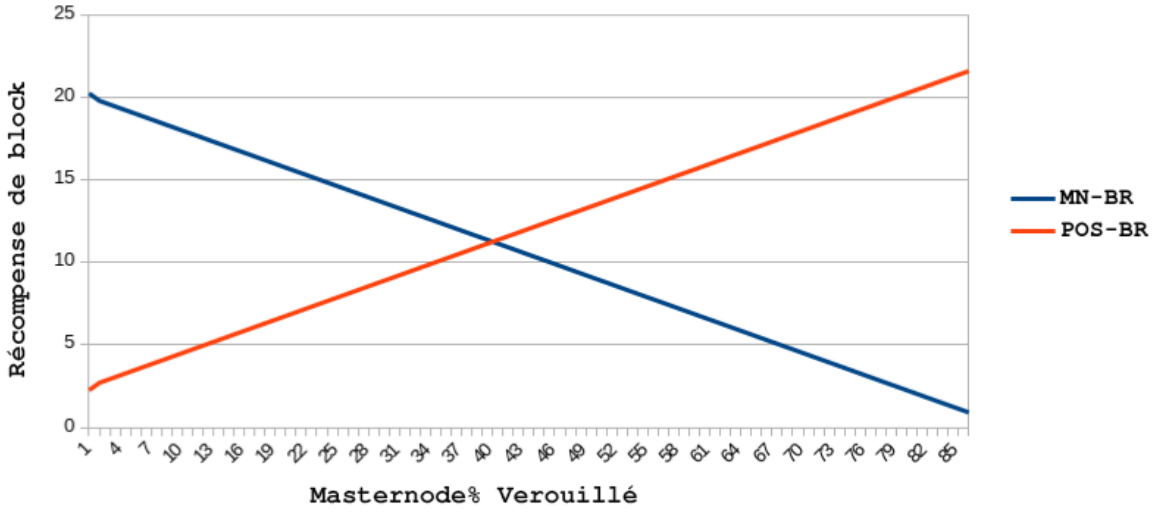
- Chacun est libre d'adapter sa proposition pour inclure le remboursement du coût de ces deux commissions. Veuillez-vous assurer que vous indiquez ajouter le remboursement des frais de traitement requis dans votre proposition officielle.
- Assurez-vous de reprendre contact avec toutes les personnes avec lesquelles vous avez discuté pour que votre idée soit votée. Pour qu'une proposition soit remboursée, 10% des masternodes éligibles doivent voter "oui" en faveur de cette proposition. Ce processus pour obtenir un consensus de 10% peut être plus difficile que cela en a l'air, soyez diligent, informatif, et respectueux pour obtenir les votes nécessaires pour que votre proposition soit payée.

6.7 PoS SeeSaw/Récompenses de Masternode

Nous avons décidé d'utiliser le système de récompense SeeSaw popularisé par PIVX (jakiman 2017). Le système de récompense SeeSaw commence avec un ratio par block de 9:1 (favorisant les masternodes), et ajuste homogènement le ratio de récompense entre le staking et les opérateurs de node jusqu'à ce que 41.5% des coins en circulation soit verrouillées dans les masternodes, moment auquel les récompenses de staking obtiennent un avantage léger sur les récompenses de masternode. La raison pour laquelle le SeeSaw favorise légèrement les récompenses de staking est que nous voulons éviter les problèmes – comme une importante volatilité du prix ou une faible liquidité – qui impactent les coins avec un très haut pourcentage de leur masse monétaire verrouillée dans les nodes. Cette stratégie atténuera la frustration de l'utilisateur par rapport à l'accès à la réserve de coins et maintiendra la pertinence de notre robuste réseau. Un de nos objectifs étant d'être une plateforme privilégiée pour le commerce anonyme, la transactabilité est de la plus haute importance pour ceux acceptant Bulwark et ceux holdant Bulwark.

Graph 3. SeeSaw @ Hauteur 345601 – 432000

(après pourcentage du budget)



Chapitre 7

Le Futur

7.1 La Boîte à Outils de Bulwark

Une collection d'extraits de code, d'APIs, de scripts, et de connaissances qui serviront à encourager un environnement de bazaar où les développeurs qui rechercheraient l'ajout du support de cryptomonnaie dans leurs projets seraient libre d'échanger des connaissances, des informations, et du code. Nous croyons que fournir aux développeur ces outils équivaut à fournir à un menuisier les outils dont il a besoin pour créer d'excitants et remarquables projets.

7.2 Vie Privée et Améliorations du Software

Nous sommes déterminés à adopter de nouveaux protocoles qui amélioreront la privacité de notre base d'utilisateurs. Il y a plusieurs voies que nous évaluons au moment présent et que nous planifions de commencer à tester en interne et développer dans la première moitié de 2018. Quelques-unes de ces améliorations incluent :

- Réseau de privacité I2P.
- Protocole Zerocoin ou adressage Stealth (quand nous seront confiants en la maturité de la solution).
- Synchroniser notre codebase plus près des grandes lignes de Bitcoin.
- Modernisation/Mise à jour du QT Wallet.
- Intégration Libtox.
- Virtualisation/conteneurisation de la wallet Bulwark pour ajouter une couche de sécurité supplémentaire.

7.3 Node Sécurisé Bulwark Domestique

Nous travaillerons avec des spécialistes CAD pour concevoir un node domestique Bulwark, petit et autonome. Les utilisateurs pourront se connecter à leur réseau domestique et le configurer en utilisant une Web UI. Les fonctionnalités que nous prévoyons de lancer sont les suivantes :

- Pour ceux ayant une connexion internet stable, un onionized masternode (ou full node) facile à installer utilisant les services de dissimulation de TOR.
- La possibilité de fonctionner comme un relais pour améliorer le réseau TOR global.
- UN VPN et/ou proxy qui peut être utilisé pour router le trafic domestique à travers le réseau TOR/I2P.
- Le staking de Bulwark à travers la virtualisation ou un service d'add-on.

En accord avec l'esprit de la décentralisation, les fichiers d'impression 3D et toute le code source seront disponibles pour la communauté pour un assemblage maison.

7.4 Extension de notre Image de Marque

Nous continuerons d'étendre notre marque et prévoyons de travailler avec des vendeurs d'hardware et des intégrateurs de système qui partagent la même passion et les idéaux que nous avons. Nous voulons, que dans cinq ans, le nom 'Bulwark' soit synonyme non seulement de cryptomonnaie mais aussi de privacité, sécurité, et de respect de la liberté des utilisateurs. L'objectif principal de Bulwark est de fournir la liberté de choix à travers la privacité.

7.5 Design et Visuel

Par la Recherche et le Développement, nous aspirons à créer un langage de design visuel pour Bulwark qui le différencie de sa compétition dans le marché des cryptos. Notre équipe de design planifie d'innover et d'expérimenter avec les UI/UX/Branding actuels pour réaliser un design d'excellence en recherchant un medium qui permette la meilleure expérience utilisateur, et une esthétique belle et innovative. Cela sera fait en étudiant notre compétition, en restant au top des tendances et standards technologiques actuels et en aspirant continuellement à apporter des visuels nouveaux et excitants pour les utilisateurs finaux.

Chapitre 8

Conclusion

8.1 Résumé

Bulwark est une coin orienté vers la privacité avec des masternodes, une gouvernance, et un écosystème évolutif d'outils. Le projet a commencé avec un lancement équitable et un focus sur une large distribution des coins. Le démarrage lent, le partage des récompenses de block, et l'algorithme de hashing ont été délibérément sélectionnés pour créer une participation significative de la communauté. Bulwark a été lance avec une importante variété de fonctionnalités de privacité et l'équipe de développement travaille dur pour introduire de nouvelles fonctionnalités et construire par-dessus les technologies existantes. Bulwark a pour but de promouvoir le choix à travers la privacité et concentrera d'importants efforts pour arriver à cette fin.

8.2 Travail futur

L'écosystème des coins de privacité à masternodes a récemment été inondé par des coins cherchant à attirer de nouveaux utilisateurs à travers des promesses d'importants retours d'investissement, des feuilles de route gigantesques remplies de produits improbables, et un focus sur le marketing plutôt que de réelles améliorations dans ce domaine. Bulwark a pour but d'être l'opposé : faible sur la création de hype et fort sur une vraie création. Les objectifs présents et futurs pour le projet vont suivre la formule suivante : spécifique, mesurable, réalisable, pertinent et limité dans le temps.

Références

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Disponible sur : https://131002. net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Disponible sur : https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Disponible sur : https://bitcoin.org/en/ developer-reference#block-headers.

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Disponible sur : http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Disponible sur : http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Disponible sur : http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Disponible sur : http://www.groestl.info/Groestl.pdf.

jakiman, 2017. PIVX purple paper. Disponible sur : https://pivx.org/wp-content/uploads/2017/03/ PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Disponible sur : https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Disponible sur : https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Disponible sur : https://bitcoin.org/ bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Disponible sur : https://lopp.net/pdf/Bitcoin_ Developer_Reference.pdf.

strophy, 2017. Understanding sporks. Disponible sur: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Dash instamine issue clari cation Disponible sur : https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. The hash function jh. Disponible sur : http://www3.ntu.edu.sg/home/wuhj/research/jh/ jh_round3.pdf.