[**WHITE PAPER**]
VERSION FRANÇAISE

Bitcore BTX

The future is NOW!

Bitcore BTX

Une Solution de Paiement Authentique et Communautaire

ÊTES-VOUS PRÊTS POUR LE FUTUR ?

Ecrit par
Christina

Illustré par
DgCarlosLeon

Traduit par
Bireuc from Bitcorion

Prenez contact avec l'équipe fondatrice du Bitcore :

JON, STEVE et CHRIS

info@bitcore.cc | www.bitcore.cc

Sommaire

1 Bitcore - Une solution de paiement authentique et communautaire

Bitcore est une cryptomonnaie ayant comme objectif final d'assurer la pérennité de la vision originelle du Bitcoin.

Bitcore a choisi de conserver les avantages centraux du Bitcoin – Bien que l'équipe fondatrice du Bitcore souhaite rendre la technologie originelle du Bitcoin plus audacieuse pour le futur. Bitcore est à l'origine un *hybrid fork* du Bitcoin se caractérisant par un mécanisme de consensus par preuve de travail, et implémente tous les BIPs (*Bitcoin Improvement Proposals*) du protocole Bitcoin.

Du fait de sa structure particulière et une communauté active, Bitcore est plus agile que d'autres cryptomonnaies pour implémenter des innovations incontournables. Ainsi, la blockchain Bitcore a intégré et activé le SegWit (*Segregated Witness*) quatre mois et demi avant la blockchain Bitcoin, la rendant **compatible au *Lightning Network*.**

Plus important, **Bitcore met en œuvre une véritable décentralisation et une émancipation des utilisateurs du protocole :**

- L'algorithme de minage **résistant aux ASICs** renoue avec une participation communautaire et s'oppose aux phénomènes de centralisation dans le minage,
- L'application des filtres de Bloom [i] réduit significativement les espaces de stockage requis pour activer **un nœud complet à la blockchain Bitcore** et permettant ainsi à plus de personnes de contribuer à la blockchain Bitcore en complète autonomie grâce à des portefeuilles SPV/light,
- Le processus d'*airdrop* innovateur a permis **une répartition nettement plus équitable des pièces Bitcore (BTX)** encourageant ainsi l'utilisation du Bitcore comme une solution de paiement. La décision de la communauté Bitcore de renoncer à une *Initial Coin Offering* (ICO) laissa à quai toutes tentatives de spéculations,
- Bitcore est plus rapide que le Bitcoin, plus rapide que PayPal, devenant ainsi **une véritable option de paiement quotidienne** renforcée par l'implémentation du SegWit et d'autres solutions. Avec le *Lightning Network*, un nombre théoriquement illimité de transactions hors-ligne peut être supporté. Les **faibles taxes** du Bitcore avoisinant les 0,0003$ dollars américains (USD) par transaction rendent le protocole Bitcore d'autant plus acceptable pour des utilisations quotidiennes de paiements et de micropaiements,
- Bitcore est **un projet *open source*** : Produit en collaboration, partagé gratuitement, publié avec transparence, et développé pour être un bien communautaire plus que la propriété ou le business d'une seule entreprise ou d'une seule personne [ii].

"Bitcore : Le fork du Bitcoin le plus ingénieux"

-- Jimmy Song[iii], Developpeur appartenant au Bitcoin Core

En résumé:

Bitcore est **la solution de paiement numérique authentique, communautaire et en pair-à-pair** adaptée aux besoins de demain. Si Satoshi Nakamoto eut en 2008 l'expérience acquise de ces dix dernières années vécues par la communauté des cryptomonnaies, Bitcore serait ce que le Bitcoin[iv] fut en ses débuts. Bitcore offre à tous l'opportunité de faire partie de la vision originelle de Satoshi, limpide et non souillée de tous développements économiques fallacieux du passé.

2 Du Bitcoin au Bitcore

> *"Un système de monnaie électronique entièrement en pair-à-pair permettrait d'effectuer des paiements en ligne directement d'un tiers à un autre sans passer par une institution financière. Les signatures digitales fournissent une telle solution, mais perdent ses avantages si un tiers de confiance reste nécessaire pour éviter le double paiement. Nous proposons une solution au problème du double paiement en faisant appel à un réseau pair-à-pair."*
>
> -- Satoshi Nakamoto, 2008

Cette annonce donna naissance au concept moderne de la cryptomonnaie et, de surcroît, de la finance décentralisée. Au moment où Satoshi Nakamoto a défini le concept originel du Bitcoin, la majeure partie du monde financier se trouvait relier à des autorités centrales ou plus précisément : **à des points de rupture centralisés**. La sécurité de l'argent de chacun était secondaire face à la sécurité et à la santé économique des banques et des institutions financières possédant les fonds.

Chaque cas de failles de sécurité, d'erreurs de conduite ou de banqueroute dans le monde financier montre que ceux qui font confiance en ces institutions pour protéger leur épargne pourraient potentiellement, un jour, être délaissés sans apports suffisants.

Sans avoir besoin d'inventer une technologie encore inexistante, Satoshi Nakamoto a combiné des paradigmes existants sous une nouvelle forme pour résoudre ce problème : Un registre distribué et sécurisé par preuve de travail qui fournirait un cadre de travail dans lequel les participants seraient forcément honnêtes et ne feraient pas appel – et donc éviterait des manipulations potentielles – à des autorités centrales.

Le processus incitatif appelé minage était et est donc une fonction vitale à ce système. Un ensemble de lois permettent au système **d'opérer de façon autonome** et durable sans passer par des décisionneurs

ou une quelconque entité. Le but étant de maintenir le principe de la décentralisation : En effet, si une entreprise devait s'assurer en partie du bon fonctionnement du système, cette entité représenterait un risque potentiel de faille – ce qui anéantirait le but même du protocole.

Dans ce livre blanc, nous allons mettre en évidence les caractéristiques du protocole Bitcoin d'origine et comprendre comment Bitcore les a préservées voire améliorées et perfectionnées.

Cela permettra ainsi de montrer pourquoi et comment le protocole Bitcore est une **cryptomonnaie alternative puissante** qui facilitera la mise en application de certains cas d'usage qui ne peuvent être réalisables avec les solutions technologiques de cryptomonnaie existantes.

2.1 Bitcore : une solution open source

Le projet Bitcore, comme Bitcoin, est avant tout une initiative communautaire et dont le **code source est en libre accès**. La communauté du Bitcore a souhaité conserver cette démarche puisqu'elle correspond à l'esprit décentralisé, participatif et communautaire du protocole.

De plus, le développement du Bitcore n'a été rendu possible que parce que le protocole Bitcoin respecte les nombreuses caractéristiques stipulées par l'*Open Source Initiative*[v]. Par conséquent, le code source du Bitcore s'y soumet aussi avec les mêmes degrés de liberté qui sont :

1. Une distribution gratuite.

2. L'inclusion dans le programme du code source.

3. L'autorisation de modifications, d'œuvres dérivés et de leur distribution.

4. L'intégrité du code source de l'auteur.

5. Aucune discrimination envers une personne ou un groupe de personnes.

6. Aucune discrimination envers les domaines d'application.

7. L'utilisation de la licence sans dépendance à une autre licence.

8. La licence ne doit pas être spécifique à un produit.

9. La licence ne doit pas restreindre d'autres logiciels.

10. La neutralité technologique de la licence.

En adhérant à ces principes et standards pour les logiciels open source, le projet Bitcore autorise la communauté à accéder, modifier et même développer son code sans discrimination concernant l'identité, l'historique, l'intention de la personne physique ou morale, ou l'industrialisation du protocole.

2.2 Distribution : Processus de réclamation 1 pour 1, Hybrid Fork et Airdrop

Les *forks* classiques du Bitcoin consiste à copier la blockchain à un temps/bloc donné et de dériver sur sa propre branche. Bitcore a agi différemment en créant une nouvelle monnaie à partir d'une blockchain vide afin de séparer explicitement le Bitcore du Bitcoin afin d'être une entité unique.

16.2 millions de Bitcore (BTX) ont été « pré-minés » (équivalent au nombre de BTC au moment de la création de la blockchain Bitcore) et furent prêts pour une distribution à l'ensemble de la communauté des cryptomonnaies.

La redistribution des BTX à la communauté et futures utilisateurs potentiels s'est faite en trois étapes :

- Réclamation de pièce 1 pour 1
- Hybrid fork
- Airdrop

2.2.1 Réclamation de pièce 1 pour 1

Durant les six premiers mois de l'existence de Bitcore, du 24 Avril au 2 Novembre 2017, les utilisateurs du protocole Bitcoin pouvaient réclamer la quantité de BTC en BTX selon un ratio 1 pour 1.

Cet échange s'est appuyé sur une base de données et la fonction de signature numérique du Bitcoin [vi].

Des 16,2 millions de BTX issus du *fork*, 590 000 furent réclamés durant cette première étape de distribution. L'opportunité de faire cet échange prit fin le 2 Novembre 2017.

2.2.2 Hybrid fork

Au bloc n°492 820 du protocole Bitcoin, émis le 2 Novembre 2017, une image (*snapshot*) de la blockchain a été réalisée. Les 15,8 millions de BTX restants furent alors redistribués différemment de la réclamation 1 pour 1.

Toutes les adresses de la blockchain Bitcore correspondant à des adresses de la blockchain Bitcoin et contenant au moins 0.01 BTC ont alors reçu une quantité de BTX équivalent à 50% de leur fond en BTC. En d'autres termes, le ratio d'échange était (et est) de 0.5 BTX pour 1 BTC pour toutes les adresses du Bitcoin contenant au moins 0.01 BTC.

Dans les jours qui ont suivi, approximativement 5 millions de transactions ont été effectuées, et environ 8 millions de BTX furent répartis entre les adresses éligibles. Ce ne fut pas uniquement un moyen de distribuer des BTX, mais a servi aussi à démontrer que la blockchain BTX est capable de gérer un grand nombre de transactions sur une période relativement courte.

Ainsi, environ 8 millions des 16 millions de BTX existants furent distribués à la communauté. Sur les 8 millions restants, 10% ont été conservés par l'équipe Bitcore pour les développements techniques futurs et la promotion du protocole Bitcore.

2.2.3 Airdrop

90% des 8 millions de BTX restants furent finalement distribués à travers des *airdrops* hebdomadaires selon une planification différentielle.

Lors du *airdrop* initial, un bonus de 25% pour les utilisateurs de Bitcore fut accordé selon les montants de leur portefeuille en BTX. Puis, les *airdrops* suivants ont été effectués la planification suivante (en pourcentage du portefeuille des utilisateurs) :

+5% tous les lundis en Janvier 2018

+6% tous les lundis en Février 2018

+7% tous les lundis en Mars 2018

+8% tous les lundis en Avril 2018

+9% tous les lundis en Mai 2018

Cette dernière étape a permis de finaliser la redistribution des BTX jusqu'en Mai 2018.

2.2.4 Exemple de Airdrop

L'exemple suivant permettra de comprendre le processus de *airdrop* :

Alice a 20 Bitcore (BTX) dans son portefeuille. Elle a enregistré son portefeuille pour le *airdrop* de janvier, lorsque le bonus était de 5%. Elle est donc éligible de recevoir 5% de son portefeuille durant les *airdrops* de janvier :

20 BTX * 5% = 1 BTX

Ainsi, Alice reçoit 1 BTX supplémentaire et son portefeuille contient maintenant 21 BTX. Le *airdrop* de la semaine suivante calculera son bonus selon les BTX restants sur le portefeuille.

2.2.5 Pourquoi un *hybrid fork* et un *airdrop* ?

La différence cruciale entre ce modèle de distribution et d'autres modèles basés sur le classique *hard fork* est que : Au lieu de distribuer les pièces en équivalence aux détenteurs d'adresses Bitcoin au moment de l'image de la blockchain, uniquement 50% des BTX furent reversés de cette manière. Les 50% autres BTX ont put alors être distribués aux membres actifs du protocole. De cette façon, l'équipe Bitcore s'est assurée que les « baleines » possédant un nombre conséquent de Bitcoin ne puissent devenir des « baleines » en BTX et par conséquent, cela a permis d'éviter de biaiser la force d'action communautaire du Bitcore et de se retrouver avec une quantité de BTX en circulation assez limitée ce qui pouvait compromettre les futures opérations de l'écosystème. De ce fait, l'équipe Bitcore a réussi à offrir une **meilleure distribution des pièces** que d'autres *forks* du Bitcoin, en accord avec les idéaux d'une décentralisation participative de la communauté Bitcore.

2.3 Pas de ICO

Du fait de son approche *hybrid fork*, le lancement de Bitcore n'a pas été imaginé comme ou financer par une *initial coin offering* (ICO).

Cela fut volontairement choisi par la communauté Bitcore afin de prôner l'égalité des chances et favoriser la participation de potentiels utilisateurs du protocole à travers le monde. Comme les dernières tendances et investissements de la crypto-sphère l'ont montré, les ICOs attirent les spéculateurs, ce qui engendre une augmentation de la volatilité de la cryptomonnaie en question et diminue son utilité première. De plus, les ICOs mènent à un afflux d'investisseurs privés très riches qui s'octroient des pouvoirs disproportionnés et influencent les communautés des cryptomonnaies. Dernière chose et non des moindres, différents cadres de régulation des ICOs peuvent s'appliquer aux équipes localisées dans plusieurs pays, et certains cadres empêchent même des citoyen issus de certains pays à participer aux ICOs.

Ces limitations arbitraires ont paru inacceptable aux yeux de la communauté Bitcore. Nous nous efforçons de créer un crypto-écosystème qui soit accessible pour tous et par tous.

Dans le but d'être indépendant de toutes régulations possibles, nous avons choisi d'opérer comme consortium d'individus intéressés à but non lucratif. Les membres de l'équipe fondatrice et la participation de la communauté Bitcore est donc purement dépendant de l'expertise, de l'intérêt et des initiatives de chacun, et non de frontières géographiques arbitraires.

3 Solution et spécification technique

Bitcore regroupe un ensemble d'innovations clés rendant le protocole particulièrement adapté pour devenir un moyen de paiement du quotidien pour le monde civil et des affaires. Chaque innovation, ainsi que leur rôle dans l'efficacité augmenté et l'utilité avancé du protocole Bitcore, va être détaillée dans cette section.

Brièvement, les spécifications techniques majeures du Bitcore sont résumées ci-dessous :

Nombre **Bitcore**

Symbole **BTX**

- Lancé le 24 Avril 2017
- Réserve maximum de 21 millions de pièces
- Bloc de taille 10 Mo (20 Mo en SegWit)
- Temps de validation des blocs moyen de 2,5 min
- Taille de la blockchain 1 Go (Septembre 2018)
- Algorithme Timetravel10 pour le minage
- Fonctionnalités SegWit et Bloom actives
- Algorithme « Smooth diff64_15 » pour l'ajustement de la difficulté de minage

- Distribution équitable : Réclamation BTC et *airdrops*

"[Bitcore] innove en rendant les choses claires."

-- Jimmy Song[vii], Developpeur de Bitcoin Core

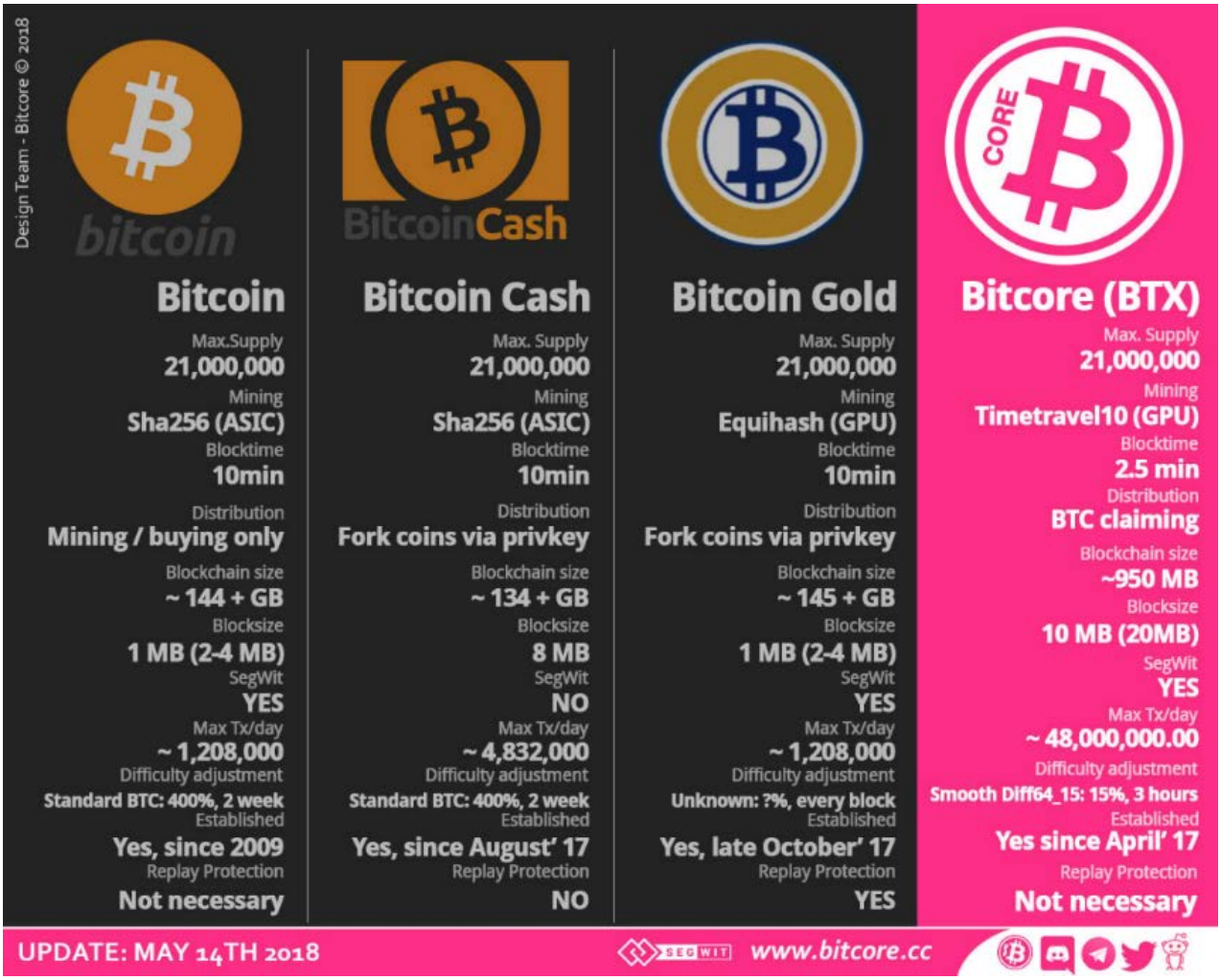

Figure 1: Bitcoin, Bitcoin Cash, Bitcoin Gold et Bitcore – Graphique comporatif

3.1 Réserve de pièces

La protocole Bitcore produira un nombre de pièces défini à 21 millions. Ce choix est délibéré dans le but de correspondre à la réserve finale et totale du protocole Bitcoin.

Cette limite de pièces résulte de l'algorithme de division des récompenses pour les mineurs de Bitcoin qui consiste à diviser par deux, tous les 210 000 blocs, la récompense pour la validation d'un bloc, réduisant tous les quatre ans le nombre de pièces nouvellement miné jusqu'à atteindre une valeur très proche de zéro en 2140.

La récompense à la validation des blocs dans le protocole Bitcore fut identique à Bitcoin pour les 10 000 premiers blocs : 12,5 BTX par bloc avec un temps de validation de 10 minutes. Puis, une mise à jour modifia la récompense à 3,125 BTX par bloc avec un temps de validation de 2,5 minutes.

Bitcore applique le même schéma de division des récompenses, mais tous les 840 000 blocs. Ainsi, la réserve totale et finale du Bitcore sera équivalent à celle du Bitcoin.

Le graphique ci-dessous montre la division par deux de la récompense :

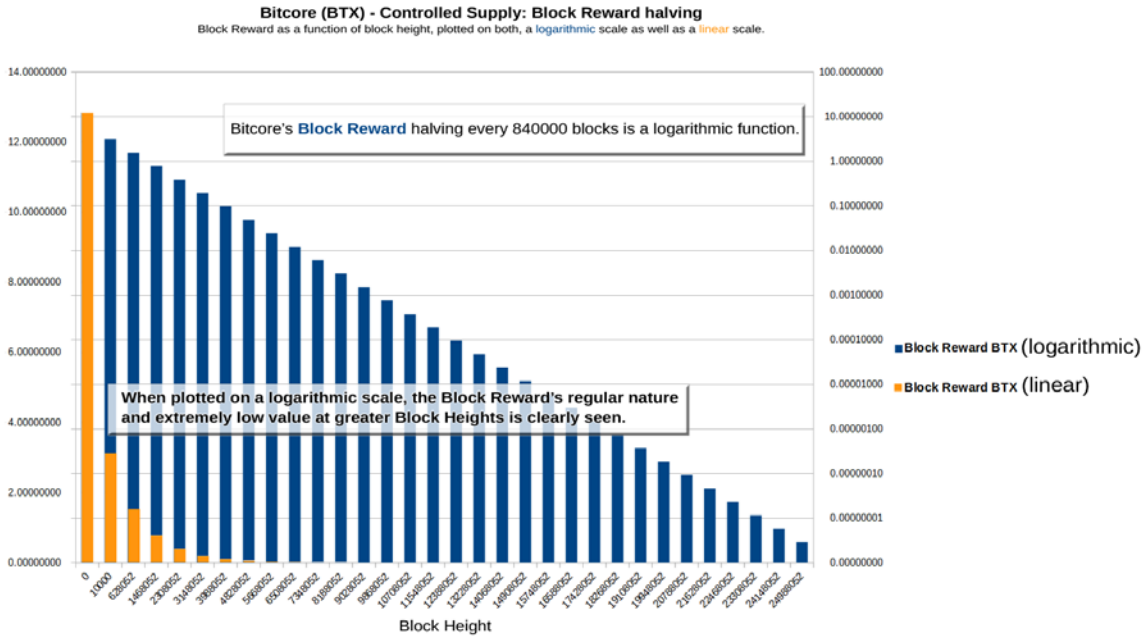

Figura 2: Recompensa de bloque disminuyendo a la mitad en el tiempo.

Pour rappel, cette division des récompenses a pour but de connaître le nombre de pièces totales circulant sur le protocole, un concept nommé la réserve monétaire contrôlée.

3.2 La blockchain et les algorithmes

Comme le Bitcoin, le Bitcore est basé sur la preuve de travail. Cependant, une innovation a été apportée grâce à l'algorithme d'ajustement de la difficulté, le *Core Shield 64_15* qui est décrit plus loin dans la section.

Une autre différence cruciale qui sera décrite dans cette section est la conséquence de la réduction du temps de confirmation des blocs par rapport au protocole Bitcoin rendant Bitcore plus usuel et sécurisé. En parallèle, la taille des blocs a été significativement augmentée contribuant encore à augmenter la vitesse et le nombre de transactions, et à rendre plus applicable le protocole.

Finalement, l'activation du SegWit – 4 mois et demi en avance par rapport à la blockchain Bitcoin – et la compatibilité au *Lightning Network* permet au protocole Bitcore de devenir un moyen de paiement idéal pour les besoins des personnes et des entreprises de demain.

3.2.1 Ajustement de la difficulté de minage avec le *Core Shield 64_15*

Dans les cryptomonnaies basées sur la preuve de travail, l'ajustement de la difficulté – difficulté avec laquelle les mineurs doivent valider/trouver le prochain bloc – a pour but d'assurer une cohérence dans le temps de validation d'un bloc. Sans cela, le temps de valider un bloc se verrait diminuer par l'augmentation du nombre de mineurs actifs sur la blockchain et augmenterait le risque que la valeur correcte de hachage soit découverte par aucune personne parmi ce grand nombre de mineurs.

Ainsi, dans l'ajustement de la difficulté, le niveau de difficulté pour découvrir un nouveau bloc augmente lorsque beaucoup de mineurs sont présents sur le protocole, et diminue lorsque le nombre de mineurs actifs est moindre.

Sur le protocole Bitcoin, le niveau de difficulté est ajusté tous les 2016 blocs. Avec une moyenne de validation des blocs de 10 minutes, cela revient à un ajustement toutes les deux semaines – un taux plutôt léthargique qui ne peut répondre à une augmentation ou diminution de l'activité des mineurs sur un court terme. Et malheureusement, ce type de fluctuation de court terme est fréquemment observé lorsque les mineurs naviguent entre le Bitcoin et ses *forks* afin de trouver le meilleur ratio entre la difficulté de minage et les récompenses associées.

Pour répondre à ce défi, Bitcore a remplacé la méthode d'ajustement de la difficulté du Bitcoin par un algorithme innovant, le ***Core Shield 64_15***.

Dans le *Core Shield 64_15*, la difficulté est réajustée tous les 64 blocs. Avec un temps de validation des blocs du Bitcore moyen à 2,5 minutes, l'ajustement de la difficulté s'effectue toutes les 2 heures et 40 minutes. La difficulté des blocs dans le protocole Bitcore devient plus réactive que celle du Bitcoin, mais les ajustements court terme extrêmement brusques peuvent survenir : La difficulté ne sera donc pas changée de plus de 15% par rapport à la précédente, ce qui permet d'avoir des ajustements graduels plutôt que drastiques.

L'algorithme d'ajustement de la difficulté du protocole Bitcore n'est donc pas uniquement plus efficace, mais rend le temps de validation d'un nouveau bloc plus prédictible et augmente la sécurité du réseau contre des attaques du type double paiements qui réussissent avec une plus forte probabilité sur les périodes de difficulté de hachage disproportionnellement bas.

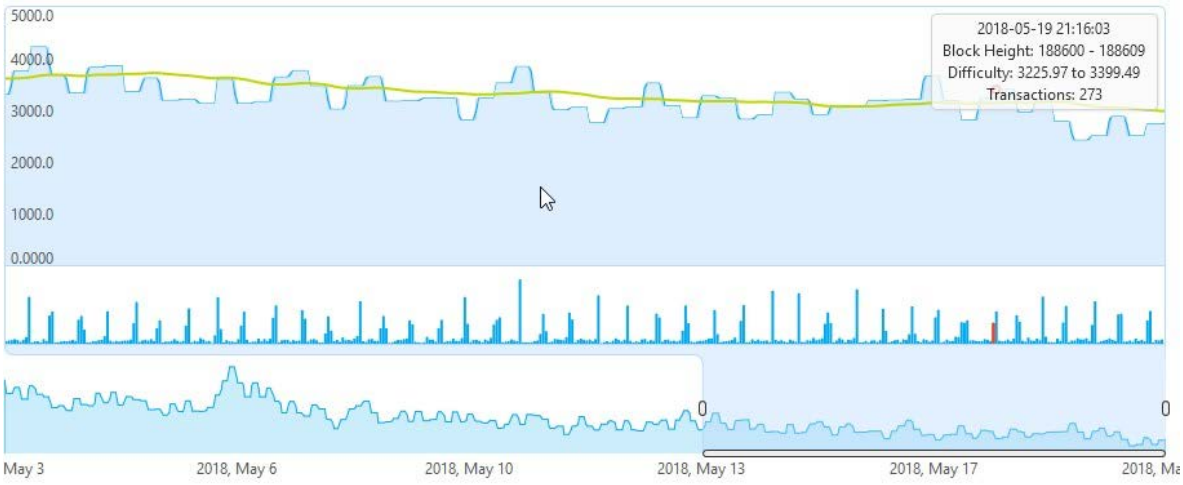

Figura 3: Reorientación de Dificultad en Bitcore (datos de mayo 2018).

3.2.2 Un temps de validation des blocs plus court

Le protocole Bitcore est conçu pour livrer un nouveau bloc toutes les 2,5 minutes – soit un quart des 10 minutes pour valider un bloc sur le Bitcoin.

Le temps de validation des blocs plus court est avantageux pour diverses raisons.

La première raison est que cela permet de **plus rapides confirmations**. Chaque transaction sur la blockchain est en premier lieu vu comme non-confirmée, et qui peut être pris par les mineurs en compétition pour créer le prochain bloc. Chaque fois qu'un bloc est validé sur la blockchain, les transactions contenus dans ce dernier sont dites confirmées.

Comme plusieurs blocs concurrents avec différentes transactions valides peuvent exister sur la blockchain, seule la création des blocs futures suivant le bloc courant prouve qu'une transaction appartient vraiment à la chaine active, c'est-à-dire, la plus longue chaîne existante. Cette politique fait partie du mécanisme de consensus de la preuve de travail pour empêcher les attaques double paiements par des nœuds malicieux : Or, la quantité de travail (et donc d'énergie) pour créer un unique bloc avec une transaction frauduleuse peut encore être faisable pour un attaquant. Cependant, cette transaction frauduleuse ne fera pas partie de la blockchain active sur le long terme à moins que l'attaquant puisse dépenser suffisamment d'efforts pour créer un nombre significatif de blocs dans le but que sa chaîne devienne la plus longue : Une attaque des 51%.

Pour cette raison, beaucoup de commerçants et autres entités acceptant les crypto-paiements attendront la validation de plus d'un bloc pour accepter une transaction comme confirmée. En général, les paiements comportant de forts montants ont un fort risque d'être falsifiés, et cela requière donc un temps de confirmation plus long afin d'assurer la sécurité du commerçant.

Pour rappel, le temps de validation des blocs sur 10 minutes a été originellement choisi par Satoshi Nakamoto pour sécuriser le réseau Bitcoin à son échelle… il y a dix ans. Depuis, le réseau s'est considérablement agrandi, rendant plus difficile d'y soumettre des transactions frauduleuses, ce qui n'est pas vrai pour les plus petits réseaux.

Finalement, Vitalik Buterin, fondateur de l'Ethereum, affirme que le temps de validation des blocs plus court est préférable parce qu'ils fournissent une plus grande granularité d'informations[viii]. Les chaînes actives correctes seront plus rapidement détectées et préférées aux chaînes incorrectes, et un niveau de sécurité acceptable pour la petite et moyenne transaction serait atteint plus tôt. Cependant, la réduction du temps de validation augmente le risque de centralisation des blockchains basées sur la preuve de travail, donnant aux gros acteurs plus de pouvoirs pour trafiquer le réseau. Ainsi, le temps de validation ne peut être arbitraire réduit, mais doit être prudemment conçu en gardant en mémoire ces tendances conflictuels.

Dans la lumière de ces considérations, Bitcore a décidé de bénéficier pleinement du privilège et des bénéfices fournis par une modeste réduction du temps de validation des blocs à 2,5 minutes où le *Core Shield 64_15* et la réduction du temps de validation permettent donc de diminuer le risque d'attaque 51%.

3.2.3 Taille de Bloc plus large

Les blocs du Bitcore ont une taille de 10 Mo, sans prendre en compte les contenus complémentaires qui viennent avec la « repondération » des données grâce au SegWit, ce qui augmente la capacité à 20 Mo. Le Bitcore peut donc fournir 80 Mo de blocs (40 Mo sans le SegWit) dans le même intervalle de temps que le Bitcoin qui lui peut fournir 2 Mo (1Mo sans le SegWit).

Des blocs plus larges peuvent contenir plus de transactions qui, à un temps de validation des blocs donné, équivaut à un débit de transactions plus important. Le débit de transactions a toujours été un point critique concernant la capacité des cryptomonnaies à concurrencer les solutions de paiements fiduciaires : VISA peut effectuer 1700 transactions par seconde (TPS), et PayPal 115 TPS au moins.

Avec le SegWit, le Bitcoin peut atteindre 11 TPS, bien que des pics à 20 TPS ont été effectués pendant de courtes périodes.

Dans le but de permettre une adoption répandue des méthodes de paiements par cryptomonnaies, l'évolutivité des réseaux doit être améliorée et le débit de transactions augmenté. Deux solutions sont habituellement proposées : L'augmentation de la taille des blocs et l'introduction de solution d'évolutivité hors chaine telle que le *Lightning Network*.

Sachant qu'une transaction occupe 224 octets et que la communauté Bitcore a choisi d'augmenter la taille des blocs à 10 Mo, cela donne un débit de 310 transactions par seconde. Avec le SegWit, la capacité maximum des blocs peut aller jusque 20 Mo ce qui donne une capacité de traitement d'environ

550 transactions par seconde dans des conditions optimales, et sans compter le fait que des transactions supplémentaires puissent se faire hors chaine via le *Lightning Network*.

Bitcore a déjà prouvé son efficacité en supportant un grand nombre de transactions lorsqu'approximativement 5 millions de transactions furent traiter en quelques jours pour l'activation du *hybrid fork* le 2 Novembre 2017. (Voir section 2.2)

3.2.4 Activation du *Segregated Witness* (SegWit)

La couche Segregated Witness (SegWit) a été active sur la blockchain Bitcore en Avril 2017 au bloc n°3000 - quasi une demi année avant le Bitcoin. Avant l'activation, des mineurs Timetravel10 du Bitcore avaient réussi avec succès la création de blocs conformes au SegWit prouvant sa possible intégration.

SegWit fournit plusieurs avantages immédiats :

- L'élimination de la malléabilité involontaire des transactions,
- L'augmentation du volume de transactions,
- La pondération des données selon son effet sur la performance d'un nœud,
- Le camouflage par signature des valeurs,
- L'évolutivité linéaire des opérations dites *sighash*,
- L'augmentation de la sécurité pour le *multisig*,
- La sécurité renforcée sur presque tous les nœuds et
- Le contrôle des versions de script.

3.2.5 Compatibilité au *Lightning Network*

Le Lighting Network[ix] est un réseau de transfert opérant sur une couche supérieure à la blockchain Bitcore. En utilisant la fonctionnalité des contrats intelligents, cela autorise des paiements instantanés au sein d'un réseau de participants, obviant à une attente de confirmation comme décrit dans les précédentes sections du livre blanc.

En complément à ces paiements instantanés, le *Lightning Network* confère d'autres avantages :

- L'évolutivité augmentée comme effet secondaire aux paiements instantanés,
- La taxation réduite facilitant ainsi les micropaiements à travers cette solution,
- *L'atomic swaps* entre chaînes en hors chaîne rendu possible avec des règles de consensus hétérogènes sur la blockchain.

Bitcore est aujourd'hui totalement compatible avec le *Lightning Network* et est donc capable de réaliser des paiements instantanés ainsi que des micropaiements.

3.2.6 Taxation faible

Avec une taxe moyenne de 0,0003 USD par kilooctet et une médiane de 0.0002 USD par kilooctet, les taxes du Bitcore sont excessivement moins importantes que celles des autres cryptomonnaies (voir Figure 4). Comme 1 kilooctet peut accueillir grosso modo 3 transactions, cela fait donc 0.01 centimes de dollars américains par transaction.

Cette taxation favorable contribue davantage à la pertinence du protocole Bitcore pour les transactions quotidiennes et pour les micropaiements.

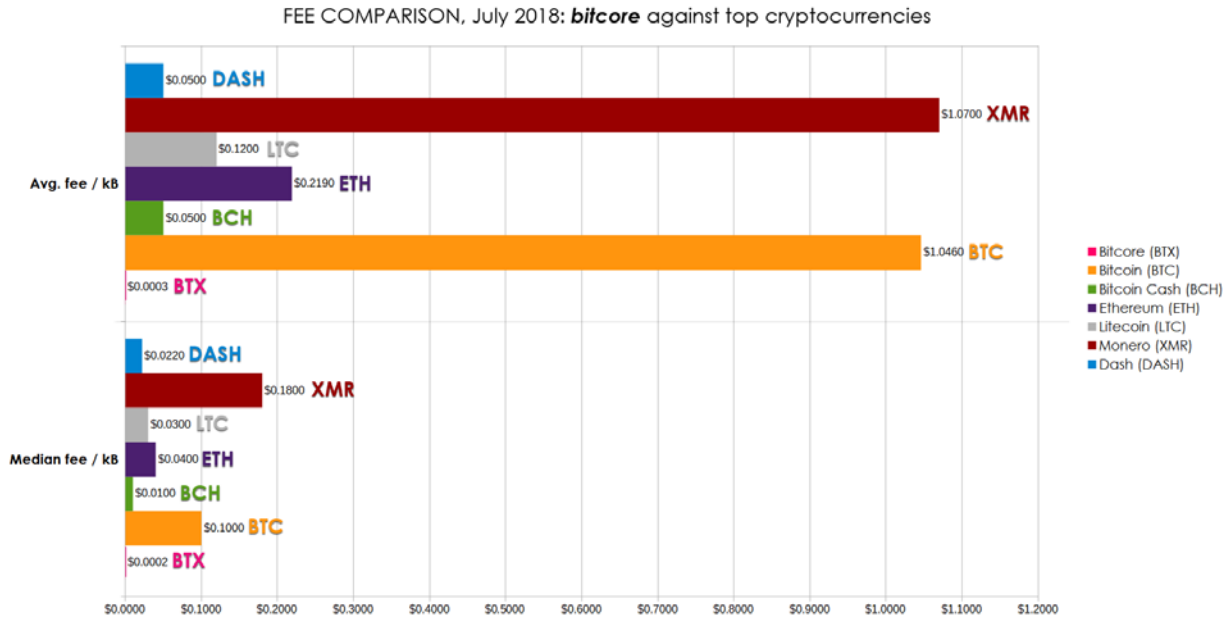

Figura 4: Table comparativa, Bitcore contra otras criptomonedas.

Comme Bitcore demande au minimum 0.00001 USD par kilooctet, la taxe recommandée en Juillet 2018 était de 0.001 BTX par kilooctet afin de soutenir la participation des mineurs. Actuellement, les blocs de Bitcore ne sont pas totalement remplis et payer une taxe plus importante pour augmenter la vitesse de transactions sera une réalité que lorsque la blockchain supportera un plus fort volume d'échanges et de transactions.

4 La communauté et la feuille de route

4.1 La communauté

Bitcore offre donc une variété d'avantages technologiques tels que des transactions rapides ou une faible taxe sur les transactions, ce qui la rend particulièrement pertinente pour des usages quotidiens. Cependant, Bitcore ne vit pas uniquement qu'à travers sa technologie : une force et un avantage considérable du Bitcore est sa communauté diverse et à facettes multiples.

Depuis ses premiers pas, Bitcore s'est efforcé à former une communauté dépassant les limites géographiques de notre monde. Cela s'est aperçu, entre autres, par la décision au sein de Bitcore d'outrepasser une ICO en faveur d'un mode de distribution des BTX décentralisé et équitable (voir la section 2.2) – une décision à la suite d'un vote de la communauté.

Le lieu et la nationalité est donc sans importance pour être un membre de la communauté Bitcore, mais la langue reste importante. C'est pourquoi Bitcore est présent sur différents réseaux sociaux, dans une multitude de pays et de langues et ce, depuis le commencement.

Il y a de nombreuses communautés secondaires au sein du Bitcore et dans une multitude de langues comme en Espagne ou en Turquie. Le but de Bitcore est de renforcer les initiatives dans ces régions qui contribuent fortement à la force de Bitcore, mais sans oublier que ces initiatives peuvent aussi naître avec force et conviction dans les autres pays et régions du monde.

4.2 La feuille de route

Comme précédemment présenté, le protocole Bitcore est un projet exclusivement communautaire.

Il n'y a aucune autorité centrale ou de comité exécutif responsable de certaines étapes faites pour satisfaire les actionnaires ou des investisseurs institutionnels.

Au contraire, Le développement du Bitcore répond aux besoins et visions des membres de sa communauté. L'histoire du Bitcore a montré que son mode opératoire et sa stratégie est propice à l'innovation et à l'implémentation rapide des améliorations incontournables.

Même s'il n'y a pas de feuilles de route pour les 10 prochaines années, l'équipe de Bitcore est bien entendu constamment au travail pour implémenter de nouvelles fonctionnalités requises par la communauté. Les projets en cours ou planifiés sont présents sur notre site officiel, https://bitcore.cc.

5 L'équipe

Chris

Développeur majeur en C++ et Qt

Chris est le développeur principal du Bitcore. Il travaille sur d'autres projets comme BitSend, Bitcloud et plus.

Jon

Administrateur des services et systèmes, et multi-compétences

Jon développe les API, l'Electrum et les infrastructures de Bitcore, et est le responsable de la maintenance de notre réseau de serveurs. Il était la personne en charge de la mise en place de l'*hybrid fork* et des *airdrops* hebdomadaires.

Steve

Ambassadeur de la marque et médias sociaux

Steve supervise le contact avec les échanges et les sites de listage, c'est notre homme n°1 pour les contacts professionnels.

David

Publications et Design graphique

David est la pensée artistique derrière Bitcore. Il fait aussi de la publication sur les médias sociaux et informe des travaux de l'équipe centrale.

Ivo

Chef de projet principal pour les services et les entreprises

Ivo contribue à la notoriété croissante du Bitcore sur le plan légal et technique.

Thomas

Gestionnaire des échanges

Thomas est notre manager responsable de la plupart de nos communications officielles avec les plateformes d'échanges et de services.

Greg (GM)

Expert en minage et manager d'un pool

Administrateur d'un pool de minage et aide aux minages via Telegram.

DgCarlosLeon

Dessinateur graphique et contributeur

Communication Reddit de Bitcore et graphiste.

Fahim Altınordu
Contributeur

Gestion des échanges internationaux et Turques.

Jose Martin
Manager de la communauté espagnole

Hampus
Contributeur

Hampus organise des campagnes de signature et gère des files de discussion sur de nombreux forums « altcoin ».

Brad
Contributeur

Brad gère la page officielle Facebook de Bitcore.

Ugur
Contributeur

Ugur gère la communauté turque du Bitcore et les travaux de soutien au Telegram turque.

Eric
Contributeur Facebook et Telegram.

Klaas
Contributeur

Klaas fournit un soutien sur les forums « altcoins » et Telegram.

Ibrahim Acir
Equipe de développeur en Turquie.

6 Avertissements légaux

Cette présentation n'est, et ne doit être interprété comme une offre, une invitation ou une recommandation à une offre, ou une sollicitation à une offre à acheter. L'investissement dans les cryptomonnaies est fortement spéculatif avec une forte volatilité comparée aux instruments d'investissement traditionnels et ne doit pas être approprié pour votre situation financière particulière. Les investisseurs potentiels sont priés de rencontrer des conseillers en finance, des comptables et autres conseillers de confiance, et d'évaluer si le Bitcore est un investissement approprié selon vos contraintes financières et vos objectifs. Les performances passées du Bitcore ne garantisse en rien ses performances futures.

Sources:

[i] https://blog.medium.com/what-are-bloom-filters-1ec2a50c68ff
[ii] Citing CoinCenter's definition of open source, https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects
[iii] https://medium.com/@jimmysong/bitcoin-diamond-super-bitcoin-bitcore-what-you-need-to-know-f49c35688a39
[iv] https://bitcoin.org/bitcoin.pdf
[v] https://opensource.org/osd
[vi] See https://www.reddit.com/r/Bitcoin/comments/18qy88/bitcoin_message_signing_and_verification/ for further details on message signing in Bitcoin.
[vii] https://medium.com/@jimmysong/bitcoin-diamond-super-bitcoin-bitcore-what-you-need-to-know-f49c35688a39
[viii] https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/
[ix] https://lightning.network/

Bitcore BTX
The future is NOW!

SEGWIT

www.bitcore.cc